Équations fonctionnelles de Mahler et applications aux suites p-régulières

Bernard Randé

▶ **To cite this version:**

Bernard Randé. Équations fonctionnelles de Mahler et applications aux suites p-régulières. Mathématiques [math]. Université Bordeaux 1, 1992. Français. NNT : . tel-01183330

HAL Id: tel-01183330
https://theses.hal.science/tel-01183330v1

Submitted on 7 Aug 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

N° d'ordre : 834

THÈSE

présentée à

L'UNIVERSITE BORDEAUX I

POUR OBTENIR LE GRADE DE DOCTEUR

SPECIALITE MATHEMATIQUES ET INFORMATIQUE

par

Bernard RANDE

EQUATIONS FONCTIONNELLES DE MAHLER ET APPLICATIONS AUX SUITES *p*-REGULIERES

Soutenue le 25 septembre 1992, devant la Commission d'Examen :

MM.	M. MENDES FRANCE	*Président*
	J.-P. ALLOUCHE	
	J.-M. DESHOUILLERS	
	J.-P. ELLOY	*Examinateurs*
	A. VAN DER POORTEN	
	G. RENAULT	
	M. WALDSCHMIDT	

– 1992 –

AVERTISSEMENT

La qualité de numérisation de ce fichier dépendant de l'état général de la microfiche, l'A.N.R.T. ne peut garantir un résultat irréprochable.

Le présent ouvrage est uniquement consultable en bibliothèque.

Cette thèse est dédiée à mon ami ***Christian Roy****, mathématicien mort en montagne. Parce que son souvenir est encore si vivant.*

Il est d'autant plus facile de remercier que l'on doit moins au récipiendaire. C'est dire si les lignes qui suivent auraient dû me demander de peine ; et il faut que le plaisir que j'ai pris à les écrire ait été bien grand pour qu'elles me paraissent si naturelles lorsque je les relis .

La chronologie étant le meilleur des diplomates en matière de préséance, je commencerai par ceux qui m'ont donné le goût des mathématiques, et celui de le transmettre : **Mme Larelle, Claude Deschamps, Georges Flory** ont beaucoup compté à cet égard. Ce serait plus que de l'ingratitude, ce serait de l'inconséquence que d'oublier le rôle que jouent l'enseignement, et l'enseignant, dans la construction des choix d'un jeune. Les classes préparatoires scientifiques en sont un exemple, suffisamment marquant pour que j'y aie exercé ensuite ; grâce à l'état d'esprit que j'y ai rencontré, au lycée Louis-le-Grand, à Paris, puis au lycée Clemenceau, à Nantes, grâce également à ceux qui, de plus haut, ont permis que je trouve les conditions optimales de travail : **Mme Deleau, MM. E.Ramis, P.Legrand, Dablanc, P.Attali, P.Deheuvels, Bernard-Brunet,** j'ai pu mener ce travail, sinon à bien, du moins à son terme. Les collègues y ont été nombreux, qui m'ont stimulé ou aidé : **R.Antetomaso, A.Warusfel, A.Tissier, D.Monasse, H.Pépin, D.Mollier, J.F. Ruaud, J.Yebbou, A.Pommellet.** J'aimerais y ajouter **Jacques Boutigny** et **Laurence Scetbun**, mes amis physicien et chimiste, dont la compréhension m'a été utile lors de périodes professionnelles...chargées. Un peu grâce à ces derniers, beaucoup grâce à eux-mêmes, mes élèves, tant à Paris qu'à Nantes, n'ont pas semblé devoir trop souffrir du temps que je ne leur consacrai pas : constatation seulement à demi-rassurante, mais tout de même apaisante!

Un itinéraire intellectuel étant par essence multivoque, je n'aurai garde d'oublier tous ceux qui, à des titres et dans des cadres divers, m'ont éveillé l'esprit par la puissance de leurs idées, la beauté de leurs points de vue, la rigueur de leur pensée, ou bien tout simplement le charme de leurs propos. Je pense, parmi beaucoup d'autres, et sans préjuger de ceux qui sont cités ailleurs, à **J.L Ouaert**, à **M.Cabanes**, à **Y.Duval**, à **G.Esposito**, à mon ami **Rached Mneimné**.

L'ouverture d'esprit, je l'ai rencontrée aussi dans le monde universitaire, et accompagnée de quelles autres qualités ! Non seulement au groupe de travail sur les automates finis, à Paris, mais aussi ici, à Bordeaux I. L'accueil que j'y ai trouvé,

malgré mes maigres apparitions, me laisse pantois, tant on n'ose pas même espérer que la gentillesse existe là où règnent les qualités intellectuelles auxquelles on adhère le plus. **Michel Mendès France**, président du jury, et **Jean-Marc Deshouillers**, devant qui j'ai l'honneur de soutenir cette thèse, en sont les vivants exemples. Et je ne sais qui remercier en premier lieu, des hommes ou des mathématiciens. Aussi, à travers eux, rendrai-je simplement hommage à tous ceux qui, depuis l'Université de Bordeaux I, ont aidé à la réalisation de ce travail.

Guy Renault et **Michel Waldschmidt** ont eux aussi des noms si prestigieux que j'oserais à peine les écrire si je n'avais à leur égard un autre devoir ; ce n'est rien de parler de l'honneur qu'ils me font en acceptant de critiquer ce travail. Il est plus délicat de présenter des excuses en guise de remerciements ! Il est de bon ton, à l'heure actuelle, de mépriser le don qu'ont certains à travailler vite. Pourtant, voilà un défaut qu'il m'aurait été bien agréable de posséder, et qu'à coup sûr les deux rapporteurs que j'ai cités ont été dans l'obligation d'acquérir, à tel point que le délai dont ils ont disposé entre la réception d'un travail approximativement lisible, et la remise ultime du rapport, est certainement le seul mérite dont cette thèse puisse se prévaloir pour entrer dans le livre Guinness des records!

Alf van der Poorten a fait vingt mille kilomètres pour venir jusqu'ici ; y a-t-il une meilleure façon de faire constater ce que je dois à l'un des plus grands spécialistes mondiaux du sujet que j'aborde dans les pages qui suivent ?

Si **Jean-Pierre Elloy** n'a fait que quatre cents kilomètres, depuis le laboratoire d'automatique de l'Ecole Centrale de Nantes, où j'ai rencontré tant d'amitiés et tant d'aide précieuse, il apporte avec lui le souffle vivant de l'informatique qui se fait et qui s'applique. Aussi, est-il un peu l'image de cet éclectisme qui me semble d'autant plus nécessaire qu'il est plus décrié, et que je suis fier de retrouver dans ce jury.

Je parlai tout à l'heure de l'atmosphère qui m'avait si vivement impressionné dans ce monde universitaire. Dévouement, compétence, disponibilité, imagination, vigueur intellectuelle: voilà des qualités que l'on prend plaisir à y reconnaître, et que résume **Jean-Paul Allouche**, sans qu'il s'y résume. Il peut sembler hautement funambulatoire de parler ainsi de celui qui, après tout, a dirigé votre travail pendant trois ans, et à qui vous devez trop pour que vous ne soyez pas soupçonné dans vos intentions. Que je prenne le risque de ces compliments est peut-être la meilleure preuve qu'ils les mérite. Mais puisque complimenter n'est pas remercier, je me contenterai de dire que seule l'amitié peut épuiser la gratitude que je lui dois.

Et, puisque j'ai prononcé le mot "amitié", oserai-je dresser la liste de toutes celles qui m'ont permis de travailler, ou plus profondément, qui m'en ont donné le goût? Outre qu'il me faudrait citer des noms qui l'ont déjà été, je sens, au moment de commencer, que cela est inutile, car il est des remerciements que chaque instant de la vie rend superflus.

Introduction.

Les automates finis ont été introduits, et sont utilisés, par les informaticiens. Les pliages de papiers l'ont été par les enfants, ou les adultes japonais. Par ailleurs, un mathématicien, Morse, il y a cinquante ans, s'intéressait à des géodésiques non fermées de certaines surfaces, tandis que Hardy, suivant Wedderburn, étudiait les propriétés analytiques des solutions d'une équation fonctionnelle.

Entre la transversalité et les ratons laveurs, il n'y a sans doute que des contingences historiques (avec un petit h), ou le vif sentiment d'une urgence rationnelle. Dans ce dernier cas, il faut penser qu'il était partagé puisque, quelque temps après, on trouve, dans le domaine qui nous occupe, outre les tenants des cocottes en papier, des théoriciens des nombres, des informaticiens, des analystes, des physiciens, des algébristes,ou des spécialistes des langages.

Une suite reconnue par automate peut être envisagée comme un mot infini d'un langage, point fixe d'une substitution ; comme une suite dont certaines sous-suites forment un ensemble fini ; enfin, comme la suite des coefficients d'une série entière, ou d'une série formelle, vérifiant une équation que l'on appellera ici de Mahler, répondant ainsi à un usage presque constitué, et à la nécessité de rendre hommage à celui qui, il y a un demi-siècle, avait déjà beaucoup dit à ce sujet.

Les suites automatiques ont été l'objet de nombreux travaux ; elles disparaissent dans ce travail derrière la notion de suite p-régulière, elle -même subsumée dans les solutions d'équations de Mahler. Il est vrai que le risque de toute généralisation est de faire disparaître la multiplicité des approches, pour n'en retenir qu'une qui motive la généralisation. Mais qui ne risque rien n'a rien ...

Pourquoi un mathématicien veut-il étudier les suites automatiques ? Pour, en premier lieu, disposer de nouveaux objets ; il convient alors de mesurer leur degré de nouveauté, par les propriétés qu'ils supportent, propriétés qui peuvent être, pour employer une comparaison que l'on pardonnera, phénotypique ou génotypique.

Lorsque Morse inventait la suite qui prit ultérieurement son nom (accolé à celui de Thue), il cherchait un individu, susceptible de l'aider à construire un objet donné; il suffit de consulter les exemples donnés en [1] pour constater qu'il n'y a pas beaucoup de mathématiciens, ou d'informaticiens théoriciens, qui n'auraient avantage, pour illustrer leur propos, à suivre l'exemple de Morse.

Pourtant, ce n'est pas dans cette perspective que nous travaillerons ; nous préférerons partir de l'interrogation suivante : étant donné un renseignement "standard" sur une suite automatique (ou p-régulière), que peut-on dire de la suite ?

Les théoriciens des nombres connaissent bien cette situation : des résultats d'approximation diophantienne conduisent à montrer qu'un nombre est, soit

rationnel, soit transcendant.... Comme si un renseignement normatif sur le nombre le forçait, soit à la banalité, soit à l'étrangeté. De façon analogue, nous aimerions constater qu'une suite p-régulière est, soit très banale (associée à une fraction rationnelle), soit assez étrange.

Une façon de mesurer ce comportement global de la famille des suites p-régulières (ou de leur généralisation) est donc d'obtenir un renseignement du style : si la suite est assez banale, elle l'est énormément. En réalité, nous ne raisonnerons jamais directement sur les suites elles-mêmes, mais toujours sur leurs séries génératrices. Pour simplifier, nous appellerons série régulière la série génératrice d'une suite (p-) régulière.

Se pose alors la question du cadre formel ; il s'agit du domaine dans lequel la suite prend ses valeurs . En ce qui concerne les suites automatiques, le choix est limité : à l'origine, c'est {0,1}, ou encore le corps à deux éléments, pour des raisons que l'on comprend aisément ; néanmoins, dés qu'il s'agit de la transcendance des valeurs prises par la série, il ne peut plus s'agir que d'un sous-corps de $\mathbb{C}$, ou, si l'on veut, d'un corps valué et complet.

Les mêmes possibilités s'ouvrent aux séries régulières ; en réalité, une suite u, régulière - c'est là l'intérêt de la notion- peut prendre ses valeurs dans n'importe quel anneau : sa définition nous dit seulement que (dans le cas de la 2-régularité) le module engendré par :

$$u(n),u(2n),u(2n+1),u(4n),\ldots,u(4n+3),u(8n),\ldots$$

est de type fini. Le cadre formel correspondant sera donc A((X)), qui présente l'avantage d'être un corps si A en est un. Ce sera aussi le cadre formel utilisé pour tout ce qui concerne les équations de Mahler ; pratiquement, A sera noethérien, souvent intègre de surplus, et finalement, pour ne rien cacher, un corps.

Les sous-anneaux de A((X)) stables par la substitution de X^2 à X nous serviront d'anneaux de base ; tant qu'il s'agit de suites régulières, A[X] et A(X) suffisent. En vue de la généralisation entreprise, nous aborderons l'étude de ces sous-anneaux, baptisés mahlériens. Le chapitre 2 établit un certain nombre de résultas algébriques sur ces structures.

Dans ce même chapitre, nous énonçons un théorème d'existence de solutions à des équations linéaires de Mahler ; ce théorème est insuffisant, et voici pourquoi: supposons que l'on ait établi un résultat de nature algébrique par des méthodes analytiques, en supposant $A = \mathbb{C}$. Ce résultat porte alors sur des fonctions méromorphes dans le disque unité. Pour l'appliquer aux séries formelles, il est nécessaire de disposer d'une bijection bien comprise avec les solutions dans $\mathbb{C} \subset [X]]$. Or, c'est ce que n'établit pas le théorème cité. Néanmoins, tant que l'on reste dans le cadre des fonctions régulières en 0, le transfert s'effectue agréablement.

Le chapitre 3 reste de nature algébrique : il aborde essentiellement la question de la caractérisation des séries p-régulières, et quelques problèmes connexes, qui sont l'objet de travaux de P.Dumas.

Le chapitre 4, de nature analytique, se fixe pour objet de montrer qu'une solution d'équation linéaire de Mahler, à coefficients dans $\mathbb{C}(x)$, est soit une

fraction rationnelle, soit transcendante sur $\mathbb{C}(x)$. La méthode est la suivante : on associe au problème scalaire d'ordre n un problème matriciel d'ordre un, et on établit, par des méthodes élémentaires de prolongement analytique, que , si le vecteur inconnu admet un point régulier sur le cercle, il est à coefficients fractions rationnelles ; il s'agit ensuite de montrer que, si tous les points du cercle unité sont singuliers pour le vecteur, alors ils le sont pour toutes les composantes. C'est dans cette étape que réside la difficulté. On utilise alors un résultat connu sur les singularités des solutions d'équations algébriques, résultat qui, faute de références, est établi en annexe.

Le chapitre 5 s'occupe d'hypertranscendance ; le résultat général conjecturé, précisé dans les questions in fine, est hors de portée des méthodes utilisées, qui permettent néanmoins de répondre à une conjecture de Rubel, et de donner quelques exemples d'équations algébriques de Mahler dont les solutions non rationnelles sont hypertranscendantes. Il faut noter que de nombreuses études ont été menées sur l'hypertranscendance de solutions d'équations fonctionnelles (par exemple [7], [11]). La principale difficulté, dans notre cas, réside en ceci que le changement de variable naturel $x = e^t$ ne conserve pas le corps des fractions rationnelles!

Le chapitre 6 est de nature essentiellement formelle, et a été écrit en vue de décortiquer, peut-être, la situation évoquée dans le chapitre 5 dans le cas général des équations d'ordre n. On obtient néanmoins un résultat, éventuellement inattendu, qui permet d'affirmer que, par exemple,une série régulière à coefficients complexes satisfait un équation algébrique de Mahler à coefficients entiers.

Le chapitre 7, s'inspirant de l'idée que de telles suites sont "soit très banales, soit assez étranges", est motivé par une conjecture de Loxton et van der Poorten généralisant un résultat de Cobham ; ce dernier affirme qu'une suite, reconnue par un 2-automate et un 3-automate, est ultimement périodique. Le résultat obtenu dans ce chapitre ne porte en fait que sur les équations d'ordre un.

Notations.

Autant que possible, les notations et conventions sont spécifiées au fur et à mesure de leur emploi. Néanmoins, certaines constantes de notation sont rappelées ici.

Les anneaux considérés sont toujours unifères ; A désigne un anneau commutatif, qui pourra être un corps. En revanche, K désignera nécessairement un corps.

La notation X fait toujours allusion à un cadre de séries formelles, tandis que x désigne l'argument d'une fonction. Ainsi, $\mathbb{C}(X)$ est le corps des fractions rationnelles à coefficients dans $\mathbb{C}$, tandis que $\mathbb{C}(x)$ désigne le corps des fonctions fractions rationnelles sur $\mathbb{C}$.

$M_{m,p}(A)$ désigne le module des matrices à n lignes et p colonnes à coefficients dans A. L'algèbre $M_{m,m}(A)$ sera souvent aussi notée $M_m(A)$.

L'opérateur μ_p de Mahler, défini au chapitre 2, sera souvent noté μ, tout au moins lorsque la confusion sur p ne sera pas possible. L'usage de l'une ou l'autre notation obéit à des motifs typographiques. On désigne par p un entier, non nécessairement premier, mais supérieur ou égal à 2.

L'ordre sur $K[X_0,...,X_n]$, qui en fait est un préordre, utilisé dans le chapitre 5, est celui qui est défini dans l'annexe 2.

On désigne par D un connexe ouvert dans $\mathbb{C}$. Ce pourra être le disque unité Δ ; en revanche, Δ désigne nécessairement le disque unité.

CHAPITRE 1

Ce chapitre a pour but de poser, dans un cas simple, les problématiques qui seront abordées dans un cadre plus général dans la suite. L'intérêt de cette démarche est évident : le formalisme est réduit au minimum, les calculs se font sans grande difficulté, et les résultats s'obtiennent à moindre coût. Les inconvénients sont moins apparents, mais réels; le principal est celui de laisser prévoir des généralisations dont le lecteur sera le plus souvent frustré. Par exemple, la transcendance des solutions de certaines équations fonctionnelles (paragraphe 4) ne sera obtenue dans un cadre plus général qu'au prix d'une restriction sur le corps de base (chapitre 4).

Le paragraphe 1 préfigure une partie des résultats du chapitre 2. Les paragraphes 2 et 3 introduisent des techniques réutilisées dans les chapitres 2 et 8. Le paragraphe 4, outre le chapitre 4, anticipe les notions introduites dans le chapitre 5.

Dans tout ce chapitre, A désigne un anneau commutatif unitaire et intègre; K désigne un corps algébriquement clos contenant A. Comme d'habitude, $A((X))$ désigne l'anneau des séries formelles de la forme $\sum_{k=-\infty}^{+\infty} a_k X^k$, où $(a_k)_{k\in\mathbb{Z}}$ est une famille d'éléments de A nuls pour k assez petit. Si A est un corps, $A((X))$ est aussi un corps.
On note p un entier supérieur ou égal à 2.

1. Solutions d'une équation fonctionnelle dans $A((X))$.

Soit b un élément de $A((X))$. On désigne par (1) l'équation fonctionnelle :

$$f(X) = b(X)f(X^p). \tag{1}$$

dont l'inconnue f est dans $A((X))$. On suppose $b \neq 0$.

Proposition 1.1. *Posons $\beta = val(b)$, et $b(X) = X^\beta b_1(X)$.*

(a) L'équation (1) admet une solution F non nulle si, et seulement si : $p-1$ divise β et $b_1(0) = 1$.

(b) Supposons les hypothèses du (a) vérifiées. L'ensemble des solutions de (1) est un A-module, engendré par :

$$\varphi(X) = X^{-\frac{\beta}{p-1}} \prod_{k=0}^{+\infty} b_1(X^{p^k}),$$

le produit infini convergeant pour la topologie canonique de $A((X))$.

Preuve :
Soit f une solution non nulle de (1), de valuation n. On pose :

$$f(X) = X^n f_1(X), \quad \text{avec} \quad f_1(0) \neq 0.$$

Nécessairement : $X^n f_1(X) = X^\beta X^{pn} f_1(X^p) b_1(X)$.

D'où : $n(1-p)=\beta$ et $f_1(X)=f_1(X^p)b_1(X)$. D'où encore, puisque $f_1(0)\neq 0$: $b_1(0)=1$. Il reste à déterminer l'ensemble des solutions de :

$$f_1(X)=b_1(X)f_1(X^p),\quad val(f_1)=0.$$

Nécessairement :

$$f_1(X)=\prod_{k=0}^{j} b_1(X^{p^k})\, f_1(X^{p^{j+1}}).$$

Comme $f_1(X^{p^{j+1}}) \underset{j\to+\infty}{\longrightarrow} f_1(0)$, on a :

$$\prod_{k=0}^{j} b_1(X^{p^k}) \underset{j\to+\infty}{\longrightarrow} \varphi_1(X),\quad \varphi_1(X)\in A[[X]],\quad \text{et}\quad f_1(X)=f_1(0)\varphi_1(X).$$

Montrons qu'effectivement la suite $(\prod_{k=0}^{j} b_1(X^{p^k}))_{j\geq 0}$ converge vers un élément de $A[[X]]$ de valuation nulle, ce qui complètera le résultat. Si l'on note $P_j(X)$ le terme général de cette suite, on a :

$$P_{j+1}(X)-P_j(X)=[b_1(X^{p^{j+1}})-1]P_j(X).$$

Or : $val[b_1(X^{p^{j+1}})-1]\geq p^{j+1}$.
Donc : $P_{j+1}-P_j \underset{j\to+\infty}{\longrightarrow} 0$, et $P_j \underset{j\to+\infty}{\longrightarrow} \varphi_1$, avec $\varphi_1(0)=1$.

2. Un cas particulier.

Dans l'équation (1), supposons à présent que $b\in A(X)$. On peut, grâce à l'étude précédente, supposer que $val(b)=0$ et que $b(0)=1$. Plongeons A dans un corps K algébriquement clos, et posons :

$$b(X)=\prod_{\alpha\in K^*}(1-\alpha X)^{m(\alpha)},$$

où $m : K^*\to\mathbb{Z}$ est une fonction à support fini.

Cherchons f sous la forme :

$$f(X)=\prod_{\alpha\in K^*}(1-\alpha X)^{\varphi(\alpha)},$$

où $\varphi : K^*\to\mathbb{Z}$ est, elle aussi, à support fini.

Proposition 1.2. *Soit A un anneau intègre, dont la caractéristique ne divise pas p. Soit :*

$$f(X) = \prod_{\alpha \in A \setminus \{0\}} (1 - \alpha X)^{\varphi(\alpha)},$$

un élément de $A(X)$. Alors :

$$f(X^p) = \prod_{\alpha \in A \setminus \{0\}} (1 - \alpha X)^{\varphi(\alpha^p)}.$$

Preuve :
Dans K, clôture algébrique de A, le polynôme $Y^p - 1$ admet p racines distinctes. Notons Ω leur ensemble, et désignons par S un système de représentants de K^*/Ω. Cet ensemble est donc en bijection avec K^* par :

$$\begin{aligned} S &\to K^* \\ \alpha &\mapsto \alpha^p \end{aligned}$$

Il vient alors :

$$\begin{aligned} f(X^p) &= \prod_{\alpha \in K^*} (1 - \alpha X^p)^{\varphi(\alpha)} = \prod_{\beta \in S} (1 - \beta^p X^p)^{\varphi(\beta^p)} \\ &= \prod_{\beta \in S} \prod_{\omega \in \Omega} (1 - \beta\omega X)^{\varphi((\beta\omega)^p)} \\ &= \prod_{\alpha \in K^*} (1 - \alpha X)^{\varphi(\alpha^p)}. \end{aligned}$$

Proposition 1.3. *Soit A un anneau intègre dont la caractéristique ne divise pas p, K un corps algébriquement clos contenant A, b un élément de $A(X)$, de la forme :*

$$b(X) = \prod_{\alpha \in K^*} (1 - \alpha X)^{m(\alpha)}.$$

Pour qu'il existe une solution f, non nulle, appartenant à $A(X)$, de l'équation :

$$f(X) = b(X) f(X^p),$$

il faut et il suffit qu'il existe une application φ, de K^* dans $\mathbb{Z}$, à support fini, telle que :

$$\forall \alpha \in K^* \quad \varphi(\alpha) - \varphi(\alpha^p) = m(\alpha).$$

Preuve :
Dans $K(X)$, cette équivalence résulte immédiatement de la proposition 1.2, et du fait que f *est nécessairement* de valuation nulle.
Reste à vérifier que, s'il existe une solution non nulle g dans $K(X)$, il existe une solution non nulle f dans $A(X)$. Soit :

$$\varphi = \prod_{k=0}^{+\infty} b(X^{p^k}),$$

qui est un élément de $A[[X]]$. D'après la proposition 1.1, on a : $\varphi = ag$, où a appartient à K.
Donc : $\varphi \in K(X) \cap A[[X]]$. Il en résulte que φ appartient à $A(X)$ grâce, par exemple, à la caractérisation de Hankel des éléments de $A[[X]]$ qui sont dans $A(X)$.

Interprétation.

On peut identifier un élément f de $K(X)$, de valuation nulle et tel que $f(0) = 1$, à la famille $(\varphi(\alpha))_{\alpha \in K^*}$; c'est-à-dire à un élément de $\mathbb{Z}^{(K^*)}$. Cette identification transforme la loi $\times$ en la loi $+$. Considérons alors l'application :

$$\begin{aligned} \Psi : \quad \mathbb{Z}^{(K^*)} &\to \mathbb{Z}^{K^*} \\ \varphi \quad &\mapsto (\varphi(\alpha) - \varphi(\alpha^p))_{\alpha \in K^*}. \end{aligned}$$

Elle arrive en fait dans $\mathbb{Z}^{(K^*)}$. Si, en effet, α et α^p n'appartiennent pas au support de φ, noté $supp(\varphi)$, on a : $\varphi(\alpha) - \varphi(\alpha^p) = 0$. Il en résulte que le support de $\Psi(\varphi)$ est inclus dans :

$$supp(\varphi) \cup \{x \in K^*,\ x^p \in supp(\varphi)\}.$$

Ce dernier ensemble est évidemment fini. La proposition 2 nous dit alors que $Im(\Psi)$ coïncide avec l'ensemble des fractions de la forme $\frac{f(X)}{f(X^p)}$. Nous allons étudier cet ensemble de plus près.

3. Un sous monoïde de $(A[X]\backslash\{0\}, \times)$.

Dans ce paragraphe, A est un corps.

L'ensemble des éléments de $A(X)$, image de $f \mapsto \frac{f(X)}{f(X^p)}$, est évidemment un sous-groupe de $A(X)\backslash\{0\}$. Nous allons nous limiter à l'étude des éléments de $A[X]$ qui sont dans ce sous-groupe : leur ensemble forme un sous-monoïde de $A[X]\backslash\{0\}$, noté $\mathcal{M}_p$.

Lemme. *Soient h, k deux éléments de $A[X]$, premiers entre eux. Alors $h(X^p)$, $k(X^p)$ sont aussi premiers entre eux.*

Preuve :
Cela résulte immédiatement de l'égalité de Bezout.

Remarque.
Ce résultat serait encore vrai dans le cas d'un anneau factoriel A. Soit en effet B le corps des fractions de A; $h(X^p)$ et $k(X^p)$ sont premiers entre eux dans $B[X]$. Mais $cont(h) = cont(h(X^p))$, $cont(k) = cont(k(X^p))$. Donc, d'après Gauss, $h(X^p)$ et $k(X^p)$ sont premiers entre eux dans $A[X]$.

Proposition 1.4. *Soit $b \in A[X]$, $val(b) = 0$. Pour que b appartienne à $\mathcal{M}_p$, il faut et il suffit qu'il existe h, de valuation nulle, appartenant à $A[X]$, tel que :*

$$b(X) = \frac{h(X^p)}{h(X)}.$$

Preuve :
Un sens étant évident, supposons b dans $\mathcal{M}_p$. On peut écrire :

$$b(X) = \frac{f(X^p)}{f(X)}, \text{ avec } f \in A[X],\ val(f) = 0,\ f(0) = 1.$$

Posons $f = \dfrac{h}{k}$, avec $pgcd(h, k) = 1$. On a donc :

$$b(X)h(X)k(X^p) = k(X)h(X^p).$$

Il en résulte que $k(X^p)$ divise $k(X)h(X^p)$, donc (lemme), que $k(X^p)$ divise $k(X)$. Ceci impose $k = 1$, puis le résultat.

Posons alors $h(X) = \prod_{\alpha \in K^*}(1 - \alpha X)^{\varphi(\alpha)}$, et déterminons une condition nécessaire et suffisante pour que $h(X)$ divise $h(X^p)$, ce qui équivaut, d'après la proposition 1.3, à :

(3) $$\forall \alpha \in K^*, \quad \varphi(\alpha) \leq \varphi(\alpha^p).$$

Il est commode de mettre sur K^* la relation de préordre :

$$\alpha \prec \beta \text{ si et seulement si } \exists k \in \mathbb{N}, \quad \beta = \alpha^{p^k}.$$

La condition (3) s'exprime alors en disant que φ est croissante.

Le lemme suivant décrit les classes d'équivalence associées à la relation $\prec$.

Lemme. *Soit $n \in \mathbb{N}^*$. Posons $n = p^m q$, avec $pgcd(p,q) = 1$, et $m \in \mathbb{N}$. Il existe un couple (k,l) de $\mathbb{N} \times \mathbb{N}$, avec $l > k$, tel que :*

$$p^l \equiv p^k \mod(n).$$

De plus, le plus petit couple (k,l) (pour l'ordre lexicographique habituel sur $\mathbb{N}^2$) vérifiant ces propriétés est défini par :

$$k = m;\ l = m + \omega, \quad \text{où } \omega \text{ est l'ordre de } p \text{ dans } ((\mathbb{Z}/q\mathbb{Z})^*, \times).$$

Preuve :
Le couple indiqué convient. On a en effet : $p^\omega \equiv 1 \mod(q)$, et donc : $p^{\omega+m} \equiv p^m \mod(n)$.
Soit réciproquement un couple (k,l) qui convient. On a :

$$p^k(p^{l-k} - 1) \equiv 0 \mod(p^m q),$$

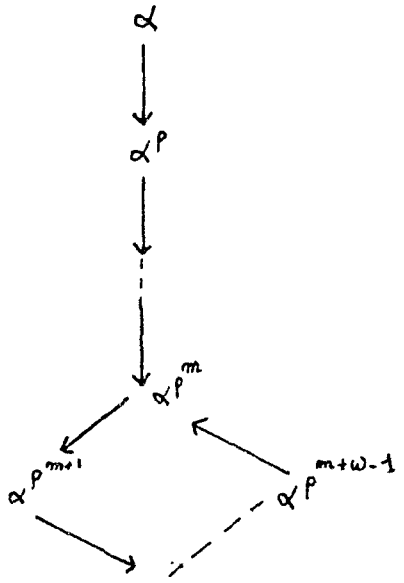
donc $k \geq m$. Si de plus $k = m$, on obtient :

$$p^{l-k} - 1 \equiv 0 \mod(q),$$

donc $l - k \geq \omega$.

Dans ces conditions, le procédé pour déterminer si $h(X)$ divise $h(X^p)$ est le suivant :

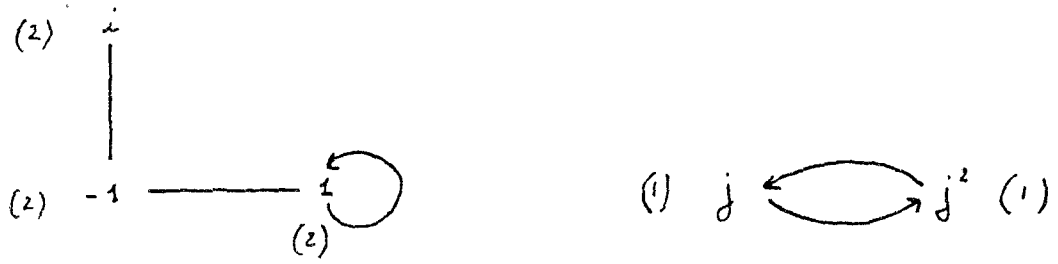
Soit α tel que $\varphi(\alpha) \geq 1$; on a donc, pour tout $k \in \mathbb{N}$, $\varphi(\alpha^{p^k}) \geq 1$.
Il en résulte que la suite $(\alpha^{p^k})_{k \geq 0}$ ne peut être injective, et que α est une racine de l'unité.
D'après le lemme, si n est l'ordre de α, on a la situation suivante, la notation "$x \to y$" signifiant "$x \prec y$" :



La partie fermée du graphe correspond aux éléments équivalents. La condition cherchée est donc la croissance de la fonction φ sur la partie initiale du graphe, et sa constance sur la partie fermée.

Illustration 1.

Cherchons l'élément h de $\mathbb{C}[X]$, de plus petit degré, tel que $h(X)$ divise $h(X^2)$, et qui soit divisible par $(X-j)(X-i)^2(X+1)$. On dispose du diagramme suivant



Le polynôme cherché est :

$$(X-i)^2(X-1)^2(X+1)^2(X-j)(X-j^2).$$

Illustration 2.

Cherchons les polynômes irréductibles h de $\mathbb{Q}[X]$ tels que $h(X)$ divise $h(X^p)$; h est nécessairement un polynôme cyclotomique Φ_n.

Premier cas : $pgcd(n,p) \neq 1$.
Soit α une racine primitive n-ième de 1. Alors α^p n'est pas racine primitive n-ième de 1 : donc $\Phi_n(X)$ ne divise pas $\Phi_n(X^p)$.

Deuxième cas : $pgcd(n,p) = 1$.
Si α est racine de Φ_n, α^p est aussi racine de Φ_n. Comme les racines de Φ_n sont simples, on en déduit que $\Phi_n(X)$ divise $\Phi_n(X^p)$.

On montrerait de façon analogue que les polynômes h de $\mathbb{Q}[X]$ tels que $h(X)$ divise $h(X^p)$ sont de la forme :

$$\prod_{pgcd(p,q)=1} \prod_{m=0}^{N_q} \Phi_{p^m q}(X).$$

4. Indépendance algébrique d'une famille de solutions d'équations fonctionnelles.

Introduction. Multidegré d'un élément de $A[X_i]_{i\in\mathbb{N}}$.

Nous mettons sur $\mathbb{N}^{n+1}$ l'ordre suivant :

. pour $n = 0$, c'est l'ordre usuel,

. nous disons que $(p_0, \cdots, p_n)$ est plus petit que $(q_0, \cdots, q_n)$ si ou bien $p_n < q_n$, ou bien $p_n = q_n$ et $(p_0, \cdots, p_{n-1})$ est plus petit que $(q_0, \cdots, q_{n-1})$.

Nous étendons ensuite cet ordre à $\mathbb{N}^{(\mathbb{N})}$, considéré comme réunion croissante des $\mathbb{N}^{n+1}$, pour n décrivant $\mathbb{N}$. On obtient alors un bon ordre sur $\mathbb{N}^{(\mathbb{N})}$.

Soit alors P un élément de $A[X_i]_{i\in\mathbb{N}}$, identifié à la famille $(p_\alpha)_{\alpha\in\mathbb{N}^{(\mathbb{N})}}$ de ses coefficients dans la base $(X^\alpha)_{\alpha\in\mathbb{N}^{(\mathbb{N})}}$. Ici $X^{(\alpha)}$ désigne $X_0^{\alpha_0}X_1^{\alpha_1}\cdots X_n^{\alpha_n}$, lorsque α désigne $(\alpha_0, \alpha_1, \cdots, \alpha_n)$.

Définition. *Soit $P \in A[X_i]_{i\in\mathbb{N}}$, $P \neq 0$. On appelle multidegré de P l'élément $deg(P)$ égal à :*

$$max\{\alpha \in \mathbb{N}^{(\mathbb{N})},\ \ p_\alpha \neq 0\}.$$

Exemple.
Le multidegré de $X_3X_0 + X_2^2X_0^5 + X_1^8$ est $(3, 0, 0, 1)$.

Proposition 1.5. *Soit A un corps, $(b_0, \cdots, b_n)$ une famille d'éléments non nuls de $A(X)$, de valuation nulle, tels que $b_i(0) = 1$, et θ_i solution de*

$$\theta_i(X^p) = b_i(X)\theta_i(X).$$

Si la famille $(\theta_0, \cdots, \theta_n)$ est algébriquement liée sur $A(X)$, elle est multiplicativement liée sur $A(X)$.

Preuve :
Soit $P \in A(X)[Y_0, \cdots, Y_n]$ un polynôme non nul, de multidegré minimal, tel que

$$P(\theta_0, \cdots, \theta_n) = 0.$$

Posons $P(Y_0, \cdots, Y_n) = \sum_{\alpha\in\mathbb{N}^{n+1}} p_\alpha(X)Y^\alpha$, et $\delta = deg(P)$.
Il n'est pas restrictif de supposer que $p_\delta = 1$.
On a donc : $\sum_{\alpha\in\mathbb{N}^{n+1}} p_\alpha\theta_0(X)^{\alpha_0}\cdots\theta_n(X)^{\alpha_n} = 0$,
et par conséquent : $\sum_{\alpha\in\mathbb{N}^{n+1}} p_\alpha(X^p)\theta_0(X^p)^{\alpha_0}\cdots\theta_n(X^p)^{\alpha_n} = 0$.
D'où : $\sum_{\alpha\in\mathbb{N}^{n+1}} p_\alpha(X^p)b_0(X)^{\alpha_0}\cdots b_n(X)^{\alpha_n}\theta_0(X)^{\alpha_0}\cdots\theta_n(X)^{\alpha_n} = 0$.
Le polynôme $Q(Y_0, \cdots, Y_n) = \sum_{\alpha\in\mathbb{N}^{n+1}} q_\alpha(X)Y^\alpha$, où :

$$q_\alpha(X) = b_0(X)^{\alpha_0}\cdots b_n(X)^{\alpha_n}p_\alpha(X^p),$$

annule donc $(\theta_0, \cdots, \theta_n)$, et est toujours à coefficients dans $A(X)$. Il en résulte que le polynôme $q_\delta P - Q$, qui annule $(\theta_0, \cdots, \theta_n)$, et est de multidegré strictement plus petit que δ, est le polynôme nul. D'où :

$$\forall \alpha \in \mathbb{N}^{n+1}, \quad q_\delta p_\alpha = q_\alpha.$$

Il existe α, différent de δ, tel que $p_\alpha \neq 0$: sinon, l'un des θ_i est nul On obtient ainsi :

$$b_0(X)^{\delta_0} \cdots b_n(X)^{\delta_n} p_\alpha(X) = b_0(X)^{\alpha_0} \cdots b_n(X)^{\alpha_n} p_\alpha(X^p).$$

Il en résulte, en posant $\mu_i = \alpha_i - \delta_i$:

$$\theta_0(X)^{\mu_0} \cdots \theta_n(X)^{\mu_n} p_\alpha(X) = \theta_0(X^p)^{\mu_0} \cdots \theta_n(X^p)^{\mu_n} p_\alpha(X^p),$$

et donc (d'après l'unicité dans la proposition 1.1) :

$$\theta_0(X)^{\mu_0} \cdots \theta_n(X)^{\mu_n} p_\alpha(X) \in A.$$

Donc $\theta_0(X)^{\mu_0} \cdots \theta_n(X)^{\mu_n} \in A(X)$.
Puisque $(\mu_0, \cdots, \mu_n) \neq (0, \cdots, 0)$, le résultat est démontré.

Corollaire. *Soit A un corps de caractéristique ne divisant pas p, b un élément non nul de $A(X)$, de valuation nulle, tel que $b(0) = 1$, et θ une solution non nulle, dans $A((X))$, de l'équation :*

$$\theta(X^p) = b(X)\theta(X).$$

Si θ est algébrique sur $A(X)$, alors $\theta \in A(X)$.

Preuve :
D'après la proposition 1.5, $\theta(X)^\mu \in A(X)$, pour un $\mu \neq 0$. Posons $\psi(X) = \theta(X)^\mu$. On a alors :

$$\frac{\psi(X^p)}{\psi(X)} = b(X)^\mu.$$

Posons alors $b(X) = \prod_{\alpha \in K^*}(1 - \alpha X)^{m(\alpha)}$, $\psi(X) = \prod_{\alpha \in K^*}(1 - \alpha X)^{\varphi(\alpha)}$.
D'après l'étude du paragraphe 2, on a :

$$\forall \alpha \in K^*, \quad \mu m(\alpha) = \varphi(\alpha^p) - \varphi(\alpha),$$

et donc :

$$\mu[m(\alpha) + \cdots + m(\alpha^{p^n})] = \varphi(\alpha^{p^{n+1}}) - \varphi(\alpha).$$

Soit alors $\beta \in K^*$; β admet p^{n+1} racines p^{n+1}-ièmes. Comme $supp(\varphi)$ est fini, il existe n et α tels que $\alpha^{p^{n+1}} = \beta$ et $\varphi(\alpha^{p^{n+1}}) = 0$. Donc $\varphi(\alpha) \equiv 0 \ mod(\mu)$.

Il en résulte que :

$$v(X) = \lambda(X)^{\mu}, \quad \text{où} \quad \lambda \in K(X),$$

et donc que :

$$\theta(X) = \omega\lambda(X), \quad \text{où} \quad \omega^{\mu} = 1.$$

Finalement : $\theta \in K(X)$.

Mais $\theta \in A((X))$. Il en résulte que $\theta \in A(X)$ (*cf.* la fin de la preuve de la proposition 1.3).

Remarque.

Le corollaire peut s'interpréter de la façon suivante : *l'extension* $A(X)(\theta)$ *est une extension transcendante pure de* $A(X)$.

CHAPITRE 2

Ce chapitre est consacré aux équations de Mahler linéaires. Ce sont des équations fonctionnelles exprimant une dépendance linéaire entre $f(X), f(X^p), \cdots, f(X^{p^n})$, où f est une série formelle.
La structure adaptée à cette étude est celle "d'algèbre p-mahlérienne", c'est-à-dire d'une algèbre de séries formelles stable par la substitution de X^p à X. Le théorème principal du paragraphe 1, (théorème 1), caractérise les sous-corps de $A(X)$, (ici, A est un corps), qui sont p-mahlériens. Outre les "évidents", (c'est-à-dire les $A(X^d)$), on en découvre une nouvelle race : ceux engendrés par $X^d + \frac{\varepsilon}{X^d}$, où $\varepsilon^{p-1} = 1$. Ils sont bien entendu étroitement liés aux polynômes de Tchebychev.
En ce qui concerne les sous-algèbres p-mahlériennes de $A[X]$, la situation est loin d'être aussi limpide : il semble qu'il y en ait d'exotiques. Les résultats obtenus dans cette direction sont très partiels : cela résulte de la difficulté à décrire les sous-algèbres de $A[X]$. Les résultats obtenus sont valables en caractéristique ne divisant pas p.

Le paragraphe 2 étudie le cas simple des équations de Mahler linéaires sur l'anneau de base. Le cas d'un anneau intègre est évident (proposition 2); dans le cas général, on se ramène aisément à l'étude des solutions de valuation plus grande que 1 : elles sont toutes annulées par un élément non nul de A (théorème 2).

Lorsque l'on peut exprimer $f(X^{p^n})$ en fonction de $f(X), \cdots, f(X^{p^{n-1}})$, on dit que l'équation de Mahler est résoluble à gauche. Cette situation est agréable pour l'étude globale de l'ensemble $ML_p(B)$ des solutions de telles équations, sous réserve de supposer B nœthérienne (proposition 5). $ML_p(B)$ est en effet une B-algèbre (théorème 3). Les résultats de ce genre s'apparentent à ceux concernant les entiers algébriques. La situation actuelle diffère de la précédente en ce qu'il n'y a pas de relation "universelle" de liaison, du type Cayley-Hamilton.

On étudie un cas particulier : un polynôme de $A[X]$ (A est un corps), vérifie une équation de Mahler résoluble à gauche sur $A[X]$, équation dont on mesure la taille (proposition 6). Le cas des corps finis A de caractéristique p est simple : $ML_p(A[X])$ est l'anneau des entiers algébriques de $A[[X]]$ sur $A[X]$ (proposition 8).
De façon générale, on constate que la caractéristique p transforme une équation de Mahler en une équation plutôt algébrique, tandis que le cas général conduit à des situations plutôt transcendantes.

Lorsqu'au contraire c'est $f(X)$ qui s'exprime à l'aide de $f(X^p), \cdots, f(X^{p^n})$, l'équation est dite résoluble à droite. Cette fois, c'est l'étude d'une équation donnée qui est favorisée. Les propositions 11 et 12 donnent des résultats d'existence et d'unicité dans cette direction. La difficulté provient en réalité du fait que $A((X))$ n'est pas fermée : la présence de $\frac{1}{X}$ conduit, par itération, à des conditions de compatibilité parfois lourdes à exprimer.

On étudie le cas particulier où $f \in A[X]$, A étant un corps : la différence entre les équations résolubles à droite et celles résolubles à gauche, apparaît clairement (proposition 10). Le cas où les coefficients de l'équation sont dans $A(X)$ cumule les avantages des deux points de vue : cette situation sera donc favorisée dans la suite.

1. *Soit p un entier supérieur ou égal à 2, et A un anneau commutatif et unitaire.* Considérons $A((X))$, anneau des séries formelles $\sum_{-\infty}^{+\infty} a_n X^n$ à coefficients dans A, où $(a_n)_{n\in\mathbb{Z}}$ est une suite nulle pour n assez petit. Si A est un corps, $A((X))$ est aussi un corps. Dans $A((X))$, on dispose de l'application μ_p, notée plus rapidement μ, substitution de X^p à X :

$$\begin{aligned} \mu \ : \ A((X)) &\to A((X)) \\ S(X) &\mapsto S(X^p). \end{aligned}$$

On a donc :

$$\forall S \in A((X)) \quad [\mu(S)](X) = S(\mu(X)). \tag{1}$$

Cette application μ est un endomorphisme de A-algèbre, comme on le voit aisément grâce à (1). Si $S(X) = \sum_{-\infty}^{+\infty} a_n X^n$, on a donc :

$$[\mu(S)](X) = \sum_{-\infty}^{+\infty} a_n X^{pn}.$$

Il en résulte que μ est injective. Son image n'est autre que $A((X^p))$.

Définition. *Soit B une sous-A-algèbre de $A((X))$. B est dite p-mahlérienne lorsqu'elle est stable par μ. Lorsque B est en outre un corps, on parlera de corps p-mahlérien.*

Exemples.

Exemple 1 : $A[X]$, $A(X)$, $A[[X]]$, $A((X))$ sont p-mahlériennes.

Exemple 2 : Soit q un entier relatif. Les A-algèbres $A[X^q]$, $A(X^q)$ sont p-mahlériennes. Si q est un entier naturel, il en est de même de $A[[X^q]]$ et $A((X^q))$.

Exemple 3 : Soit, plus généralement, P un élément de $A[X]$ tel que $P(X^p)$ soit un polynôme en P. Par récurrence sur n, $P(X^{p^n})$ est encore un polynôme en P. Il en résulte que $A[P]$ et $A(P)$ sont p-mahlériennes. Si en outre P est de valuation 0, $A[[P]]$ est elle ausi p-mahlérienne.

Illustration Soit p un nombre premier, $A = \mathbb{Z}/p\mathbb{Z}$, et P un élément de $A[X]$. Puisque $P(X^p) = P(X)^p$, $A[P]$ et $A(P)$ sont p-mahlériennes. De façon générale, toute sous-algèbre de $A((X))$ est p-mahlérienne.

En caractéristique nulle, la portée de la généralisation obtenue en passant de l'exemple 2 à l'exemple 3 est mesurée par la proposition 1, qui repose sur le lemme suivant :

Lemme. *Soit A un anneau intègre, de caractéristique ne divisant pas p, et P un élément de $A[X]$ tel que $P(X^p)$ soit un polynôme en P. Il existe alors $(a, b) \in A^2$ et $q \in \mathbb{N}^*$ tels que :*

$$P(X) = aX^q + b.$$

Preuve :
Soit $q = deg(P)$. Raisonnons par l'absurde en supposant que P n'est pas de la forme indiquée. On a donc $q \geq 2$. Soit $n = max\{k \in [1, q-1],\ a_k \neq 0\}$ où les a_i sont les coefficients de P; n est bien défini, puisque $(a_1, \cdots, a_{q-1}) \neq (0)$. De plus, $n \in [1, q-1]$. Ecrivons donc :

$$P(X) = a_q X^q + \sum_{k=0}^{n} a_k X^k$$

et donc :

$$P(X^p) = a_q X^{pq} + \sum_{k=0}^{n} a_k X^{pk}.$$

On sait qu'il existe $Q \in A[Y]$ tel que :

$$P(X^p) = Q(P(X)) \tag{2}$$

En particulier on peut écrire :

$$deg(P(X^p)) = pq = deg(Q \circ P) = p\ deg(Q),$$

la dernière égalité car A est intègre.
D'où :

$$deg\ Q = p \ \text{ et } \ Q(Y) = \sum_{k=0}^{p} b_k Y^k, \ \ b_p \neq 0.$$

L'égalité (2) se réécrit ainsi :

$$a_q X^{pq} + \sum_{k=0}^{n} a_k X^{pk} = \sum_{k=0}^{p} b_k (P(X))^k.$$

À gauche, le coefficient de $X^{(p-1)q+n}$ est nul, puisque $pq > (p-1)q + n > pn$.
Si, de plus, $k \in [0, p-1]$, on a :

$$deg(P(X)^k) \leq (p-1)q < (p-1)q + n.$$

Le coefficient de $X^{(p-1)q+n}$ dans le membre de droite est donc $\binom{p}{1} a_q^{p-1} a_n b_p$, et ce terme est non nul. D'où la contradiction.

Proposition 2.1. *Soit A un corps, de caractéristique ne divisant pas p, et B une sous-A-algèbre de $A[X]$, p-mahlérienne, engendrée par un polynôme P. Il existe alors un entier naturel q tel que :*

$$B = A[X^q].$$

Preuve :
On peut écrire $B = A[P]$, et $\mu(P) \in B$. Donc $\mu(P)$ est un polynôme en P, et par conséquent (lemme) :

$$P(X) = aX^q + b.$$

Il est alors clair (si $a \neq 0$) que $B = A[X^q]$. Si $a = 0$, $B = A$.

Étudions à présent plus complètement le cas d'un sous-corps p-mahlérien de $A(X)$, lorsque A est un corps. Soit φ une fraction rationnelle, écrite sous forme irréductible $\varphi = \frac{\psi}{\theta}$, $\varphi \neq 0$. On pose : $deg\ \varphi = deg\ \psi - deg\ \theta$. Bien entendu, si $\varphi = \frac{\psi_1}{\theta_1}$, on aura aussi : $deg\ \varphi = deg\ \psi_1 - deg\ \theta_1$. Soit par ailleurs P un polynôme tel que : $\varphi = P^k \varphi_1$, où φ_1 est une fraction rationnelle dont le numérateur ψ_1 et le dénominateur ϑ_1 ne sont pas divisibles par P. On note alors : $k = v_P(\varphi)$. Cette notation ne suppose pas P irréductible.
Pour exprimer que α est pôle d'une fraction rationnelle φ, on notera : $\varphi(\alpha) = \infty$.

Lemme 1. *Soient A un corps, $\varphi \in A(X)\backslash\{0\}$, et $P \in A(X)\backslash\{0\}$. Si $deg\ P > 0$, on a : $deg(\varphi \circ P) = deg\ \varphi \times deg\ P$.*

Preuve :
Posons : $\varphi = \frac{\psi}{\theta}$, avec $\psi = \sum_{k=0}^{n} a_k X^k$, $a_n \neq 0$. Posons aussi $P = \frac{R}{S}$, où $R, S \in A[X]$. On a :

$$\psi(\frac{R}{S}) = \frac{1}{S^n} \sum_{k=0}^{n} a_k R^k S^{n-k}.$$

Si $k \neq n$, on a :

$$deg(R^k S^{n-k}) = k\ deg\ R + (n - k)\ deg\ S < n\ deg\ R.$$

Donc

$$deg(\sum_{k=0}^{n} a_k R^k S^{n-k}) = deg\ R^n,$$

et :

$$deg\ \psi(\frac{R}{S}) = n\ deg\ \frac{R}{S} = deg\ \psi \times\ deg\ P.$$

De même,

$$deg\ \theta(\frac{R}{S}) = deg\ \theta \times deg\ P.$$

Donc :

$$deg(\varphi o P) = deg\ \varphi \times deg\ P.$$

Lemme 2. *Soient $P \in A(X)$, où A est un corps dont la caractéristique ne divise pas p, $\alpha \in A\backslash\{0\}$, et $v = v_\Pi(\mu(P))$, où $\Pi(X) = X - a$. Alors, si $\Pi_1 = X - \alpha^p$, on a : $v_{\Pi_1}(P) = v$.*

Preuve :
On peut écrire : $P(X^p) = (X-\alpha)^v P_1(X)$, et α n'est ni pôle, ni zéro de P_1.
Il n'est pas restrictif de supposer A algébriquement clos. Soit donc ω une des p racines p-ièmes de 1 dans A.
On a :

$$P(X^p) = (\omega X - \alpha)^v P_1(\omega X);$$

Les polynômes $(\omega X - \alpha)$ sont premiers entre eux deux à deux. Donc :

$$P(X^p) = \prod_{\omega^p=1} (\omega X - \alpha)^v . S(X) = (X^p - \alpha^p)^v S(X).$$

Il en résulte que $S \in A(X^p)$: $S(X) = S_1(X^p)$.
D'où :

$$P(X) = (X - \alpha^p)^v S_1(X).$$

Si $S_1(\alpha^p) = 0$, on a : $S(\alpha) = 0$ et donc $(X-\alpha)^{v+1}$ divise $P(X^p)$, ce qui n'est pas. De même, α^p n'est pas pôle de S_1. Donc :

$$v_{\Pi_1} = v.$$

Lemme 3. *Soient A un corps de caractéristique ne divisant pas p et B un sous-corps p-mahlérien de $A(X)$, contenant strictement A. Il existe $e \in \mathbb{Z}$ et $Q \in A[X]$, avec deg $Q >$ e, tels que $B = A(\frac{Q(X)}{X^e})$.*

Preuve :
D'après le théorème de Luroth, il existe $P \in A(X)$ tel que $B = A(P)$. On a $P \notin A$. Supposons *deg* $P \leq 0$: $P = a + P_1$, avec *deg* $P_1 \leq -1$ et $a \in A$. On a encore $B = A(\frac{1}{P_1})$, et *deg* $P_1 \geq 1$. Il n'est donc pas restrictif de supposer : *deg* $P \geq 1$ et, en outre, que P est normalisé.

Puisque $\mu(P) \in B$, il existe $\varphi \in A(Y)$, telle que : $\mu(P) = \varphi(P)$.

On a alors d'après le lemme 1 : *deg* $\varphi(P) =$ *deg* $\varphi \times$ *deg* P.

Comme *deg* $\mu(P) = p$ *deg* P, on obtient : $p =$ *deg* φ.

Plongeons A dans une clôture algébrique K, dans laquelle nous supposerons, par l'absurde, que P admet un pôle différent de 0. Soit α un tel pôle, de multiplicité maximale. On peut écrire :

$$P = (X-\alpha)^{-d} R, \text{ où } R(\alpha) \neq 0, \quad R(\alpha) \neq \infty, \text{ et } d > 0.$$

Si $\varphi(Y) = \frac{\sum_{k=0}^{n} a_k Y^k}{\sum_{k=0}^{m} b_k Y^k}$, avec $n - m = p$, $a_n b_m \neq 0$, on obtient : $\mu(P) = \frac{(X-\alpha)^{-dn}}{(X-\alpha)^{-dm}} R_1$, avec $R_1(\alpha) \neq 0$, $R_1(\alpha) \neq \infty$

Donc, si $\Pi = X - \alpha$:

$$v_\Pi(\mu(P)) = d(m-n) = -dp.$$

D'après le lemme 2, on a :

$$v_{\Pi_1}(P) = -dp, \text{ où } \Pi_1 = X - \alpha^p.$$

Or $dp > d$: ceci est une contradiction.
Finalement, il existe $e \in \mathbb{Z}$, tel que :

$$P(X) = \frac{1}{X^e} Q(X),\ Q \in A[X],\ Q(0) \neq 0,\ deg\ Q > e.$$

Remarquons que la condition $deg\ Q > e$ n'a d'intérêt que si $e \in \mathbb{N}$

Ces lemmes permettent d'alléger la démonstration qui suit, et pour laquelle je suis largement redevable à Richard Antetomaso.

Théorème 2.1. *Soient A un corps de caractéristique ne divisant pas p, B un sous-corps p-mahlérien de $A(X)$. Alors :*
- *ou bien il existe $d \in \mathbb{N}$ tel que $B = A(X^d)$,*
- *ou bien il existe $d \in \mathbb{N}^*$ et $\varepsilon \in A$ tel que $\varepsilon^{p-1} = 1$, tels que $B = A(X^d + \frac{\varepsilon}{X^d})$.*

Preuve :
Nous pouvons supposer que P n'appartient pas à A. Nous appuyant sur le lemme 3, écrivons $B = A(P)$, avec $P(X) = \frac{Q(X)}{X^e}$, $Q \in A[X]$, $Q(0) \neq 0$, et $deg\ Q > e$. On suppose P normalisé.
En particulier, il existe $\varphi \in A(Y)$ telle que : $P(X^p) = \varphi(P(X))$. Posons $\varphi = \frac{N}{D}$, où $N,\ D \in A[Y]$, et où N et D sont premiers entre eux.
Supposons, par l'absurde, que D n'est pas dans A. Soit K une extension algébriquement close de A, et α une racine de D. Alors α n'est pas racine de N.
L'équation $Q(x) - \alpha x^e = 0$ admet dans K une solution non nulle. En effet :

$e > 0 \implies deg[Q(X) - \alpha X^e] \geq 1$ et $Q(0) \neq 0$,

$e \leq 0 \implies deg[X^{-e}Q(X) - \alpha] \geq 1$.

On a donc, si β est une telle solution : $\frac{Q(\beta)}{\beta^e} = P(\beta) = \alpha$. Donc $D(P(\beta)) = D(\alpha) = 0$.
Ceci contredit l'égalité : $P(X^p)D(P(X)) = N(P(X))$.

Il en résulte qu'en réalité φ est un polynôme.

Premier cas : $e \leq 0$.
On peut écrire : $P(X^p) = \varphi(P(X))$, $\varphi \in A[Y]$, $P \in A[X]$. Nous avons vu (lemme précédant la proposition 2.1) que ceci entraîne que $P(X) = X^d + \lambda$, et donc que $A(P) = A(X^d)$.

· Second cas : $e > 0$.

On écrit : $P(X) = \sum_{k=-e}^{d} \lambda_k X^k$, avec $\lambda_d = 1$, $d > 0 > -e$.
Supposons, par l'absurde, qu'il existe $k \in [1, d-1]$ tel que $\lambda_k \neq 0$, et posons :

$$P(X) \equiv X^d + \lambda_q X^q \ mod\ (X^{q-1}), \text{avec } \ q \in [1, d-1],\ \lambda_q \neq 0,$$

$mod\ (X^{q-1})$ désignant ici : $mod\ (Vect(X^j)_{j \leq q-1})$.
On a ainsi : $P(X^p) \equiv X^{pd} + \lambda_q X^{pq}\ mod\ X^{p(q-1)}$.
Par ailleurs, si $\varphi(Y) = a_p Y^p + \cdots + a_0$, on obtient : $\varphi(P(X)) \equiv a_p P(X)^p\ mod\ X^{d(p-1)}$.
Or $d(p-1) \leq p(q-1)$ si et seulement si $p(q-d) \geq p-d$, ce qui est réalisé, puisque $p(q-d) \geq p \geq p-d$.
Donc :

$$X^{pd} + \lambda_q X^{pq} \equiv a_p(X^{pd} + p\lambda_q X^{(p-1)d+q}) \quad mod\ (X^{max(p(q-1),(p-1)d+q-1)}).$$

En particulier, puisque $(p-1)d+q \neq pq$ et $(p-1)d+q-1 \geq p(q-1)$: $a_p = 1$ et $p\lambda_q = 0$.
Ceci est une contradiction.
On a donc : $P(X) = X^d + \lambda_0 + \cdots + \lambda_{-e} X^{-e}$. Le raisonnement précédent, appliqué à $X^d P(\frac{1}{X})$, nous montre que P est de la forme $X^d + \lambda_0 + \varepsilon X^{-e}$, avec $\varepsilon \neq 0$. Il n'est évidemment pas restrictif de supposer que $\lambda_0 = 0$. Dans ces conditions, l'égalité : $P(X^p) = \varphi(P(X))$ s'écrit encore :

$$X^{pd} + \varepsilon X^{-pe} = a_p(X^d + \varepsilon X^{-e})^p + \cdots + a_0.$$

Supposons, par l'absurde, $d \neq e$. Quitte à changer X en $\frac{1}{X}$, on peut supposer $d > e$. On a alors :

$$a_p(X^d + \varepsilon X^{-e})^p + \cdots + a_0 \equiv a_p X^{pd} + a_{p-1} X^{(p-1)d} \quad mod\ (X^{(p-1)d-1}).$$

Donc $a_{p-1} = 0$. Puis :

$$a_p(X^d + \varepsilon X^{-e})^p + a_{p-2}(X^d + \varepsilon X^{-e})^{p-2} + \cdots + a_0 \equiv a_p(X^d + \varepsilon X^{-e})^p \quad mod\ (X^{(p-2)d}).$$

Or $(p-2)d < (p-1)d - e$, puisque $d > e$. On obtient donc :

$$a_p(X^d + \varepsilon X^{-e})^p + \cdots + a_0 \equiv a_p(X^{pd} + p\varepsilon X^{(p-1)d-e}) \quad mod\ (X^{(p-1)d-e-1}).$$

Finalement, $a_p p\varepsilon = 0$. On obtient alors une contradiction (puisque $a_p \neq 0$).

On a, à présent : $P(X) = X^d + \varepsilon X^{-d}$. L'examen des termes de degré pd et $-pd$ dans l'égalité : $P(X^p) = \varphi(P(X))$ nous conduit aux relations : $a_p = 1$; $a_p \varepsilon^p = \varepsilon$, soit : $\varepsilon^{p-1} = 1$.

En résumé : $B = A(X^d + \frac{\varepsilon}{X^d})$, avec $\varepsilon^{p-1} = 1$.

Montrons que, réciproquement, un tel corps est p-malhlérien. Soit, dans K, ω une racine carrée de ε. On a donc : $\omega^2 = \varepsilon \implies \varepsilon = \varepsilon^p = \omega^{2p}$.
Soit $P_1(X) = X + \frac{\varepsilon}{X}$. On a

$$P_1(X^p) = X^p + \frac{\varepsilon}{X^p} = \omega^p[(\frac{X}{\omega})^p + (\frac{\omega}{X})^p] = \omega^p T_p(\frac{X}{\omega} + \frac{\omega}{X}),$$

où $T_p(Y) \in K[Y]$ est défini par : $T_p(Y + \frac{1}{Y}) = Y^p + \frac{1}{Y^p}$ (relation de Tchebychev).

Il vient alors : $P_1(X^p) = \omega^p T_p(\frac{1}{\omega} P_1(X))$.

Cette relation s'écrit encore : $P_1(X^p) = \sum_{j=0}^{p} \alpha_j P_1(X)^j$, $\alpha_j \in K$.

La famille $((P_1(X))^j)_j$ étant échelonnée en degrés, on en déduit qu'en réalité les α_j sont dans A.

Finalement : $P_1(X^p) = \varphi(P_1(X))$, où $\varphi \in A[Y]$. Alors $P_1(X^{pd}) = \varphi(P_1(X^d))$, ce qui permet de conclure, car $P(X) = P_1(X^d)$.

Il reste à vérifier que $A(X^l + \frac{\varepsilon}{X^d})$ ne peut être de la forme $A(X^l)$, $l \in \mathbb{N}^*$. Dans le cas contraire : $X^l = \frac{N(X^d + \frac{\varepsilon}{X^d})}{D(X^d + \frac{\varepsilon}{X^d})}$, avec (lemme 1) : $l = d(deg\ N - deg\ D) = d(\nu - \delta)$.
Posons :

$N(X^d + \frac{\varepsilon}{X^d}) = \frac{1}{X^{d\nu}} N_1(X), \quad N_1(0) \neq 0,$

$D(X^d + \frac{\varepsilon}{X^d}) = \frac{1}{X^{d\delta}} D_1(X), \quad D_1(0) \neq 0.$

Il vient : $X^l = X^{d(\delta-\nu)} \frac{N_1(X)}{D_1(X)}$, soit $X^{2l} = \frac{N_1(X)}{D_1(X)}$. Ceci est une contradiction, puisque $l \in \mathbb{N}^*$.

Corollaire 1. *Sous les hypothèses du théorème 2.1, on suppose que de plus B contient un polynôme non constant. Alors il existe $d \in \mathbb{N}^*$, tel que : $B = A(X^d)$.*

Preuve :
Il suffit de montrer que, si $d \in \mathbb{N}^*$, $A(X^d + \frac{\varepsilon}{X^d})$ ne contient pas de polynôme non constant. Supposons au contraire que Q soit un tel polynôme, appartenant à $A(X^d + \frac{\varepsilon}{X^d})$. Reprenant la fin de la démonstration du théorème 1, on écrit :

$$Q(X) = \frac{N(X^d + \frac{\varepsilon}{X^d})}{D(X^d + \frac{\varepsilon}{X^d})} = X^{d(\delta-\nu)} \frac{N_1(X)}{D_1(X)},$$

avec cette fois : $deg\ Q = d(\nu - \delta)$, $N_1(0) \neq 0$, $D_1(0) \neq 0$.
Donc : $Q(X)X^{deg\ Q} = \frac{N_1(X)}{D_1(X)}$, ce qui est une contradiction.

Corollaire 2. *Soit A un corps de caractéristique ne divisant pas p, et B une sous-algèbre de $A[X]$, p-mahlérienne. Le corps des fractions de B est de la forme $A(X^d)$.*

Preuve :
On remarque que le corps des fractions de B est encore p-mahlérien.

Il faut être bien conscient du fait que ceci ne nous donne en fait que peu de renseignements sur B. Le problème de la détermination de B reste posé. Voici un exemple particulièrement typique. Soit $P \in A[X]$ tel que $P(X)$ divise $P(X^p)$ (cf chapitre 1), et :

$$B = A \oplus A.P \quad .$$

Il est clair que B est une sous-algèbre p-mahlérienne de $A[X]$, dont le corps des fractions contient $\frac{XP}{P} = X$. Ce corps est donc égal à $A(X)$.

Une idée pour étudier B pourrait être de déterminer les idéaux de $A[X]$ inclus dans B.

Définition : Extensions p-mahlériennes. *Soient $A_1 \subset A_2$ deux sous-A-algèbres p-mahlériennes de $A((X))$. On dit alors que A_2 est une extension p-mahlérienne de A_1.*

L'application μ est un endomorphisme de l'anneau A_2, mais pas, en général, de la A_1-algèbre A_2; ce n'en est qu'un semi-endomorphisme.

2. Équations de Mahler linéaires

Définition. *Soit A un anneau commutatif et unitaire, soient B une sous-A-algèbre p-mahlérienne de $A((X))$, et f un élément de $A((X))$. On dit que f vérifie une p-équation linéaire de Mahler sur B s'il existe n dans $\mathbb{N}$, et une famille non nulle $(b_0, \cdots, b_n) \in B^{n+1}$, tels que :*

(3) $$b_n \mu^n(f) + \cdots + b_1 \mu(f) + b_0 f = 0.$$

En d'autres termes, f est annulé par : $b_n\mu^n + \cdots + b_1\mu + b_0 id$, qui est une application A-linéaire. L'ensemble des solutions de (3) forme un A-module, (mais pas un B-module en général).
Le cas où $B = A$ et où A est intègre, est particulièrement simple :

Proposition 2.2. *Soit A un anneau intègre. Si $B = A$, l'ensemble des solutions de (3) est inclus dans A.*

Preuve :
Utilisons la décomposition de A-module :

(*) $$A((X)) = A \oplus XA[[X]] \oplus \tfrac{1}{X}A[\tfrac{1}{X}].$$

Chacun des A-modules est stable par μ. Si donc la décomposition de f sur cette somme directe est :

$$f = a + g + h,$$

chacune des composantes a, g et h vérifie (3). Or, si $g \neq 0$, la famille $(g, \mu(g), \cdots, \mu^n(g))$ est échelonnée en degrés : elle est donc libre sur A. Donc $g = 0$. De même, la famille $(h, \mu(h), \cdots, \mu^n(h))$ est, si $h \neq 0$, échelonnée en valuations. Donc $h = 0$, et $f = a$.

Corollaire. *Sous les hypothèses de la proposition 2, l'ensemble des solutions de (3) est :*

$$\{0\} \quad si \quad \sum_{k=0}^{n} b_k \neq 0,$$

$$A \quad si \quad \sum_{k=0}^{n} b_k = 0.$$

Remarque : La décomposition (*) précédente permet de ramener l'étude d'une équation mahlérienne à la recherche séparée des solutions dans A, dans $\frac{1}{X}A[\frac{1}{X}]$ - c'est à-dire dans $XA[X]$ - et dans $XA[[X]]$.

Étudions à présent le cas où A n'est pas forcément intègre.

Théorème 2.2. *Soit $f \in XA[[X]]$, solution de l'équation (3). Il existe alors $\alpha \in A\backslash\{0\}$ tel que $\alpha f = 0$.*

Preuve :
On raisonne par récurence sur n.

- Si $n = 0$, l'équation se résume à : $b_0 f = 0$, avec $b_0 \neq 0$.
- Supposons donc le résultat vrai pour des équations d'ordre $\leq n - 1$.

  premier cas : $\exists \alpha \in A\backslash\{0\}$ tel que : $b_0\alpha = 0$ et $\exists i \in [1, n]$ $b_i\alpha \neq 0$.

  Multipliant (3) par α, on obtient : $\sum_{i=1}^{n} b_i\alpha\mu^i(f) = 0$.

  Soit $g = \mu(f)$; g vérifie alors une équation de Mahler d'ordre $\leq n - 1$.

  Donc : $\exists \beta \in A\backslash\{0\}$ $\beta g = 0$. Soit $\mu(\beta f) = 0$. Mais μ est injective. Donc $\beta f = 0$.

  deuxième cas : $\forall \alpha \in A\backslash\{0\} : b_0\alpha = 0 \implies \forall i \in [1, n]$ $b_i\alpha = 0$.
  Supposant $f \neq 0$, posons $f(X) = \sum_{k=m}^{\infty} a_k X^k$, avec $a_m \neq 0$.
  On obtient $b_0 a_m = 0$, et donc $b_1 a_m = \cdots = b_n a_m = 0$.
  Posons : $f(X) = a_m X^m + g(X)$. Il vient :
  $\sum_{i=0}^{n} b_i\mu^i(g) = 0$, et donc, de même : $b_0 a_{m+1} = 0$.
  Par une récurrence immédiate, on obtient : $\forall k \geq m$ $b_0 a_k = 0$, et donc : $b_0 f = 0$.

Comme b_0 est nécessairement non nul dans ce cas (prendre $\alpha = 1$), le résultat est démontré.

Remarque : La démonstration précédente, (ou bien un examen direct), prouve que, si b_0 n'est pas diviseur de 0, alors $f = 0$. Autrement dit, dans ce cas, si $g \in A((X))$ est solution de (3), alors $g \in A$.

Exemples.

Exemple 1 : Soit $A = \mathbb{Z}/6\mathbb{Z}$ et $f \in A[[X]]$ solution de

$$3f(X^4) + 2f(X^2) + f(X) = 0.$$

Alors $f \in A$. La réciproque est claire.

Exemple 2 : Soit $A = \mathbb{Z}/6\mathbb{Z}$, et $f \in A[[X]]$, solution de

$$2f(X) + 3f(X^2) = 0.$$

Cette égalité équivaut à $2f(X) = 3f(X^2) = 0$, soit $f = 0$.

La proposition ci-dessous montre que, dans certains cas, on peut sans restriction supposer que A est nœthérien.

Proposition 2.3. *Soit $f \in A((X))$ solution de :*

(3) $\sum_{i=0}^{n} b_i \mu^i(f) = 0$, *où* $(b_0, \cdots, b_n) \in A^{n+1}$.

On suppose que les coefficients de f sont dans un ensemble fini. Il existe alors un sous-anneau A_1 de A, nœthérien, tel que $f \in A_1((X))$, et tel que $\forall i \in [0, n]$, $b_i \in A_1$.

Preuve :
Soit A_2 le sous-anneau de A engendré par 1; A_2 est, soit fini, soit égal à $\mathbb{Z}$. Donc A_2 est un anneau nœthérien. Il suffit de considérer : $A_1 = A_2[b_0, \cdots, b_n, a_0, \cdots, a_k]$, où $\{a_0, \cdots, a_k\}$ est l'ensemble des coefficients de f.

Exemples : La proposition 2.3 s'applique lorsque f est un polynôme, mais aussi lorsque f est la série génératrice d'une suite automatique.

La proposition 2.4, plus technique, permet de préciser la recherche des solutions de l'équation (3).

Proposition 2.4. *Soient A un anneau, $f \in XA[[X]]$ une solution de l'équation (3), avec $f(X) = \sum_{k=1}^{\infty} a_k X^k$.*

(a) On a : $\forall k \in \mathbb{N}^*$, $b_0^k a_k = 0$.

(b) Si A est nœthérien, il existe $m \in \mathbb{N}^*$ tel que $\forall k \in \mathbb{N}^*$, $b_0^m a_k = 0$.

(c) Si f est un polynôme, il existe $q \in \mathbb{N}^*$, tel que $\forall k \in \mathbb{N}^*$, $b_n^q a_k = 0$.

(d) Si f est un polynôme, et si les idéaux (b_0) et (b_n) sont copremiers, alors $f = 0$.

Preuve :

(a) Clairement, $b_0 a_1 = 0$. Supposons le résultat vrai pour $k \leq m-1$. Alors : $\sum_{k=0}^{n} b_0^{m-1} b_k \mu^k(f) = 0$. Le coefficient de X^m dans cette égalité est : $b_0^m a_m$. Il est donc nul.

(b) Soit $I_k = \{x \in A,\ b_0^k x = 0\}$. La suite des idéaux $(I_k)_{k \geq 1}$ est croissante. Elle est donc stationnaire, égale à I_m. Soit : $\forall k \in \mathbb{N}^*$, $I_k \subset I_m$. Or $a_k \in I_k$, d'après (a). Donc $b_0^m a_k = 0$.

(c) Montrons que $b_n^{k+1} a_{d-k} = 0$ par récurrence sur k, où $d = deg(f)$. Le résultat est clair pour $k = 0$. L'admettant jusqu'à l'ordre $m-1$, on a :

$$\sum_{k=0}^{n} b_n^m b_k \mu^k(f) = 0.$$

Le coefficient du terme de plus haut degré est : $b_n^{m+1} a_{d-m}$. Il est donc nul. En particulier, $\forall k \in \mathbb{N}^*$, $b_n^{d+1} a_k = 0$.

(d) Si f est un polynôme, on peut appliquer (c), et (b) d'après la proposition 2.3. Soient $u, v \in A$, tels que : $ub_0 + vb_n = 1$. Alors $a_k = (ub_0 + vb_n)^{m+q-1} a_k = 0$.

Exemples.

Exemple 1 : Soit $A = \mathbb{Z}/10\mathbb{Z}$, et l'équation :

$$3f(X^4) + 3f(X^2) + 2f(X) = 0, \text{ où } f \in XA[[X]].$$

On a $b_0 = 2$. Il existe donc m tel que $2^m f(X) = 0$. Or $2^5 = 2$. Donc $2f(X) = 0$. Il en résulte que :

$$3f(X^4) + 3f(X^2) = 0,$$

soit $f(X^2) = 0$, puisque 3 est inversible. Finalement la seule solution est la solution nulle.

Exemple 2 : Soit $A = \mathbb{Z}/50\mathbb{Z}$, et l'équation :

$$2f(X^4) + 5f(X^2) + 5f(X) = 0, \text{ où } f \in XA[[X]].$$

On obtient $25f(X) = 0$, puis $10f(X^4) = 0$. Soit $10f(X) = 0$. D'où $5f(X) = 0$, et $2f(X^4) = 0$. Finalement $f = 0$.

Exemple 3 : Soit $A = \mathbb{Z}/27\mathbb{Z}$, et l'équation :

$$3f(X^2) + 9f(X) = 0, \quad \text{où } f \in XA[[X]].$$

On obtient de même $9f(X^2) = 0$, donc $9f(X) = 0$, puis $3f(X) = 0$.
Soit : $f(X) = \sum_{n=1}^{\infty} a_n X^n$, avec $a_n \in \{0, 9\}$. L'ensemble des solutions n'est pas un A-module de type fini.

3. Équations de Mahler résolubles à gauche.

Définition. *Sous les hypothèses de la définition donnée au début du paragraphe 2 ci-dessus, l'équation (3) est dite résoluble à gauche si b_n est inversible dans B.*

Remarques :

- De façon générale, quitte à considérer $n' = max\{i \in [0, n], \ b_i \neq 0\}$, on peut toujours supposer que b_n est non nul.
- Si (3) est résoluble à gauche, l'équation est équivalente à une équation de Mahler telle que $b_n = 1$.

Proposition 2.5. *Soit B une sous A-algèbre p-mahlérienne de $A((X))$, et f un élément de $A((X))$. On suppose B nœthérien (comme anneau). Les conditions suivantes sont équivalentes :*

(1) f vérifie une p-équation de Mahler linéaire résoluble à gauche sur B.

(2) le sous B-module de $A((X))$ engendré par $\{\mu^i(f)\}_{i\in\mathbb{N}}$ est de type fini.

(3) il existe un B-module de type fini stable par μ et contenant f.

Preuve :

(1) $\Longrightarrow$ (2) : Posons $\mu^n(f) = -\sum_{i=0}^{n-1} b_i \mu^i(f)$. Par une récurrence immédiate, on constate que :

$$\forall k \geq n, \quad \mu^k(f) \in \sum_{i=0}^{n-1} B.\mu^i(f).$$

Notons, dans la suite, V le sous-B-module de $A((X))$ engendré par $\{\mu^i(f)\}_{i\in\mathbb{N}}$; V n'est donc rien d'autre que $\sum_{i=0}^{n-1} B.\mu^i(f)$. Il est donc de type fini.

(2) $\Longrightarrow$ (3) : Le module V répond à la question.

(3) $\Longrightarrow$ (1) : Soit W un B-module satisfaisant aux conditions. Il contient évidemment V, qui est donc de type fini (c'est le seul moment où le caractère nœthérien de B est utilisé); V admet donc une famille finie de générateurs, qui peut, on le sait, être choisie de la forme $(\mu^i(f))_{i\in I}$. Soit $n = max\ I + 1$. On a évidemment :

$$\mu^n(f) \in \sum_{i\in I} B.\mu^i(f),$$

d'où le résultat.

Notons, à présent, $ML_p(B)$ l'ensemble des éléments f de $A((X))$ qui vérifient une p-équation de Mahler linéaire sur B, résoluble à gauche.

Théorème 2.3. *Soit B une sous-A-algèbre de $A((X))$, p-mahlérienne, et nœthérienne. Alors $ML_p(B)$ est une sous-B-algèbre de $A((X))$, p-mahlérienne.*

Preuve :

(1) Tout d'abord, $B \subset ML_p(B)$. En effet, l'idéal de B engendré par $\{\mu^i(f)\}_{i\in\mathbb{N}}$ est de type fini.

(2) Soient f et g dans $ML_p(B)$, V et W les B-modules engendrés par, respectivement, $\{\mu^i(f)\}_{i\in\mathbb{N}}$ et $\{\mu^i(g)\}_{i\in\mathbb{N}}$, et $(f_i)_{i\in I}$, $(g_j)_{j\in J}$ des familles génératrices finies de V, W. Le B-module $V+W$, engendré par $\{f_i\}_{i\in I}\cup\{g_j\}_{j\in J}$ est de type fini, contient $f+g$, et est stable par μ. De même, pour $\lambda \in B$, $\lambda f \in V$. Soit enfin U engendré par $\{f_i g_j\}_{(i,j)\in I\times J}$. Ce B-module est stable par μ, et contient fg. Donc $fg \in ML_p(B)$.

(3) Si $f \in V$ (avec les notations précédentes), $\mu(f) \in V$. Donc, si $f \in ML_p(B)$, alors $\mu(f) \in ML_p(B)$.

Effectivité.

La recherche d'une équation vérifiée par f sur B se ramène en fait à la recherche d'un système de générateurs d'un B-module, puis de l'expression de $\mu^n(f)$ comme combinaison linéaire de ces générateurs. Un cas simple est celui où A est un corps, $B = A[X]$, et $f \in B$. Il convient alors de chercher le pgcd Δ de $(\mu^i(f))_{i\in\mathbb{N}}$, qui est aussi le pgcd de $(\mu^i(f))_{i\leq n-1}$, et, grâce à l'identité de Bézout, d'écrire :

$$\Delta|\mu^n(f) \implies \mu^n(f)(X) = \Delta(X)Q(X) = \sum_{i=0}^{n-1} u_i(X)Q(X)\mu^i(f).$$

Exemple :

Soit $f = 1+X$; $\Delta = pgcd(1+X, 1+X^2) = 1$, et : $1 = \frac{1}{2}[1+X^2+(1-X)(1+X)]$. On obtient :

$$1+X^4 = \frac{1}{2}(1+X^4)(1+X^2) + \frac{1}{2}(1+X^4)(1-X)(1+X),$$

soit :

$$\mu^2(f) = \frac{1}{2}(1+X^4)\mu(f) + \frac{1}{2}(1+X^4)(1-X)f,$$

(ici, $p=2$).

Ce calcul-ci s'applique plus généralement lorsque A est un anneau (de caractéristique différente de 2).

Pour déterminer la taille d'une équation satisfaite par f, on peut introduire l'ordre (n) de l'équation, et sa hauteur : $h = \max_{0 \leq i \leq n-1} (deg\ b_i)$. Il est clair que l'ordre minimal d'une équation de Mahler résoluble à gauche sur B est, avec les notations précédentes :

$$n = min\{m \in \mathbb{N},\ \ \Delta \in \sum_{i=0}^{m-1} B\mu^i(f)\}.$$

Reste à majorer h.
La démonstration du lemme qui suit est due à Judicael Courant.

Lemme. *Soit $\Delta = pgcd(P_1, \cdots, P_n)$, où $P_i \in A[X]$, $P_i \neq 0$. Il existe $U_1, \cdots, U_n \in A[X]$ tels que :*

$$\sum_{i=1}^{n} U_i P_i = \Delta \ et\ \ \forall i,\ deg\ U_i \leq \max_{i \in [1,n]} (deg\ P_i).$$

Preuve :
Par récurence sur n. Si $n = 1$, c'est évident. Supposons le résultat vrai à l'ordre $(n-1)$, et considérons n polynômes $P_1, \cdots, P_n$ non nuls, avec $deg\ P_1 = \min_{i \in [1,n]} (deg\ P_i)$.

Divisons P_i par P_1 ; $P_i = P_1 Q_i + R_i$, avec $deg\ R_i < deg\ P_1$.
Alors $\Delta = pgcd(P_1, R_2, \cdots, R_n)$.

premier cas : l'un des R_i est nul.

Alors il existe $U_1, \cdots, U_{n-1}$ tels que : $U_1 P_1 + \sum_{i=2}^{n-1} U_i R_i = \Delta$, en supposant $R_n = 0$.
De plus : $deg\ U_i \leq deg\ P_1$, puisque $\forall i \in [2, n-1]$ $deg\ R_i < deg\ P_1$. Il vient alors :

$$(U_1 - \sum_{i=2}^{n-1} U_i Q_i) P_1 + \sum_{i=2}^{n-1} U_i P_i = \Delta.$$

Or : $deg\ Q_i = deg\ P_i - deg\ P_1$. Donc : $deg\ U_i Q_i \leq deg\ P_i \leq max(deg\ P_i)$.
Soit : $deg(U_1 - \sum_{i=2}^{n-1} U_i Q_i) \leq max(deg\ P_i)$.

deuxième cas : les R_i ne sont pas nuls.

Mais : $deg\ P_1 + \sum_{i=2}^{n} deg\ R_i < \sum_{i=1}^{n} deg\ P_i$. Une récurrence sur $\sum_{i=1}^{n} deg\ P_i$ et la méthode précédente permettent de conclure.

Proposition 2.6. *Soit A un corps, $B = A[X]$, $f \in B$, $deg\ f = d$. Si f vérifie une équation de Mahler résoluble à gauche d'ordre n, elle en vérifie une d'ordre n et de hauteur $h \leq 2p^n d$.*

Preuve :
On applique le résultat précédent à $P_i = \mu^i(f)$, $i = 0, \cdots, n-1$. Multipliant Δ par $\frac{P_n}{\Delta}$, on obtient :

$$P_n = \sum_{i=0}^{n-1} (U_i \frac{P_n}{\Delta}) P_i, \text{ et } deg(U_i \frac{P_n}{\Delta}) \leq (p^n + p^{n-1})d \leq 2p^n d.$$

Cas d'un corps fini de caractéristique p.

Soit $A = \mathbb{F}_{p^k}$ le corps à p^k éléments, où p est un nombre premier. Nous savons alors que, pour tout x dans A, $x^{p^k} = x$. Il en résulte que, si $f \in \mathbb{F}_{p^k}((X))$:

$$f^{p^k} = (\sum_{-\infty}^{+\infty} a_n X^n)^{p^k} = \sum_{-\infty}^{+\infty} a_n (X^{p^k})^n = f(X^{p^k}) = \mu^k(f).$$

Remarquons en outre le résultat général suivant :

Proposition 2.7. *Soit A un anneau, B une sous-A-algèbre p-mahlérienne et nœthérienne de $A((X))$. Alors, pour tout k dans $\mathbb{N}^*$, on a :*

$$ML_p(B) = ML_{p^k}(B).$$

Preuve :

(1) Soit $f \in ML_p(B)$. Le B-module engendré par $\{\mu^i(f)\}_{i\in\mathbb{N}}$ est de type fini et contient le B-module engendré par $\{\mu^{ki}(f)\}_{i\in\mathbb{N}}$. La proposition 2.5 conclut.

(2) Soit $f \in ML_{p^k}(B)$. Une p^k-équation résoluble à gauche vérifiée par f est du type :

$$\mu^{kn}(f) + \sum_{i=0}^{n-1} b_i \mu^{ki}(f) = 0,$$

avec $b_i \in B$. C'est aussi une p-équation de Mahler résoluble à gauche.

Ceci nous permet de décrire $ML_p(B)$, lorsque B est une sous-$\mathbb{F}_{p^k}$-algèbre de $\mathbb{F}_{p^k}((X))$.

Proposition 2.8. *Soit B une sous-$\mathbb{F}_{p^k}$-algèbre p-mahlérienne et nœthérienne de $\mathbb{F}_{p^k}((X))$; $ML_p(B)$ coïncide alors avec l'anneau des séries formelles entières (algébriques) sur B.*

Preuve :

(1) Soit $f \in ML_p(B)$. Puisque $f \in ML_{p^k}(B)$, on peut écrire :

$$\mu^{kn}(f) + \sum_{i=0}^{n-1} b_i \mu^{ki}(f) = 0, \quad b_i \in B.$$

Soit encore :

$$f^{p^{kn}} + \sum_{i=0}^{n-1} b_i f^{p^{ki}} = 0.$$

(2) Soit f entière sur B. Le B-module engendré par $\{f^i\}_{i\in\mathbb{N}}$ est de type fini, et contient le B-module engendré par $\{f^{p^{kj}}\}_{j\in\mathbb{N}}$, c'est-à-dire par $\{\mu^{kj}(f)\}_{j\in\mathbb{N}}$. Il en résulte que $f \in ML_{p^k}(B)$, et donc $f \in ML_p(B)$.

On constate, dans ce cas, que les éléments de $ML_p(B)$ sont algébriques sur B, et que, d'autre part, on connaît les inversibles de $ML_p(B)$. Les questions se posent évidemment dans le cas général : un élément de $ML_p(B)$ peut-il être algébrique sur B ? Quels sont les éléments inversibles de $ML_p(B)$?

4. Équations de Mahler résolubles à droite.

Définition. *Sous les hypothèses de la définition donnée au début du deuxième paragraphe, l'équation (3) est dite résoluble à droite si b_0 est inversible dans B.*

Constatons tout d'abord qu'il n'est pas certain, une équation de Mahler sur B pour f étant donnée, d'en déduire que f vérifie une équation de Mahler avec $b_0 \neq 0$. Néanmoins :

Proposition 2.9. *Soit A un anneau intègre de caractéristique ne divisant pas p, et B l'anneau $A[X]$. Si f vérifie une p-équation de Mahler linéaire sur B, alors f vérifie une p-équation de Mahler linéaire sur B, avec $b_0 \neq 0$.*

Preuve :
Soit $\sum_{i=0}^{n} c_i\mu^i(f) = 0$ une équation de Mahler vérifiée par f sur B. Supposons $c_0 = 0$, et montrons que f vérifie une équation d'ordre $(n-1)$, ce qui assurera le résultat.

Plongeons A dans un corps K algébriquement clos. Puisque *car* K ne divise pas p, l'équation : $z^p - 1 = 0$ admet dans K p solutions distinctes, formant l'ensemble U_p. On a :

$$\sum_{i=1}^{n} c_i(X) f(X^{p^i}) = 0,$$

et donc :

$$\forall \omega \in U_p \quad \sum_{i=1}^{n} c_i(\omega X) f(X^{p^i}) = 0.$$

Posons :

$$\sum_{\omega\in U_p} c_i(\omega X) = d_i(X^p), \quad \text{où} \quad d_i \in A[X].$$

S'il existe $i \in [1,n]$ tel que $d_i \neq 0$, on a :

$$\mu(\sum_{i=1}^{n} d_i \mu^{i-1}(f)) = 0.$$

et, d'après l'injectivité de μ, le résultat est atteint.
Sinon, on a :

$$\forall i \in [1,n], \quad \sum_{\omega \in U_p} c_i(\omega X) = 0.$$

En particulier, le terme constant de c_i est nul. Or on peut toujours supposer que ce n'est pas le cas pour l'un des c_i, en divisant au préalable l'équation par X^j, avec : $j = \min_{i \in [1,n]} val(c_i)$.

Remarque : Le résultat ne s'étend pas à une sous-algèbre p-mahlérienne quelconque de $A[X]$. Soit par exemple : $f = 1 - X$, $p = 2$. On a : $(1+X)f(X) - f(X^2) = 0$, et donc : $(1+X^2)f(X^2) - f(X^4) = 0$.
Donc f vérifie une 2-équation de Mahler sur $A[X^2]$. Si f vérifiait une équation sur $A[X^2]$ telle que b_0 soit non nul, f serait un élément de $A(X^2)$, ce qui n'est pas.

Corollaire. *Soit A un corps de caractéristique ne divisant pas p, et $B = A(X)$. Pour $f \in A((X))$, il y a équivalence entre :*

(1) f vérifie une p-équation linéaire de Mahler résoluble à droite sur B.

(2) f vérifie une p-équation linéaire de Mahler résoluble à gauche sur B.

(3) f vérifie une p-équation linéaire de Mahler sur B.

Preuve :
Il suffit de constater que l'inversibilité d'un élément de B équivaut à sa non nullité, et d'appliquer la proposition 2.9.

Pour mettre en valeur la nuance entre la résolubilité à gauche et la résolubilité à droite, nous allons étudier le cas particulier où A est un corps, et où $B = A[X]$. Nous savons dans ce cas (théorème 2.3) que tout f de B vérifie une p-équation de Mahler linéaire sur B résoluble à gauche. Nous allons donc étudier, toujours pour $f \in B$, l'éventualité d'être solution d'une équation résoluble à droite.

Lemme 1. *Soit A un corps, $B = A[X]$, et $f \in B$. Il y a équivalence entre les propriétés suivantes :*

(1) f vérifie une p-équation de Mahler linéaire résoluble à droite sur B.

(2) $pgcd(\mu^i(f))_{i \in \mathbb{N}} = 1$.

Preuve :

(1) $\Longrightarrow$ (2) : Notons Δ ce pgcd : $\Delta = pgcd(\mu^i(f))_{i\in[0,n]}$.

On peut écrire :

(4) $$f + \sum_{i=1}^{n} b_i \mu^i(f) = 0,$$

quitte à ajouter des termes nuls dans l'équation de Mahler, ou au contraire à remarquer que, si l'ordre m de l'équation vérifiée par f est plus grand que n, $\Delta = pgcd(\mu^i(f))_{i\in[0,m]}$.

Notons $\delta = pgcd(\mu^i(f))_{i\in[1,n]}$. On a donc : $\Delta = pgcd(f, \delta)$. Grâce à (4), on voit que $\delta | f$. Donc $\Delta = \delta$.

Mais $\mu(\Delta)$ divise $\mu^i(f)$, pour $i \in [1, n]$ - puisque Δ divise $\mu^i(f)$ pour $i \in [0, n-1]$ - donc $\mu(\Delta)$ divise Δ.

Comme $deg\ \mu(\Delta) = p\ deg\ \Delta$, il est alors clair que $deg\ \Delta = 0$.

(2) $\Longrightarrow$ (1) est évident.

Lemme 2. *Soit A un corps, $B = A[X]$, et $f \in B\backslash\{0\}$. Les propriétés suivantes sont équivalentes :*

(1) $pgcd(\mu^i(f))_{i\in\mathbb{N}} \neq 1$.

(2) Soit K une clôture algébrique de A. Il existe dans K un élément ω nul ou racine de l'unité tel que :

$$\forall i \in \mathbb{N}, \quad f(\omega^{p^i}) = 0.$$

Preuve :

(1) $\Longrightarrow$ (2) : Soit ω une racine commune (dans K) aux $\mu^i(f)$. Supposons $\omega \neq 0$. On a :

$$\forall i \in \mathbb{N}, \quad f(\omega^{p^i}) = 0.$$

En outre, l'ensemble des racines de f est fini. Il existe donc $j > i$ tels que : $\omega^{n^j} = \omega^{p^i}$. D'où : $\omega^{p^j - p^i} = 1$.

(2) $\Longrightarrow$ (1) : Le résultat est clair.

Proposition 2.10. *Soit A un corps, $B = A[X]$, $f \in B\backslash\{0\}$, p un nombre premier. Il y a équivalence entre*

(1) f vérifie une p-équation de Mahler résoluble à droite sur B.

(2) $f(0) \neq 0$; de plus, soit ω un élément d'une clôture algébrique de A, racine de l'unité, d'ordre s. Posons $s = p^l q$, où $pgcd(p, q) = 1$. Soit j l'ordre de p dans $((\mathbb{Z}/q\mathbb{Z})^*, \times)$. Alors f n'est pas divisible par : $\prod_{0\leq i\leq l+j-1}(X - \omega^{p^i})$.

Preuve :

Soit K la clôture algébrique de A. La conjonction des lemmes 1 et 2 montre que tout revient à établir l'équivalence entre (avec les notations de la proposition 10) :

(1) $\forall i \in \mathbb{N}, \quad f(\omega^{p^i}) = 0.$

(2) f est divisible (dans $K[X]$) par $\prod_{0\leq i\leq l+j-1}(X-\omega^{p^i})$.

Remarquons tout d'abord que, p étant inversible dans $\mathbb{Z}/q\mathbb{Z}$, j est bien défini. Considérons les éléments $\omega, \omega^p, \cdots, \omega^{p^{l+j-1}}$.
Ils sont distincts. Soient en effet i, k tels que : $0 \leq i < k \leq l+j-1$.
Si $\omega^{p^k} = \omega^{p^i}$, alors $\omega^{p^k-p^i} = 1$, donc $s|p^i(p^{k-i}-1)$.
On a donc : $i \geq l$ et $p^{k-i} \equiv 1\ (mod\ q)$. Donc $i \geq l$ et $j|k-i \implies k \geq l+j$.
De plus, soit $n \geq l+j$. L'intervalle $[l, l+j-1]$ est de longueur j. Il contient donc un élément i de la progression arithmétique $\{n-kj\}_{k\in\mathbb{Z}}$.
De plus, $n-kj \leq l+j-1 \implies kj \geq 1$. Donc $k > 0$. On a donc $n-kj = i$, soit : $p^n = p^i p^{kj}$.
Or $p^{kj} \equiv 1\ mod\ q \implies p^n \equiv p^i\ mod\ (p^i q)$. Comme $i \geq l$, s divise $p^i q$ et donc $\omega^{p^n} = \omega^{p^i}$.
En d'autres termes, $\{\omega^{p^n}\}_{n\geq l+j} \subset \{\omega^{p^m}\}_{m\leq l+j-1}$ et finalement :

$$(1) \text{ équivaut à : } \quad \forall i \in [0, l+j-1]\ f(\omega^{p^i}) = 0,$$

avec des ω^{p^i} distincts dans le second cas. La propriété précédente équivaut à :

$$\prod_{0\leq i\leq l+j-1} (X-\omega^{p^i}) \text{ divise } f.$$

Exemples.

Exemple 1 : Le polynôme $X-1$ ne vérifie pas d'équation de Mahler résoluble à droite (A, p sont quelconques).

Exemple 2 : Si $p=2$ et $A=\mathbb{Q}$, le polynôme X^2+X+1 ne vérifie pas d'équation de Mahler résoluble à droite sur A (prendre $\omega = \frac{-1+i\sqrt{3}}{2}, l=0, j=1$).

Exemple 3 : Si $A=\mathbb{Q}$, X^2-2 vérifie une p-équation de Mahler sur $\mathbb{Q}$, résoluble à droite. Il suffit ici de constater que X^2-2 et $X^{2p}-2$ sont premiers entre eux, et ce quel que soit p.

Illustration 1 : Soit $A=\mathbb{F}_{p^k}$, où p est un nombre premier, et $f \in A[X]$, non constant. Il est évident, sans avoir recours à la proposition 2.10, que f ne vérifie pas de p^k-équation de Mahler résoluble à droite sur $A[X]$. Une égalité :

$$f(X) = \sum_{i=1}^{n} b_i(X) f(X^{p^{ki}}), \quad b_i \in A[X]$$

s'écrit en effet :

$$f(X) = \sum_{i=1}^{n} b_i(X) f(X)^{p^{ki}},$$

puisque, si g est dans $A[X]$, $[g(X)]^{p^k} = g(X^{p^k})$.
Or, après division par $f(X)$, on aboutit à une contradiction évidente.

Étudions maintenant la situation où $A = \mathbb{F}_{p^k}$, p étant toujours premier, et où f est dans $A[X]$, irréductible (non constant), différent de X.
On suppose que f ne vérifie pas de p-équation de Mahler résoluble à droite sur $A[X]$. Soit ω une racine de f dans $\mathbb{F}_{p^{kd}}$, où d est le degré de f. Son ordre s est premier avec p. Soit j l'ordre de p dans $((\mathbb{Z}/s\mathbb{Z})^*, \times)$.

Examinons d'abord le cas où : $j = 1$. Alors $p \equiv 1 \ mod\ s$, donc $\omega^{p-1} = 1$. Autrement dit ω est dans $\mathbb{F}_p$, et : $f = X - \omega$.
L'étude initiale prouve que, réciproquement, un tel polynôme ne vérifie pas de p-équation de Mahler résoluble à droite sur $A[X]$.

Supposons à présent : $j \geq 2$. Dans ce cas, ω^p est racine de f. On sait que les conjugués de ω sont $\omega, \omega^{p^k}, \omega^{p^{2k}}, \cdots, \omega^{p^{(d-1)k}}$, donc il existe un entier l tel que : $\omega^p = \omega^{p^{lk}}$.
D'où : $s|p^{lk} - p$, ou encore : $s|p^{lk-1} - 1$. Soit : $p^{lk-1} \equiv 1 \ mod\ s$, donc $j|lk - 1$, c'est-à dire $lk \equiv 1 \ mod\ j$, ce qui implique $pgcd(k, j) = 1$.

Si, réciproquement, $pgcd(k, j) = 1$, alors j divise un entier de la forme $lk - 1$, donc aussi un entier de la forme $lk_i - i$. Il en résulte que s divise $p^{lk_i} - p_i$, et donc que :

$$\forall i \in [0, j-1] \quad \omega^{p^i} = \omega^{p^{lk_i}}.$$

Donc $\prod_{0 \leq i \leq j-1}(X - \omega^{p^i})$ divise f.

En résumé, en regroupant les deux cas : *f irréductible ne vérifie pas d'équation de Mahler résoluble à droite sur $A[X]$ si, et seulement si : $pgcd(k, j) = 1$.*

Illustration 2 : Soit $A = \mathbb{Q}$, cherchons, toujours avec les notations de la proposition 2.10, une condition équivalente à la condition (2). Si $\omega \in \mathbb{C}^*$, et ω est d'ordre s, le polynôme minimal de ω sur $\mathbb{Q}$ est Φ_s, polynôme cyclotomique d'ordre s. Lorsque $f \in \mathbb{Q}[X]$, f est divisible par $X - \omega$ si, et seulement si, f est divisible par Φ_s. Par ailleurs, si $i \in [0, l]$, l'ordre de ω^{p^i} est $\frac{s}{p^i}$, et si $i \in [l+1, l+j-1]$, l'ordre de ω^{p^i} est $\frac{s}{p^l}$. Il en résulte que f est divisible par $\prod_{0 \leq i \leq l+j-1}(X - \omega^{p^i})$ si, et seulement si, f est divisible par $\prod_{i=0}^{l} \Phi_{\frac{s}{p^i}}$.
En d'autres termes :

Corollaire. *Soit p un nombre premier, $f \in \mathbb{Q}[X]$, telle que $f(0) \neq 0$; f vérifie une p-équation de Mahler linéaire résoluble à droite sur $\mathbb{Q}[X]$ si, et seulement si, pour tout q premier avec p et pour tout $l \in \mathbb{N}$, le polynôme $\prod_{i=0}^{l} \Phi_{p^i q}$ ne divise pas f.*

5. Résolution d'une équation de Mahler résoluble à droite

Soit B une algèbre p-mahlérienne, et l'équation :

$$f = \sum_{i=1}^{n} b_i \mu^i(f), \quad (b_1, \cdots, b_n) \in B^n. \tag{5}$$

Introduisons la matrice $F \in M_{n,1}(A((X)))$:

$$F = \begin{pmatrix} f \\ \mu(f) \\ \cdots \\ \mu^{n-1}(f) \end{pmatrix}; \quad \text{alors : } \mu(F) = \begin{pmatrix} \mu(f) \\ \mu^2(f) \\ \cdots \\ \mu^n(f) \end{pmatrix},$$

(μ s'étend immédiatement aux matrices à éléments dans $A((X))$).

Soit $M = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & 0 \end{pmatrix} \in M_n(B)$.

Il est alors clair que f vérifie (5) si, et seulement si, F vérifie l'équation matricielle :

$$F = M.\mu(F).$$

Nous introduisons donc de façon générale, pour $M \in M_n(B)$, l'équation à l'inconnue $F \in M_{n,1}(A((X)))$:

(6) $$F = M.\mu(F).$$

Dans la suite, $A((X))$ est muni de sa topologie canonique, qui induit sur A la topologie discrète.

Notation. *Le produit matriciel $A_1 A_2 \cdots A_q$ est noté $\prod_{i=1}^{q} A_i$.*

Lemme 1. *Soient $M \in M_n(A[[X]])$, et $F \in M_{n,1}(A[[X]])$ vérifiant : $F = M\mu(F)$. Alors $F(0) = M(0)F(0)$.*

Preuve : Immédiate.

Lemme 2. *Soient $F_0 \in M_{n,1}(A)$, $M \in M_n(A[[X]])$. On suppose : $F_0 = M(0)F_0$. Alors la suite de terme général $\prod_{i=0}^{k-1} \mu^i(M)F_0$ converge vers un élément F de $M_{n,1}(A[[X]])$ tel que $F(0) = F_0$.*

Preuve : Posons $M_k = \prod_{i=0}^{k-1} \mu^i(M)$, et écrivons : $M = M(0) + XP$, où P appartient à $M_n(A[[X]])$. Alors : $\mu^k(M) = M(0) + X^{p^k}\mu^k(P)$, et donc :

$$M_{k+1} = M_k\mu^k(M) = M_kM(0) + X^{p^k}M_k\mu^k(P).$$

Donc

$$M_{k+1}F_0 = M_kM(0)F_0 + X^{p^k}M_k\mu^k(P)F_0,$$

et par conséquent :

$$val(M_{k+1}F_0 - M_kF_0) \geq p^k.$$

Il en résulte que $(M_kF_0)_{k\geq 0}$ converge vers un élément F de $M_{n,1}(A[[X]])$.
De plus : $F(0) = \lim_{k\to+\infty} M(0)^kF_0 = F_0$.

Proposition 2.11. *Soit $M \in M_n(A[[X]])$. L'ensemble des solutions $F \in M_{n,1}(A[[X]])$ de l'équation :*

(6) $$F = M\mu(F)$$

est isomorphe par $F \mapsto F(0)$ au A-module des éléments F_0 de $M_{n,1}(A)$ vérifiant la condition : $M(0)F_0 = F_0$.

Preuve : Si F est solution de (6), $F(0)$ vérifie $M(0)F(0) = F(0)$ d'après le lemme 1. D'après le lemme 2, si $M(0)F_0 = F_0$, il existe F tel que $M\mu(F) = F$, et $F(0) = F_0$. De plus un tel F est unique. En effet, si $F(0) = 0$, on a nécessairement :

$$\forall k, \quad F = \prod_{i=0}^{k-1} \mu^i(M)\mu^k(F),$$

et donc $\forall k \in \mathbb{N}, \quad val\ F \geq p^k$. Donc $F = 0$.

Étude du cas général.

Revenons à l'équation (6), et posons $M = X^\alpha N$, avec $val\ N = 0$, $\alpha \in \mathbb{Z}$. Cherchons les solutions F de (6) de valuation v : $F = X^v G$, avec $val\ G = 0$.

On pose $G = \sum_{i=0}^{+\infty} G_i X^i$, $G_0 \neq 0$; $N = \sum_{i=0}^{+\infty} N_i X^i$, $N_0 \neq 0$.

L'équation (6), qui s'écrit :

(7) $$G = X^{\alpha+(p-1)v} N\mu(G),$$

devient, en posant $-m = \alpha + (p-1)v$:

$$\sum_{i=0}^{+\infty} G_i X^i = X^{-m} \sum_{i=0}^{+\infty} \Big(\sum_{j+pk=i} N_j G_k \Big) X^i = \sum_{i=-m}^{+\infty} \Big(\sum_{j+pk=m+i} N_j G_k \Big) X^i.$$

On peut supposer $m > 0$, le cas $m \leq 0$ relevant de la proposition 2.11. Une condition nécessaire est la suivante :

$$\forall i \in [-m, -1], \quad 0 = \sum_{j+pk=m+i} N_j G_k,$$

$$\forall i \geq 0, \qquad G_i = \sum_{j+pk=m+i} N_j G_k.$$

Étudions une réciproque, en supposant que $(G_i)_{i\geq 0}$ est une famille d'éléments de $M_{n,1}(A)$ telle que les relations précédentes soient vérifiées. Si l'on pose :

$$G(X) = \sum_{i=0}^{+\infty} G_i X^i,$$

on a :

$$\begin{aligned} G(X) &= \sum_{i=-m}^{+\infty} \Big(\sum_{j+pk=m+i} N_j G_k \Big) X^i \\ &= X^{-m} \sum_{i=0}^{+\infty} \Big(\sum_{j+pk=i} N_j G_k \Big) X^i \\ &= X^{-m} N(X) G(X^p). \end{aligned}$$

Si donc $F(X) = X^v G(X)$, on a :

$$F(X) = M(X) F(X^p).$$

De plus, si $G_0 \neq 0$, on a bien $val\ (F) = v$.
En résumé :

Proposition 2.12.

Soient A un anneau, B une algèbre p-mahlérienne sur A, $M = X^\alpha(\sum_{i=0}^{+\infty} N_i X^i)$ un élément de $M_n(B)$, où $N_i \in M_n(A)$, et

$$F = M_{/l}(F). \tag{6}$$

une équation matricielle linéaire résoluble à droite, à l'inconnue matricielle :
$F \in M_{n,1}(A((X)))$, de valuation $v \in \mathbb{Z}$.
On pose : $-m = \alpha + (p-1)v$, et l'on note : $F = X^v(\sum_{i=0}^{+\infty} G_i X^i)$. On suppose $m > 0$.

a) Si F est solution de (6), on a nécessairement :

$$\begin{aligned} \forall i \in [-m, -1], \quad 0 &= \sum_{j+pk=m+i} N_j G_k, \\ \forall i \geq 0, \qquad\quad G_i &= \sum_{j+pk=m+i} N_j G_k. \end{aligned}$$

b) Soit réciproquement $G_0 \in M_{n,1}(A)$. On suppose qu'il existe $(G_i)_{i\geq 0}$ une famille de vecteurs de $M_{n,1}(A)$ telle que :

$$\begin{aligned} \forall i \in [-m, -1], \quad 0 &= \sum_{j+pk=m+i} N_j G_k, \\ \forall i \geq 0, \qquad\quad G_i &= \sum_{j+pk=m+i} N_j G_k. \end{aligned}$$

Alors F est solution de (6).

Donnons quelques applications des résultats qui précèdent.

Corollaire 1. *Sous les hypothèses de la proposition 2.11, si A est un anneau nœthérien, l'ensemble des solutions de (6) est de type fini.*

Preuve : A^n est de type fini.

Corollaire 2. *Sous les hypothèses de la proposition 2.11, si A est principal, l'ensemble des solutions de (6) est libre de type fini.*

Corollaire 3. *Sous les hypothèses de la proposition 2.11, si A est un corps, l'ensemble des solutions de (6) est de dimension $n - rg(M(0) - I)$.*

Corollaire 4. *L'ensemble des solutions de (5) est un A-module isomorphe à l'idéal :*

$$\{x \in A;\ (\sum_{i=1}^{n} b_i(0) - 1)x = 0\}.$$

En particulier, si A est intègre, (5) admet une solution non nulle si, et seulement si, $\sum_{i=1}^{n} b_i(0) = 1$. L'ensemble des solutions de (5) est donc isomorphe à A par : $f \mapsto f(0)$.

Preuve :
La résolution de $M(0)F_0 = F_0$ conduit, si

$$F_0 = \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{bmatrix},$$

à :

$$(\sum_{i=1}^{n} b_i(0) - 1)x_1 = 0;\ x_1 = x_2 = \cdots = x_n.$$

De plus, $x_1 = f(0)$. L'ensemble des résultats découle de ces remarques.

Corollaire 5. *On se place sous les hypothèses de la proposition 2.12, et l'on suppose A intègre.*
Si (6) admet une solution non nulle, aucune des matrices N_r, pour $r \in [0, min(m-1, p-1)]$, n'est de rang n.
En particulier, si N_0 est de rang n, l'équation (6) n'admet de solution non nulle F que parmi les séries formelles de valuation : $\frac{\alpha}{1-p}$. Si donc $p-1$ ne divise pas α, et si N_0 est de rang n, l'équation (6) n'admet d'autre solution que 0.

Preuve :
Soit $q = min(m-1, p-1)$. On suppose que l'une des matrices $N_0, \cdots, N_q$ est de rang n. Or, en faisant $i = q - m$, on obtient les égalités :

$$N_0 G_0 = N_1 G_0 = \cdots = N_q G_0 = 0.$$

Donc $G_0 = 0$, ce qui est une contradiction.

Le cas particulier où N_0 est de rang n prouve que, si F est solution non nulle de (6), on ne peut avoir $q \geq 0$. Donc $m \leq 0$. Mais si $m < 0$, la proposition 2.11 nous montre que G, donc F est nulle. Donc $m = 0$ et $v = \frac{\alpha}{1-p}$.

Exemples.

Exemple 1 : $f(X) = Xf(X^2) + (1+X)f(X^4)$, $(p = 2)$.

$$M = \begin{pmatrix} X & 1+X \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} X.$$

Ici, $N_0 G_0 = 0 \implies G_0 = 0$. Les solutions sont de valuation nulle, puisque $m = 0$, et $\alpha = 0$.
Puisque : $M(0)F(0) = F(0)$ si et seulement si $F(0) = \begin{pmatrix} \lambda \\ -\lambda \end{pmatrix}$, l'ensemble des solutions est isomorphe à A.
Une solution est : $\lim_{k \to +\infty} \left(\prod_{i=0}^{k-1} \begin{pmatrix} X^{2^i} & 1+X^{2^i} \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right)$.

Exemple 2 : $f(X) = \frac{1}{X} f(X^p) + (1 + \frac{1}{X}) f(X^{p^2})$, p quelconque.
Ici, $\alpha = -1$, $M = \frac{1}{X} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
Puisque N_1 est de rang 1, on a $min(m-1, p-1) \leq 0$. Donc $m \leq 1$.

Premier cas $m = 1$. Alors $v = 0$.
Les conditions du théorème 2.4 s'écrivent : $0 = N_0 G_0$; $G_0 = N_1 G_0$, d'où $G_0 = 0$. Ce cas est à exclure.

Deuxième cas $m = 0$. Alors $(p-1)v = 1$.
Si $p \neq 2$, il n'y a pas de solution. Si $p = 2$, $v = 1$. Les conditions de la proposition 2.12 s'écrivent : $G_0 = N_0 G_0$, soit $G_0 = \begin{pmatrix} \lambda \\ -\lambda \end{pmatrix}$.
On obtient : $G = \lim_{k \to +\infty} \left(\prod_{i=0}^{k-1} \begin{pmatrix} 1 & 1+X^{2^i} \\ X^{2^i} & 0 \end{pmatrix} \begin{pmatrix} \lambda \\ -\lambda \end{pmatrix} \right)$, puis $F = XG$.

chapitre 3.

La notion de suite p-régulière, introduite par J.P. Allouche et J. Shallit dans [1] , est destinée explicitement à généraliser celle de suite p-automatique ; une suite automatique présente en effet le défaut de prendre ses valeurs dans un ensemble nécessairement fini.

Généraliser aux suites p-régulières des résultats connus ou conjecturés concernant les suites p-automatiques est l'un des objectifs de ce travail. Dans ce chapitre, nous établissons un certain nombre de résultats élémentaires relatifs aux suites p-régulières. Le théorème 3.1 permet de caractériser matriciellement les suites p-régulières, à l'aide de leurs séries génératrices. Grâce à cette caractérisation, nous retrouvons un certain nombre de résultats établis dans [1].

Dans le cadre de ce travail, il serait de bon ton de caractériser les séries précédentes par l'équation de Mahler minimale qu'elles vérifient, notion introduite formellement dans le paragraphe 2. Les travaux de P. Dumas [2] à ce sujet vont dans cette direction.

A ce stade, nous disposerons de plusieurs sous-algèbres p-mahlériennes de $A((X))$: $ML_p(A[X])$,$ML_p(A(X))$(ch.2), et à présent $\mathfrak{R}(A[X])$. Elucider leurs rapports permettrait de préciser le statut des séries génératrices de suites p-régulières.

D'autre part, le rapport entre les équations de Mahler homographiques, brièvement étudiées dans ce chapitre (proposition 3.4), et les équations de Mahler linéaires d'ordre deux, est patent : il est évoqué dans un cadre formel.

1. Suites *p*-régulières et équations matricielles.

Dans ce paragraphe, A désigne un anneau noethérien et A_1 un anneau contenant A comme sous-anneau.

Soit u une suite, élément de $A_1^{\mathbb{N}}$. On considère alors les suites ci-dessous :

$n \longmapsto u(n)$;

$n \longmapsto u(pn)$; $n \longmapsto u(pn+1)$;.....; $n \longmapsto u(pn+p-1)$;

$n \longmapsto u\left(p^2n\right)$; $n \longmapsto u\left(p^2n+1\right)$;.....; $n \longmapsto u\left(p^2n+p^2-1\right)$;

.....

De façon générale, soit k dans $\mathbb{N}$, et r un entier de $\left[0,\ p^k-1\right]$. Posons :

$$\phi_{k,r}(n) = p^kn+r.$$

Le p-noyau de la suite u est l'ensemble des suites $u \circ \phi_{k,r}$, lorsque k décrit $\mathbb{N}$ et r décrit $\left[0,\ p^k-1\right]$. Notons le calcul immédiat suivant :

$$\phi_{k,r} \circ \phi_{k',r'} = \phi_{k+k',\ p^kr'+r}, \quad \text{et : } 0 \le p^kr'+r \le p^{k+k'}-1.$$

Par définition, la suite u est dite p-régulière sur A lorsque le A-module engendré par le p-noyau de u est de type fini.

Etant donnée une suite u de $A_1^{\mathbb{N}}$, on lui associe l'élément f de $A_1[[X]]$ défini par :

$$f(X) = \sum_{k\in\mathbb{N}} u(k)\ X^k.$$

Il s'agit donc de la série génératrice de la suite u.

Par ailleurs, l'opérateur μ_p , de Mahler, s'étend de manière naturelle aux tableaux d'éléments de A((X)). On note toujours μ_p , ou plus rapidement μ , les applications ainsi définies ; en particulier, μ_p est un endomorphisme de la A-algèbre $M_{q,q}(A((X)))$.

Le A-module $M_{q,r}(A((X)))$ sera parfois identifié au A-module $M_{q,r}(A)(X)$.

Théorème 3.1.

Soit u une suite de $A_1^{\mathbb{N}}$. Les propriétés suivantes sont équivalentes :

(1 u est p-régulière sur A ;

(2)il existe un entier naturel m, un vecteur colonne F de $M_{m,1}\left(A_1[[X]]\right)$, de première composante égale à f, et une matrice S dans $M_{m,m}(A[X])$, tels que :

$$F = S\ \mu_p(F);$$

(3)il existe un entier naturel q, un vecteur colonne G dans $M_{q,1}\left(A_1[[X]]\right)$, de première composante égale à f, et une matrice T de $M_{q,q}(A[X])$, de degré inférieur ou égal à p-1, tels que :

$$G = T\ \mu_p(G).$$

Preuve.

$\therefore$ (1) $\Longrightarrow$ (2)

Soit $\left(u_1,\ldots,u_m\right)$ une famille génératrice du A-module engendré par le p-noyau de u, telle qu'en outre u_1 soit égale à u. Soit k un entier de [0,p-1]. On a :

$$\forall\ i \in [1,m]\quad u_i(pn+k) = \sum_{j=1}^{m} \alpha_{i,j,k}\ u_j(n)\ ,$$

où les $\alpha_{i,j,k}$ sont dans A.

Posons alors:

$$U(n) = \begin{bmatrix} u_1(n) \\ \vdots \\ u_m(n) \end{bmatrix} \quad ; \quad U(n) \in M_{m,1}\left(A_1\right)$$

$$\text{et } S_k = \left[\alpha_{i,j,k}\right]_{1\le i\le m,\,1\le j\le m} \quad ; \quad S_k \in M_{m,m}(A).$$

On peut écrire :

$$U(pn+k) = S_k\ U(n),$$

puis :

$$\sum_{k=0}^{p-1} \sum_{n=0}^{+\infty} U(pn+k)X^{pn+k} = \sum_{k=0}^{p-1} S_k \sum_{n=0}^{+\infty} U(n)X^{pn+k}$$

Posons : $F(X) = \sum_{n=0}^{+\infty} U(n)X^n$. Il vient finalement :

$$F(X) = \left(\sum_{k=0}^{p-1} S_k \ X^k \right) F(X^p).$$

La matrice S, égale à $\sum_{k=0}^{p-1} S_k X^k$, répond à la question.

$\therefore$ (2) $\Longrightarrow$ (3)

On suppose que : $F(X) = S(X)F(X^p)$.

Notons d le degré de S, et introduisons un entier k, tel que : $k \geq \frac{d+p}{p-1}$.

Posons aussi, pour j élément de $[0,k]$: $G_j(X) = X^j F(X)$. On a donc :

$$G_j(X) = \left[X^j \ S(X) \right] F(X^p) .$$

Grâce à un développement en base X^p, on peut écrire :

$$X^j \ S(X) = \sum_{i=0}^{l_j} a_{i,j}(X) \ X^{pi},$$

où $a_{i,j}(X)$ appartient à $M_{m,m}(A[X])$, et vérifie :

$$\deg\left(a_{i,j}(X)\right) \leq p-1.$$

De plus, on a :

$$p\left(l_j - 1\right) \leq j+d \leq k+d .$$

Donc : $l_j \leq 1 + \frac{k+d}{p}$.

Ce dernier nombre est inférieur ou égal à k, du fait du choix de k.

Finalement, on peut écrire :

$$G_j(X) = \sum_{i=0}^{k} a_{i,j}(X) \ X^{pi} F(X^p)$$

$$= \sum_{i=0}^{k} a_{i,j}(X) G_i\left(X^p\right).$$

Soit alors :

$$G(X) = \begin{bmatrix} G_0(X) \\ \vdots \\ G_k(X) \end{bmatrix}, \quad \text{et} \quad T(X) = \left[a_{j,i}(X)\right].$$

La matrice T est définie par blocs, et appartient à $M_{q,q}(A[X])$. De surplus, on a :

$$\deg(T(X)) \leq p-1.$$

Enfin, on observe l'égalité : $G(X) = T(X)G(X^p)$.

$\therefore$ (3) $\Longrightarrow$ (1)

Posons : $G(X) = \sum_{n=0}^{+\infty} U(n)X^n$;

par hypothèse, T(X) s'écrit $\sum_{k=0}^{p-1} T_k X^k$, avec : $T_k \in M_{q,q}(A)$.

L'égalité : $G(X) = T(X)G(X^p)$ entraîne alors :

$$\sum_{n=0}^{+\infty} U(n)X^n = \left(\sum_{k=0}^{p-1} T_k X^k\right)\left(\sum_{n=0}^{+\infty} U(n)X^{pn}\right)$$

$$= \sum_{n=0}^{+\infty} \sum_{k=0}^{p-1} T_k U(n) X^{pn+k}.$$

De ceci, il résulte immédiatement :

$$U(pn+k) = T_k U(n).$$

Le A-module engendré par $u_1,\ldots,u_q$ contient alors le p-noyau de la suite u.∎

Bien entendu, dans cette démonstration, l'hypothèse que f est l'une des composantes , non forcément la première, du vecteur-colonne considéré, est tout à fait suffisante.

Remarque. Notons γ le nombre minimal de générateurs d'un A-module contenant le p-noyau d'une suite u p-régulière sur A, et τ la taille minimale d'une matrice T vérifiant la condition (3) du théorème 3.1. La démonstration de (1) $\Longrightarrow$ (2) montre que $\gamma \leq \tau$. La démonstration de (3) $\Longrightarrow$ (1) prouve que $\tau \leq \gamma$. Donc : $\tau = \gamma$.

Corollaire 1.

Soit f un élément de $A_1[[X]]$, solution d'une p-équation de Mahler linéaire résoluble à droite sur A[X]. La suite de ses coefficients est p-régulière.

Preuve.

Cela résulte du chapitre2,§5 ; si :

$$F = \begin{bmatrix} f \\ \mu_p(f) \\ \cdot \\ \cdot \\ \mu_p{}^{n-1}(f) \end{bmatrix},$$

alors : $F = M\,\mu_p(F)$, où :

$$M = \begin{bmatrix} b_1 b_2 .. b_n \\ 1\ 0 .. 0 \\ 0\ 1 .. 0 \\ . \ . \ .. \ . \\ 0\ 0 .1\ 0 \end{bmatrix}.\blacksquare$$

Proposition 3.1.

Soient A un anneau intègre, A_1 un sur-anneau de A, B une sous-algèbre p-mahlérienne de A((X)).

Si l'élément F de $M_{m,1}\left(A_1((X))\right)$ vérifie l'équation :

$$F = S\ \mu_p(F), \qquad \text{où S appartient à } M_{m,m}(B),$$

toutes les composantes de F sont solutions d'une même équation de Mahler sur B.

Preuve.

De $F = S\ \mu_p(F)$, on tire :

$$F = \left(\prod_{k=0}^{m^2-1} \mu^k(S)\right)\mu^{m^2}(F) = S_0\,\mu^{m^2}(F) ;$$

$$\mu(F) = \left(\prod_{k=1}^{m^2-1} \mu^k(S)\right)\mu^{m^2}(F) = S_1\,\mu^{m^2}(F) ;$$

.....

$$\mu^{m^2-1}(F) = \mu^{m^2-1}(S)\,\mu^{m^2}(F) = S_{m^2-1}\,\mu^{m^2}(F) ;$$

$$\mu^{m^2}(F) = S_{m^2}\,\mu^{m^2}(F).$$

La famille $(S_0,\ldots,S_{m^2})$ est liée sur l'anneau B, qui est intègre. Soit :

$$\sum_{j=0}^{m^2}\alpha_j S_j = 0, \text{ d'où :}$$

$$\sum_{j=0}^{m^2}\alpha_j\ \mu^j(F) = 0.$$

Corollaire 2.

Soient A un anneau intègre, A_1 un sur-anneau de A, et u une suite de $A_1^{\mathbb{N}}$, qui est p-régulière sur A.
La série génératrice de u vérifie une équation de Mahler sur A[X].

Preuve.

Cela résulte du théorème 3.1 et de la proposition 3.1.

Applications.

Considérons u et v deux suites de $A_1^{\mathbb{N}}$, p-régulières sur A, et leurs séries génératrices f et g. Le théorème 3.1 permet de leur associer deux vecteurs, respectivement dans $M_{m,1}(A_1[[X]])$ et $M_{n,1}(A_1[[X]])$, de premières composantes respectives f et g, ainsi que deux matrices carrées S et R, de tailles adaptées, à coefficients dans A[X], tels que :

$$F = S\,\mu(F);\ G = R\,\mu(G).$$

∴ Supposons par exemple : m≥n ; posons :

$$G_1 = \begin{bmatrix} G \\ 0 \end{bmatrix};\ G_1 \in M_{m,1}(A_1[[X]]);$$

Si R_1 est égale à $\begin{bmatrix} R\,0 \\ 0\,0 \end{bmatrix}$, selon le même format, on a :

$$G_1 = R_1\mu(G_1).$$

De plus :

$$\begin{bmatrix} F+G_1 \\ F \\ G_1 \end{bmatrix} = \begin{bmatrix} 0 & S & R_1 \\ 0 & S & 0 \\ 0 & 0 & R_1 \end{bmatrix} \begin{bmatrix} \mu(F)+\mu(G_1) \\ \mu(F) \\ \mu(G_1) \end{bmatrix}$$

Il en suit que la première composante de $F + G_1$ est la série génératrice d'une suite p-régulière. Autrement dit, u + v est p-régulière.

∴ Notons à présent :

$$F = \begin{bmatrix} f_1 \\ \cdot \\ \cdot \\ f_m \end{bmatrix} \qquad \text{et} \qquad G = \begin{bmatrix} g_1 \\ \cdot \\ \cdot \\ g_n \end{bmatrix}.$$

Posons :

$$F \otimes G = \begin{bmatrix} f_1 & g_1 \\ & \cdot \\ & \cdot \\ f_1 & g_n \\ & \cdot \\ & \cdot \\ & \cdot \\ & \cdot \\ f_m & g_1 \\ & \cdot \\ & \cdot \\ f_m & g_n \end{bmatrix}.$$

On a alors :

$$F \otimes G = \big(S \otimes R\big)\big(\mu(F) \otimes \mu(G)\big)$$

Puisque : $\mu(F) \otimes \mu(G) = \mu(F \otimes G)$,on voit que fg est la série génératrice d'une suite p-régulière, qui n'est autre que le produit de convolution de u et de v.

Le problème reste posé de caractériser les séries génératrices des suites régulières par les équations de Mahler scalaires qu'elles satisfont. Il n'est pas nécessaire qu'elles vérifient la condition suffisante du corollaire 1 : 1-X ne vérifie pas d'équation de Mahler résoluble à droite sur A[X] (ch.2, §4). D'ailleurs, l'ensemble des séries génératrices de suites p-régulières forme une A-algèbre, ce qui n'est pas le cas des solutions d'équations de Mahler résolubles à droite.

Il n'est pas non plus suffisant qu'elles vérifient la condition nécessaire du corollaire 2 : $\frac{1}{1-2X}$ vérifie une équation de Mahler sur $\mathbb{Z}[X]$, mais $\left(2^n\right)$ n'est pas p-régulière sur $\mathbb{Z}$.

Exemple.

Depuis le chapitre 2, on sait qu'une équation de Mahler linéaire et résoluble à droite sur $A[[X]]$ admet un espace de solutions qui est isomorphe à A (ou réduit à {0}). Il en résulte que, en général, l'équation fournie par la proposition 3.1 admet, pour coefficient de f, un terme de valuation strictement positive.

Illustrons cette remarque par la situation suivante : soient des éléments a_1 et a_2 de A(X), prenant en 0 la valeur 1, et f_1, f_2 solutions de :

$$f_i = a_i \mu(f_i).$$

Pour déterminer une équation de Mahler vérifiée conjointement par f_1 et f_2, il suffit de considérer les matrices :

$$F = \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} \text{ et } S = \begin{bmatrix} a_1 & 0 \\ 0 & a_2 \end{bmatrix}$$

La famille $(S\mu(S),\ \mu(S),\ I)$ est liée, puisque les matrices sont diagonales. Une relation de liaison mahlérienne est donc donnée par :

$$\begin{vmatrix} a_1\mu(a_1) & \mu(a_1) & 1 \\ a_2\mu(a_2) & \mu(a_2) & 1 \\ F & \mu(F) & \mu^2(F) \end{vmatrix} = 0.$$

Soit :

$$\left[\mu(a_1)-\mu(a_2)\right]F-\left[a_1\mu(a_1)-a_2\mu(a_2)\right]\mu(F)+\mu(a_1)\mu(a_2)(a_1-a_2)\mu^2(F)=0.$$

On constate qu'effectivement le terme $\mu(a_1)-\mu(a_2)$ s'annule en 0, et que la division par le monôme correspondant est rendue impossible par le coefficient de $\mu^2(F)$, de valuation strictement plus petite.

Généralisation.

Soit A un anneau (non nécessairement noethérien), et B une sous-A-algèbre de A[[X]], p-mahlérienne. Considérons l'ensemble $\mathfrak{R}(B)$ des éléments f de A[[X]] tels qu'il existe un entier naturel m, un vecteur colonne F dans $M_{m,1}(B)$, de première composante égale à f, et une matrice S de $M_{m,m}(B)$, vérifiant :

$$F = S\ \mu_p(F).$$

Les calculs matriciels effectués dans le cas des suites p-régulières (cf applications ci-dessus) montrent que $\mathfrak{R}(B)$ est un sous-anneau de A[[X]] . Si de plus B est p-mahlérienne, $\mathfrak{R}(B)$ est p-mahlérien ; l'égalité $F = S\ \mu_p(F)$ implique en effet :

$$\mu_p(F) = \mu_p(S)\ \mu_p(\mu_p(F)),$$

et $\mu_p(S)$ appartient toujours à $M_{m,m}(B)$.

En outre, $\mathfrak{R}(B)$ contient B ; soit en effet f un élément de B. Puisque 1 appartient à E, on a :

$$\begin{cases} f = f.\mu_p(1) \\ 1 = 1.\mu_p(1) \end{cases}$$

Donc $\mathfrak{R}(B)$ est une B-algèbre.

Lorsque B est A[X], $\mathfrak{R}(B)$ est la A[X]-algèbre des fonctions génératrices de suites p-régulières.

2 Equations de Mahler satisfaites par un élément de A((X)).

Soient A un anneau, et f un élément de A((X)) satisfaisant à une équation de Mahler sur une sous-A-algèbre B, p-mahlérienne, de A((X)) :

$$\sum_{k=0}^{n} b_k \mu^k(f) = 0 ;$$

cette série f vérifie d'autres équations sur B ; par exemple :

$$\sum_{k=0}^{n} \lambda b_k \mu^k(f) = 0 \text{ , avec } \lambda \text{ dans B ; ou encore :}$$

$$\sum_{k=0}^{n} \mu(b_k)\ \mu^{k+1}(f) = 0 .$$

Pour tenir compte de ces possibilités, nous allons construire l'anneau de Mahler $B[m]$; c'est tout d'abord le B-module libre engendré par e, m ,m^2,.... On définit une loi •, interne dans $B[m]$, par les conditions suivantes :

→ la loi • est distributive à droite et à gauche par rapport à l'addition ;

→ $\forall\ (i,j) \in \mathbb{N}^2\ \ \forall\ (b,c) \in B^2\ \ bm^i \bullet cm^j = b\mu^i(c)\ m^{i+j}$.

On constate qu'alors :

→ $\forall\ P \in B[m]\ \ e \bullet P = P \bullet e = P$;

→ $\forall\ P \in B[m]\ \ \forall\ b \in B\ \ (be) \bullet P = bP$;

→ $m \bullet m = m^2$, et plus généralement : $m \bullet m \ldots . \bullet m = m^i$;

→ $\forall\ (i,j,k) \in \mathbb{N}^3\ \ \forall\ (b,c,d) \in B^3\ \ \left(bm^i \bullet cm^j\right) \bullet dm^k =$

$\left[b\mu^i(c)\ m^{i+j}\right] \bullet dm^k = b\mu^i(c)\mu^{i+j}(d)\ m^{i+j+k}$, et :

$$bm^i \bullet \left(cm^j \bullet dm^k\right) = bm^i \bullet \left[c\mu^j(d)\ m^{j+k}\right] = b\mu^i(c)\mu^{i+j}(d)\ m^{i+j+k} .$$

La loi • est donc associative.

Ainsi, B[m] est un anneau, non commutatif en général. Notons que ce n'est pas une B-algèbre, la structure de B-module dont il dispose n'étant pas totalement compatible.

Par sa construction même, on dispose d'une opération de B[m] sur A((X)), définie de la manière suivante :

si P est dans B[m] , on pose : $P = \sum_k b_k m^k$; pour f dans A((X)), on définit :

$$P.f = \sum_k b_k \mu^k(f) .$$

On a bien, si Q est égal à $\sum_i c_i m^i$:

$$(P \bullet Q).f = \left(\sum_{k,i} b_k \mu^k(c_i) m^{k+i} \right).f = \sum_{k,i} b_k \mu^k(c_i) \mu^{k+i}(f) ,$$

et, d'autre part :

$$P.(Q.f) = P.\left(\sum_i c_i \mu^i(f) \right) = \sum_{k,i} b_k \mu^k(c_i) \mu^{k+i}(f).$$

Soit à présent, pour f élément de A((X)), Ann(f) l'ensemble des P de B[m] tels que :

$$P.f = 0.$$

Proposition 3.2.

L'ensemble Ann(f) est un sous-B-module de B[m] , et un idéal à gauche de B[m] .

Preuve.

Soit $\sum_k b_k m^k$ un élément de Ann(f) ; si λ est dans B, on a :

$$(\lambda m^i) \bullet \left(\sum_k b_k m^k \right) = \sum_k \lambda \mu^i(b_k) m^{k+i}, \text{ et par ailleurs :}$$

$$\left(\sum_k \lambda \mu^i(b_k) m^{k+i} \right).f = \sum_k \lambda \mu^i(b_k) \mu^{k+i}(f) = \lambda \mu^i \left(\sum_k b_k \mu^k(f) \right) = 0.\blacksquare$$

Il devient intéressant de chercher les idéaux à gauche de Ann(f).

On appelle degré d'un élément de B[m] le degré habituel ; si B[m] est intègre, on a :

$$\deg(P \bullet Q) = \deg(P) + \deg(Q).$$

Il en résulte en particulier que $B[m]$ est intègre.

Lemme (de division euclidienne).

Soient P_1, P_2 des éléments de $B[m]$, le coefficient dominant de P_2 étant inversible dans B. Il existe alors un couple (Q,R) d'éléments de $B[m]$, unique, qui vérifie :

$$P_1 = Q \bullet P_2 + R \ ; \deg(R) < \deg(P_2).$$

Preuve.

Notons : $P_1 = \sum_{k=0}^{n} b_k m^k$ et $P_2 = \sum_{i=0}^{m} c_i m^i$.

∴ On démontre l'existence par récurrence sur n. On peut supposer : $n \geq m$. Puisque c_m est inversible dans B, on peut écrire : $c_m d_m = 1$, et donc :

$\mu^{n-m}(c_m)\mu^{n-m}(d_m) = 1$, avec d_m, et $\mu^{n-m}(d_m)$ par conséquent, éléments de B.

Posons :

$$\lambda = \mu^{n-m}(d_m).$$

On a :

$$P_1 - \left(b_n \lambda m^{n-m}\right) \bullet P_2 = \left(b_n - b_n \lambda \mu^{n-m}(c_m)\right) m^m + P_3,$$

avec : $\deg(P_3) < n$. Donc :

$$P_1 - \left(b_n \lambda m^{n-m}\right) \bullet P_2 = P_3.$$

L'hypothèse de récurrence conclut.

∴ L'unicité est évidente.∎

Proposition 3.3.

Soit B un sous-corps p-mahlérien de $A((X))$. Les idéaux à gauche de $B[m]$ sont principaux.

Preuve.

Soit $\mathfrak{I}$ un idéal à gauche de $B[m]$ et, s'il n'est pas réduit à 0, P_2 un élément de $\mathfrak{I}$, de degré minimal. Si P_1 appartient à $\mathfrak{I}$, on peut écrire :

$$P_1 = Q \bullet P_2 + R \quad \text{avec : } \deg(R) < \deg(P_2).$$

Donc R = 0.∎

On appelle polynôme minimal de f sur B le générateur unitaire de Ann(f). Il n'est défini que si f vérifie une équation de Mahler linéaire sur B.

3 Factorisation dans $B[m]$.

Nous débutons ici une étude de la factorisation dans $B[m]$.

Scolie.

Pour résoudre l'équation :

$$\mu^2(f) + \alpha\mu(f) + \beta f = 0,$$

il est naturel (que l'on pense aux équations différentielles) de poser : $\lambda = \frac{\mu(f)}{f}$.

On obtient alors :

$$\mu(g) + \alpha + \frac{\beta}{g} = 0,$$

équation de type homographique. Ce simple calcul est réinterpreté dans la suite.

Proposition 3.4.

Soient B une sous-algèbre p-mahlérienne , B_1 un sous-corps p-mahlérien de A((X)), et P un élément de $B[m]$.

On suppose qu'il existe f dans B_1-{0} tel que : P.f = 0.

On peut alors écrire :

$$P = Q\bullet\left(m-\lambda e\right), \text{ où : } Q \in B_1[m] \text{ et } \lambda \in B_1.$$

Preuve.

Posons : $\lambda = \frac{\mu(f)}{f}$; c'est un élément de B_1. Appliquons le lemme de division euclidienne. On peut écrire :

$$P = Q\bullet\left(m-\lambda e\right) + R, \text{ avec } \deg(R) = 0.$$

Il en suit que : $R \in B_1 e$. Mais :

$$P.f = 0 = Q.\left(\mu(f)-\lambda f\right) + R.f = R.f.$$

Soit : R = 0.∎

Exemple.

Supposons P égal à $m^2 + \alpha m + \beta e$. Supposons connu un élément f, non nul, tel que : P.f = 0.

Pour factoriser P, on peut effectuer la division, ou bien procéder par identification ; d'une part, on a :

$$P = (m-\gamma e)\bullet(m-\lambda e) = m^2 - (\gamma+\mu(\lambda))m + \gamma\lambda e.$$

D'où le système :

$$(1) \quad \begin{cases} \gamma + \mu(\lambda) = -\alpha \\ \gamma\lambda = \beta \end{cases}$$

D'après la proposition 3.4, λ, égal à $\frac{\mu(f)}{f}$, convient ; on obtient alors γ à l'aide de l'une des deux relations (1), l'autre étant alors obligatoirement vérifiée.

D'un autre côté, on peut tenter de résoudre directement le système (1), qui équivaut à :

$$(2) \quad \begin{cases} \frac{\beta}{\lambda} + \mu(\lambda) = -\alpha \\ \gamma = \frac{\beta}{\lambda} \end{cases},$$

ceci sous l'hypothèse où β est non nul. D'ailleurs, si β est nul, on obtient sans détour :

$$P = (m+\alpha e)\bullet m.$$

Revenant au cas général, nous constatons que l'équation non linéaire qui constitue le premier membre du système (2) est de type homographique. Les conditions de sa résolution, que pour la simplicité nous étudierons hors de cas particuliers, sont exprimées dans la proposition suivante.

Proposition 3.5.

Soient A un corps, A_1 un surcorps de A, et a, b , c des éléments de A[[X]] tels que a(0)b(0)-c(0) soit non nul.

Le nombre d'éléments f de $A_1[[X]]$, solutions de l'équation :

$$f\mu(f) + af + b\mu(f) + c = 0,$$

est égal au nombre de solutions de l'équation à l'inconnue z de A_1 :

$$z^2 + (a(0) + b(0))z + c(0) = 0.$$

Preuve.

Nécessairement, si : $z = f(0)$, on a :

$$z^2 + (a(0) + b(0))z + c(0) = 0.$$

Soit réciproquement un élément z de A_1 , solution de l'équation du second degré mentionnée.

L'hypothèse : z = -a(0) est exclue, puisque a(0)b(0)-c(0) n'est pas nul.

Soit alors :

$$\mathfrak{E} = \left\{ g \in A_1[[X]] \quad g(0) = z \right\},$$

et posons, pour g dans $\mathfrak{E}$:

$$\psi(g) = \frac{-b\mu(g)-c}{\mu(g)+a}.$$

On a :

$(\mu(g)+a)(0) = z + a(0)$, qui est non nul. De plus :

$$\psi(g)(0) = \frac{-b(0)z-c(0)}{z+a(0)} = z.$$

Donc ψ va de $\mathfrak{E}$ dans $\mathfrak{E}$. Si g_1 et g_2 sont dans $\mathfrak{E}$, on a :

$$\psi(g_1)-\psi(g_2) = \frac{-b\mu(g_1)-c}{\mu(g_1)+a} + \frac{b\mu(g_2)+c}{\mu(g_2)+a} = \frac{(\mu(g_1)-\mu(g_2))(c-ab)}{(\mu(g_1)+a)(\mu(g_2)+a)}.$$

D'où :

$$\mathrm{val}(\psi(g_1)-\psi(g_2)) \geq \mathrm{val}(\mu(g_1)-\mu(g_2)) = p\,\mathrm{val}(g_1-g_2).$$

Comme $\mathfrak{E}$ est un ensemble fermé de $A_1[[X]]$, ψ admet dans $\mathfrak{E}$ un point fixe, qui est solution de notre problème.∎

Soit alors : B = A[[X]], et l'élément P de B[m], égal à $m^2 + \alpha m + \beta e$. Pour factoriser P, on peut procéder comme suit :

→ On résout le système (2), c'est-à-dire tout d'abord l'équation :

$$\lambda\mu(\lambda) + \alpha\lambda + \beta = 0.$$

La condition : $c(0) \neq a(0)b(0)$ entraîne : $\beta(0) \neq 0$,ce qui signifie que l'équation P.f = 0 est résoluble à droite sur B.

L'équation :

$$z^2 + \alpha(0)z + \beta(0) = 0$$

nous fournit une ou deux solutions z_1, z_2 dans une clôture algébrique A_1 de A; notons λ_1 et λ_2 les éléments de $A_1[[X]]$ associés par la proposition 3.5.

→Le système (2) nous fournit alors γ_1 et γ_2, éléments de $A_1[[X]]$, puisque γ_1 et γ_2 sont non nuls.

On obtient ainsi :

$$P = \left(m-\gamma_i e\right)\bullet\left(m-\lambda_i e\right), \; i = 1 \text{ ou } i = 2.$$

Puisqu'en général λ_1 et λ_2 sont distincts, on constate qu'il n'y a pas unicité de la décomposition en facteurs de degré un.

Un cas particulier intéressant est celui où l'équation P.f = 0 admet une solution dans A[[X]]. Pour cela, il suffit que $\beta(0)$ soit non nul, et que $1+\alpha(0) + \beta(0)$ soit nul (chapitre 2). La méthode précédente nous conduit à :

$z_1 = 1$, $z_2 = \beta(0)$. On a donc :

$$P = \left(m-\frac{\beta}{\lambda}e\right)\bullet\left(m-\lambda e\right), \text{ avec } \lambda(0) = 1.$$

La résolution de P.f = 0 s'effectue alors comme suit :

$$P.f = 0 \iff \left(m-\frac{\beta}{\lambda}e\right).\left(\left(m-\lambda e\right).f\right) = 0.$$

Supposons $\beta(0)$ différent de 1, et donc $\frac{\beta}{\lambda}(0)$ différent de 1. L'équation :

$$\left(m-\frac{\beta}{\lambda}e\right).h = 0$$

n'admet que la solution nulle. Donc :

$$P.f = 0 \iff \left(m-\lambda e\right)(f) = 0,$$

équation qui admet une droite de solutions.

Supposons $\beta(0)$ égal à 1. Plutôt que de faire une étude distincte, on remarque simplement que, si $(m-\lambda e).f$ est nul, alors P.f l'est aussi. Comme l'ensemble des solutions de la dernière équation forme aussi une droite, on dispose toujours de l'équivalence précédente.

En résumé :

la résolution d'une p-équation de Mahler linéaire d'ordre deux et résoluble à droite sur A[[X]] équivaut aux résolutions successives d'une équation de Mahler homographique, et d'une p-équation de Mahler linéaire d'ordre un et résoluble à droite sur A[[X]].

4 Etude d'une équation matricielle dans le cas d'un sous-corps p-mahlérien.

Dans tout ce paragraphe, A est un corps, et B un sous-corps p-mahlérien de $A((X))$.

Soient F un élément de $M_{m,1}(A((X)))$, S une matrice de $M_{m,m}(B)$, tels que :

$$F = S\ \mu_p(F).$$

L'objectif de ce paragraphe est d'étudier les différentes équations matricielles vérifiées par F, en relation avec le B-espace vectoriel $\mathcal{V}$ engendré par $f_1,...,f_m$, lorsque :

$$F = \begin{bmatrix} f_1 \\ \cdot \\ \cdot \\ f_m \end{bmatrix}$$

Lemme 1.

$\mathcal{V}$ est stable par μ_p.

Preuve.

Soit $(f_1,...,f_r)$ une base de $\mathcal{V}$, avec : dim $\mathcal{V}$ = r. Les éléments $f_{r+1},...,f_m$ sont combinaisons linéaires d'éléments de la base. Il en résulte que $\mu_p(f_{r+1}),..., \mu_p(f_m)$ sont combinaisons linéaires des $\mu_p(f_1),..., \mu_p(f_r)$. Puisque $f_1,...,f_r$ sont combinaisons linéaires des $\mu_p(f_1),..., \mu_p(f_m)$, et ceci grâce à l'équation matricielle, ces éléments de base sont en fait des combinaisons linéaires des éléments $\mu_p(f_1),..., \mu_p(f_r)$. Puisque la dimension de $\mathcal{V}$ est égale à r, les éléments $\mu_p(f_1),..., \mu_p(f_r)$ sont dans $\mathcal{V}$. Cet espace vectoriel est donc stable par μ_p.∎

Lemme 2.

(a) Soit $(g_1,...,g_r)$ une base de $\mathcal{V}$; il existe P dans $M_{r,r}(B)$ telle que, si :

$$G = \begin{bmatrix} g_1 \\ \cdot \\ \cdot \\ g_r \end{bmatrix},$$

alors :

$$G = P\,\mu_p(G).$$

De plus, si P_1, dans $M_{r,r}(B)$, vérifie :

$$G = P_1\,\mu_p(G),$$

alors P_1 est inversible.

(b) On a :

$$\dim \mathcal{V} \leq rg(S).$$

Preuve.

(a) Avec les notations du lemme 1, posons :

$$F_0 = \begin{bmatrix} f_1 \\ \vdots \\ f_r \end{bmatrix}.$$

Nous avons constaté l'existence d'une matrice Q de $M_{r,r}(B)$ telle que :

$$F_0 = Q\,\mu_p(F_0).$$

Par ailleurs, on peut écrire :

$$G = R\,F_0, \text{ avec R inversible.}$$

Donc :

$$G = R\,\mu_p(F_0) = R\,Q\,\mu_p(R)^{-1}\,\mu_p(G) = P\,\mu_p(G).$$

En outre, soit P_1 telle que :

$$G = P_1\,\mu_p(G).$$

On a manifestement :

$$rg(g_1,\ldots,g_r) \leq rg(P_1).$$

Donc : $rg(P_1) = r$.

(b) Puisque : $rg(f_1,\ldots,f_m) \leq rg(S)$, on a nécessairement :

$$\dim \mathcal{V} \leq rg(S).\blacksquare$$

Proposition 3.6.

Soient F, égal à $\begin{bmatrix} f_1 \\ \vdots \\ f_r \end{bmatrix}$, un élément de $M_{r,1}(A((X)))$, et M une matrice de $M_{r,r}(B)$, tels que : $F = M\,\mu_p(F)$. On suppose que :

$$rg(f_1,\ldots,f_r) = r.$$

Soit : $G = \begin{bmatrix} g_1 \\ \vdots \\ g_r \end{bmatrix}$, où $(g_1,\ldots,g_r)$ est une base de $Vect(f_1,\ldots,f_r)$.

Il existe alors M_1 dans $GL_r(B)$ telle que : $G = M_1\,\mu_p(G)$.

De plus, il existe Q dans $GL_r(B)$ telle que :

$$M_1 = Q\,M\,\mu_p(Q)^{-1}.$$

Preuve.

L'existence de M_1 résulte du lemme 2, ainsi que son inversibilité.On peut alors écrire :

$$G = Q\,F, \text{ avec : } Q \in GL_r(B).$$

D'où :

$$Q\,F = M_1\,\mu_p(Q)\,\mu_p(F), \text{ soit : } F = Q^{-1}M_1\,\mu_p(Q)\,\mu_p(F).$$

Finalement : $\left(Q^{-1}M_1\ \mu_p(Q) - M \right)\mu_p(F) = 0.$

Puisque : $rg(\mu_p(f_1),\ldots,\mu_p(f_r)) = r$, on obtient aussitôt :

$$Q^{-1}M_1\,\mu_p(Q) - M = 0.\blacksquare$$

Définition.

Soient M_1 et M_2 des matrices de $M_{r,r}(B)$: on les dit p-conjuguées s'il existe une matrice Q de $GL_r(B)$ telle que :

$$M_1 = Q\,M_2\,\mu_p(Q)^{-1}.$$

La relation de p-conjugaison est évidemment d'équivalence sur $M_{r,r}(B)$.

Théorème 3.2.

Soit A un corps, f un élément de A((X)), B un sous-corps p-mahlérien de A((X)). On suppose que f vérifie une p-équation de Mahler linéaire sur B. Les nombres suivants sont alors finis et égaux :

$$r_1 = \dim \mathrm{Vect}_B \left\{ \mu^i(f) \right\}_{i \in \mathbb{N}} ;$$

r_2 = l'ordre minimal d'une p-équation de Mahler linéaire sur B vérifiée par f ;

r_3 = le degré d'un générateur de Ann(f) ;

r_4 = l'ordre minimal d'une matrice M à coefficients dans B, et d'un vecteur colonne F, de première composante égale à f, tels que :

$$F = M\,\mu_p(F).$$

Soit r cette valeur commune. Alors :

(1) Si **P** appartient à Ann(f), et deg(**P**) est égal à r, alors **P** engendre Ann(f).

(2) Si M appartient à $M_{r,r}(B)$, et F, de première composante égale à f, appartient à $M_{r,1}(A((X)))$, l'égalité : $F = M\,\mu_p(F)$ implique l'inversibilité de M.

(3) Si M_1 et M_2 , de taille r, vérifient :

$$F_i = M_i\,\mu_p(F_i)$$

où F_1 et F_2, de taille r, ont f pour première composante, alors M_1 et M_2 sont p-conjuguées.

Preuve.

Il est évident que r_2 et r_3 sont égaux ; l'inégalité : $r_1 \leq r_2$ résulte d'une récurrence immédiate, l'inégalité inverse étant claire.

A l'aide du vecteur :

$$F = \begin{bmatrix} f \\ \mu(f) \\ . \\ \mu^{r_2-1}(f) \end{bmatrix},$$

on constate que : $r_4 \leq r_2$.

Soient F et M, de tailles r_4 , tels que : $F = M\,\mu_p(F)$, et notons $f_1,\ldots,f_{r_4}$ les composantes de F - avec : $f = f_1$.

Soit $\mathcal{V}$ le B-espace vectoriel engendré par $f_1,\ldots,f_{r_4}$. Complétons f_1, noté à présent g_1, en une base $\{g_1,\ldots,g_r\}$ de $\mathcal{V}$. D'après le lemme 2, on a : $r \leq r_4$, et donc évidemment, $r = r_4$; puisque $\mathcal{V}$ est stable par μ_p (lemme1), on a : $r_1 \leq r$ et, en résumé :

$$r = r_1 = r_2 = r_3 = r_4 .$$

Le point (1) résulte immédiatement du §2, tandis que le point (2) découle du lemme 2. Quant à (3), constatons que, avec les hypothèses faites, les familles des

composantes de F_1 et F_2 sont des bases de $\mathcal{V}$. La proposition 3.6. entraîne alors que M_1 et M_2 sont p-conjuguées.∎

Chapitre 4

Comme nous l'avons constaté dans les chapitres antérieurs, les phénomènes mahlériens que nous étudions dépendent du corps de base, ne fût-ce qu'au travers de sa caractéristique. Bien qu'à certains égards cela paraisse décevant, il est économique d'utiliser des méthodes analytiques pour démontrer des résultats qui semblent formels, ce qui suppose bien évidemment de se placer sur un corps adapté, qui sera pris égal à $\mathbb{C}$. Traditionnellement, pour montrer que la série génératrice d'une suite p-automatique est transcendante (sur $\mathbb{C}(x)$) ou rationnelle, on utilise un résultat de Szego, selon lequel une série entière, dont les coefficients sont dans un ensemble fini, admet le cercle unité comme frontière naturelle, sauf à être rationnelle.

Pour étendre ce résultat aux suites p-régulières, on s'appuiera sur l'équation fonctionnelle satisfaite par la série génératrice, et, dans un premier temps, on étudiera le problème matriciel associé (théorème 4.2); l'application à une équation scalaire n'est pas mécanique : c'est l'objet du théorème 4.3

Le rapport entre les singularités d'une fonction et sa transcendance ou, de façon plus générale, son caractère non élémentaire, est établi dans l'annexe 1.

L'étude est précédée par un théorème d'existence et d'unicité de solution d'une équation fonctionnelle de type mahlérien (théorème 4.1), le cas linéaire faisant l'objet d'une étude un peu plus précise (proposition 4.2).

Le cadre de ce chapitre est différent de celui des précédents ; c'est celui des fonctions méromorphes sur un ouvert de $\mathbb{C}$. Si f est une fonction de la variable complexe, dont le domaine de définition D est stable par l'application $x \longmapsto x^p$, on notera $\mu_p(f)$ la fonction :

$$x \longmapsto f(x^p)$$

En particulier, si D est un ouvert de $\mathbb{C}$ stable par $x \longmapsto x^p$, et si $\mathcal{H}(D,E)$ désigne l'espace vectoriel des fonctions holomorphes sur $\mathbb{C}$ et à valeurs dans un $\mathbb{C}$-espace vectoriel E de dimension finie, on dispose d'une application $\mathbb{C}$-linéaire μ_p de $\mathcal{H}(D,E)$ dans lui-même.Lorsque E est égal à $\mathbb{C}$, on note $\mathcal{H}(D)$ l'anneau ainsi obtenu ; si D est connexe, ce que l'on supposera toujours, cet anneau est intègre. Son corps des fractions, noté $\mathcal{M}(D)$, s'identifie au corps des fonctions méromorphes sur D. L'application μ_p , qui est un monomorphisme de $\mathcal{H}(D)$, s'étend naturellement en un monomorphisme de $\mathcal{M}(D)$.

On désigne par $\mathcal{M}_0(D)$ le sous-anneau de $\mathcal{M}(D)$ formé des fonctions méromorphes régulières en 0, lorsque 0 appartient à D. On utilisera en outre les notations et identifications suivantes :

$$\mathcal{H}\left(D,\mathbb{C}^n\right) = M_{n,1}\left(\mathcal{H}(D)\right) ;$$

$$\mathcal{M}\left(D,\mathbb{C}^n\right) = M_{n,1}\left(\mathcal{M}(D)\right) ;$$

$$\mathcal{M}_0\left(D,\mathbb{C}^n\right) = M_{n,1}\left(\mathcal{M}_0(D)\right) .$$

Dans une large mesure, les résultats des chapitres antérieurs s'appliquent à la situation de ce chapitre. Il y a en effet un isomorphisme entre le corps $\mathcal{M}(D)$ et un sous-corps du corps $\mathbb{C}((X))$. Cependant, il convient de garder à l'esprit que cet isomorphisme n'est pas topologique, et que d'ailleurs les topologies ne sont pas comparables.

Une fonction entière par rapport à $Y = \left(y_1,\ldots,y_n\right)$, élément de $\mathbb{C}^n$, est une fonction analytique du n-uplet Y ou, de façon équivalente, entière par rapport à chacune des variables. Si l'on note k le n-uplet $\left(k_1,\ldots,k_n\right)$, on désignera par Y^k le monôme $y_1^{k_1}\ldots y_n^{k_n}$; une fonction entière admet un développement du type :

$$\sum_{k\in\mathbb{N}^n} a_k Y^k ,$$

où la série est absolument sommable.

Dans la suite de ce chapitre, D désigne le disque unité ouvert.

Considérons alors une fonction :

$$F : D\times\mathbb{C}^n \longrightarrow \mathbb{C}^n$$

$$(x,Y) \longmapsto F(x,Y)$$

qui est entière par rapport à Y, méromorphe sur D et régulière en 0 relativement à x. On peut ainsi écrire :

$$F(x,Y) = \left(f_1(x,Y),\ldots,f_n(x,Y)\right) ,$$

où chacune des fonctions $f_i(x,Y)$admet le développement :

$$f_i(x,Y) = \frac{1}{d(x)} \sum_{k\in\mathbb{N}^n} a_k(x) Y^k ,$$

d étant dans $\mathcal{H}(D)$, ainsi que les a_k, et d(0) étant non nul.

Nous cherchons les solutions U, appartenant à $\mathcal{M}_0(D)$, de l'équation :

$$U = F(x,\mu(U)) \ ,$$

c'est-à-dire du système :

$$u_1(x)=f_1\left(x,u_1(x^p),\ldots,u_n(x^p)\right);$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots;$$
$$u_n(x)=f_n\left(x,\ u_1(x^p),\ldots,u_n(x^p)\right).$$

Posons $U_0 = U(0)$. Il est évidemment nécessaire que l'on ait :

$$U_0 = F\left(0,U_0\right),$$

ce qui sera supposé dorénavant.

Nous nous proposons donc d'étudier le problème suivant :

(1) $U\in \mathcal{M}_0(D)$; $U = F(x,\mu(U))$; $U(0) = U_0$.

1 Solutions au problème (1).

On se fixe, pour la suite, un réel ρ_0 *de* $]0,1[$, *tel que l'application* $x \longrightarrow F(x,Y)$ soit holomorphe sur un voisinage Ω de $D'\left(0,\rho_0\right)$; il en résulte que l'application :

$$(x,Y) \longrightarrow F(x,Y)$$

est holomorphe sur $\Omega\times\mathbb{C}^n$.

Lemme.

Soit C un convexe compact de $\mathbb{C}^n$. Il existe un réel k tel que :

$$\forall\ x\in D'\left(0,\rho_0\right)\ \forall\ Y,Z\in C\quad \|F(x,Y)-F(x,Z)\| \le k\|Y-Z\| .$$

Preuve .

Etant analytique sur $\Omega\times\mathbb{C}^n$, l'application $(x,T) \longrightarrow \frac{\partial F}{\partial Y}(x,T)$ est bornée sur $D'\left(0,\rho_0\right)\times C$. L'inégalité des accroissements finis permet d'écrire :

$$\|F(x,Y)-F(x,Z)\| \le \sup_{T\in[Y,Z]} \left\|\frac{\partial F}{\partial Y}(x,T)\right\|.\|Y-Z\| .$$

Posons alors :

$$k = \sup_{(x,T)\in D'(0,\rho_0)\times C} |||\frac{\partial F}{\partial Y}(x,T)|||.$$

Ce réel k répond à la question.∎

Lorsque W est une fonction bornée sur $D'(0,\rho)$,où $\rho>0$, nous noterons $||W||_\rho$ sa norme uniforme sur $D'(0,\rho)$. Si W appartient à $\mathcal{M}_0(D)$, posons :

$$\phi(W)(x) = F\left(x,W\left(x^p\right)\right).$$

Il est clair que $\phi(W)$ est encore dans $\mathcal{M}_0(D)$. De plus, si ρ appartient à $]0,\rho_0]$, et si W est holomorphe sur un voisinage de $D'(0,\rho)$, $\phi(W)$ est aussi holomorphe sur ce voisinage.

Théorème 4.1.

Le problème (1) admet une unique solution.

Preuve.

(a)Unicité.

Soient U et V des solutions de (1), holomorphes au voisinage de $D'(0,\rho)$, où ρ est dans $]0,\rho_0]$.Soit C la boule de centre 0, de rayon $||U||_\rho+||V||_\rho$. On a, pour x dans $D'(0,\rho)$:

$$||F\left(x,U\left(x^p\right)\right) - F\left(x,V\left(x^p\right)\right)|| \le k||U\left(x^p\right)-U\left(x^p\right)||,$$

ce qui résulte du lemme. On obtient alors, pour r dans]0,ρ] :

$$||\phi(U)-\phi(V)||_r \le k||U-V||_{r^p},$$

et donc :

$$||U-V||_r \le k\,||U-V||_{r^p}.$$

Par récurrence, puisque r^{p^n} est encore dans]0,ρ] , il vient :

$$||U-V||_r \le k^n||U-V||_{r^{p^n}}.$$

Par ailleurs, U-V s'annulant en 0, il existe a tel que, pour tout x dans $D'(0,\rho)$, on ait :

$$||(U-V)(x)|| \le a|x|, \text{ et donc : } ||U-V||_r \le ar.$$

De cela, il suit :

$||U-V||_r \leq ak^n r\rho^n$, ceci pour tout n dans $\mathbb{N}$. Donc :

$||U-V||_r = 0$ pour $r \leq \rho$.

En particulier, U-V est nulle sur un voisinage de 0, et , d'après le principe du prolongement méromorphe, on a : U =V.

(b)Existence.

Soit : $U_1 = \Phi\left(U_0\right)$ - ici, U_0 est une fonction constante -. Puisque U_0 est holomorphe sur D, U_1 est holomorphe sur Ω.

De plus, $U_1(0) = \Phi\left(U_0\right)(0) = F\left(0,U_0\right) = U_0$. Donc U_1-U_0 s'annule en 0 : il existe un réel a tel que, pour x dans $D'\left(0,\rho_0\right)$, on ait :

$||U_1(x)-U_0|| \leq a|x|$.

Soit C la boule de centre 0, de rayon $||U_0|| +1$, et k donné par le lemme. Choisissons ρ, inférieur à ρ_0, tel que :

$$a\sum_{n=0}^{+\infty} k^n\rho\rho^n \leq 1.$$

Ceci est possible, car : $\sum_{n=0}^{+\infty} k^n\rho\rho^n = \rho\sum_{n=0}^{+\infty} k^n\rho\rho^{n-1}$, la dernière somme écrite tendant vers 1 lorsque ρ tend vers 0.

Posant $U_n = \Phi^n\left(U_0\right)$, montrons par récurrence :

(i) $||U_{n+1}-U_n||_\rho \leq k\,||U_n-U_{n-1}||_\rho\rho$;

(ii) $||U_{n+1}||_\rho \leq ||U_0|| +1$.

On a : $||U_1-U_0||_\rho \leq a\rho$, et comme $a\rho \leq 1$,on a :$||U_1||_\rho \leq ||U_0|| +1$. Supposons les relations (i) et(ii) vraies, et utilisons à nouveau le lemme, avec $Y = U_{n+1}\left(x^\rho\right)$, $Z = U_n\left(x^\rho\right)$, et x dans $D'\left(0,\rho\right)$. On a bien Y, Z dans C, et donc :

$$||U_{n+2}(x)-U_{n+1}(x)|| \leq k||U_{n+1}\left(x^\rho\right)-U_n\left(x^\rho\right)||.$$

Il en résulte :

$||U_{n+2}-U_{n+1}||_\rho \leq k\,||U_{n+1}-U_n||_\rho\rho$, soit (i).

De plus :

$$||U_{j+1}-U_j||_\rho \leq k||U_1-U_0||_\rho \rho^j \text{ pour } j \leq n+1.$$

Donc :

$$||U_{n+2}-U_0||_\rho \leq a\sum_{j=0}^{n+1} k_j \rho^{pj} \leq 1.$$

Le résultat en suit.

A présent, la relation (i), appliquée pour tout n, prouve l'*inégalité* :

$$||U_{n+1}-U_n||_\rho \leq ak^n\rho^{p^n},$$

et donc la convergence uniforme sur $D'(0,\rho)$ de la suite (U_n), dont la limite U est ainsi dans $\mathcal{H}(D'(0,\rho))$. De plus, l'égalité :

$$\forall\ x \in D'(0,\rho)\quad U_{n+1}(x) = F\left(x,U_n\left(x^p\right)\right)$$

implique :

$$\forall\ x \in D(0,\rho)\quad U(x) = F\left(x,U\left(x^p\right)\right).$$

Définissons alors, par récurrence, une fonction U sur D tout entier : pour x tel que $\rho \leq |x| < \sqrt[p]{\rho}$ on pose :

$$U(x) = F\left(x,U\left(x^p\right)\right),$$

et ainsi de suite. La fonction U ainsi construite vérifie la relation précédente dans D ; elle est par conséquent méromorphe dans D, puisque, si elle l'est dans $D(0,\rho)$, elle l'est aussi dans $D\left(0,\sqrt[p]{\rho}\right)$, et ainsi indéfiniment.

Enfin, une récurrence aisée montre que, pour tout n, on a : $U_{n+1}(0) = U(0)$ et par conséquent :

$$U_0 = U(0).\blacksquare$$

2 Le cas linéaire.

Soit A une matrice de $M_{n,n}(\mathcal{M}_0(D))$. On s'intéresse au problème :

$$(2)\ U \in M_{n,1}(\mathcal{M}_0(D))\ ;\ U = A\mu(U)\ ;\ U_0 = U(0),$$

où $U_0 = A(0)U_0$.

Le théorème 4.1 entraîne que le problème (2) admet une unique solution. Comme l'application qui à U associe U(0) est manifestement linéaire, on obtient :

Proposition 4.1.

L'ensemble des solutions de (2) est un $\mathbb{C}$- espace vectoriel, de codimension $rg(A(0)-i)$.

Avec les notations de la preuve du théorème 4.1, on a :

$$U_1(x) = A(x)U_0 ,$$

et plus généralement

$$U_n(x) = A(x)A\left(x^p\right).....A\left(x^{p^{n-1}}\right)U_0 .$$

Donc : $U = \lim\left(A\mu(A)....\mu^{n-1}(A)U\right)$,

tout au moins sur un certain $D\left(0,\rho\right)$, avec : $\rho>0$. Nous allons en fait prouver un peu mieux.

Proposition 4.2.

Soit U la solution de (2). La suite $\left(U_n(x)\right)$ *converge vers U, au sens de la convergence d'une suite de fonctions méromorphes sur D. Plus précisément, il y a convergence uniforme sur tout compact ne contenant pas de pôle de l'une des* $\mu^k(A)$, lorsque k décrit $\mathbb{N}$.

Preuve.

∴ Notons Ω le complémentaire de l'ensemble des pôles des fonctions $\mu^k(A)$, lorsque k décrit $\mathbb{N}$. Montrons que Ω est ouvert dans D. Soit ρ un réel, avec $\rho<1$. Le réel ρ_0 est choisi de façon que A n'ait aucun pôle dans $D'\left(0,\rho_0\right)$. Il en résulte que $\mu^k(A)$ n'a aucun pôle dans $D'\left(0,\rho_0{}^{p^{-k}}\right)$. Pour k assez grand, $\mu^k(A)$ n'a pas de pôle dans $D'\left(0,\rho\right)$. Finalement, $D-\Omega$ ne rencontre $D'\left(0,\rho\right)$ qu'en un ensemble fini, et donc $D-\Omega$ est discret. En particulier, Ω est ouvert dans D.

∴ Fixons-nous un compact K, inclus dans D, stable par $x \to x^p$, qui soit un voisinage de 0, et inclus dans Ω. Soit en outre ρ dans $]0,\rho_0]$, tel que $D'\left(0,\rho\right)$ soit inclus dans K, et notons $\| \|_\rho$ la norme uniforme sur $D'\left(0,\rho\right)$. On notera aussi $\| \|_\infty$ la norme uniforme sur K.

Il existe n_0, ne dépendant que de K, tel que :

$$x\in K \Longrightarrow x^{p^{n_0}} \in D'\left(0,\rho\right).$$

Posons : $V(x) = U_0 \cdot A(x)\ U_0$. Il existe a tel que :

$$x \in D'(0,\rho) \Rightarrow \|V(x)\| \leq a|x|.$$

Posons :

$$U_n(x) = \left(A\mu(A)....\mu^{n-1}(A)\right)(x)\ U_0\ .$$

On a :

$$U_n(x)-U_{n+1}(x) = \left(A\mu(A)....\mu^{n-1}(A)\right)(x)\left(\ U_0 - \mu^n(A)(x)U_0\right),$$

soit :

$$U_n(x)-U_{n+1}(x) = \left(A\mu(A)....\mu^{n-1}(A)\right)(x)\left(\mu^n(V)(x)\right).$$

Finalement :

$$\|U_n-U_{n+1}\|_\infty \leq a\ \|\|A\|\|_\infty....\|\|\ \mu^{n-1}(A)\|\|_\infty \|\mu^n(V)\|_\infty,$$

et donc :

$$\|U_n-U_{n+1}\|_\infty \leq a\ \|\|A\|\|_\infty^{\ n}\ \ \rho^{p^n-n_0}.$$

La convergence normale sur K de la série $\sum_{n\in\mathbb{N}}\left(U_n-U_{n+1}\right)$, et donc la convergence uniforme de la suite $\left(U_n\right)$, résultent de cette majoration.

∴ Soit à présent un réel ρ quelconque de $]0,1[$. Désignons par Ω_ρ l'ensemble $\Omega \cap D'(0,\rho)$. Soit $\{a_1,...,a_m\}$ le complémentaire de Ω_ρ dans $D'(0,\rho)$, avec a_1 de plus petit module. Soit $\varepsilon>0$ tel que $D(a_1,\varepsilon)$ ne rencontre pas $D'(0,\rho_0)$. Alors, si α est une racine p^k-ième de a_1, $D\left(\alpha,\varepsilon^{p^{-k}}\right)$ ne rencontre pas $D'(0,\rho_0)$. De plus, si $|\alpha| \leq \rho$, α n'appartient pas à Ω. L'ensemble des α, lorsque k est assujetti à vérifier $|a_1| \leq \rho^{p^k}$, est inclus dans $\{a_1,...,a_m\}$.

Enlevons à Ω_ρ la réunion des $D\left(\alpha,\varepsilon^{p^{-k}}\right)$, et recommençons avec les a_i restant ; au bout d'un nombre fini d'opérations, on aura construit, en enlevant à Ω_ρ une réunion finie de disques ouverts, un compact $K_{\rho,\varepsilon}$, contenant $D'(0,\rho_0)$, et donc voisinage de 0, qui en outre sera stable par l'application $x \longmapsto x^p$: car si x^p appartient à l'un des $D\left(\alpha,\varepsilon^{p^{-k}}\right)$, x appartient à l'un des $D\left(\alpha,\varepsilon^{p^{-k-1}}\right)$.

De plus, il est clair que, de la famille des $K_{\rho,\varepsilon}$, on peut extraire une suite exhaustive dans Ω : par exemple, la famille $\left(K_{1-1/n,1/m}\right)$.

Remarque.

Il n'est pas sans intérêt de comparer la situation dans $\mathcal{M}_0$ (D) et dans $\mathbb{C}[[X]]$.

Le problème (2) précédent a pour pendant le problème (2') suivant :

$$(2')\quad F \in M_{n,1}\left(\mathbb{C}[[X]]\right)\ ;\ F = A\mu(F)\ ;\ F_0 = F(0),$$

où $A \in M_{n,n}\left(\mathbb{C}[[X]]\right)$ et où $F_0 = A(0)F_0$.

Le théorème 4.1 affirme que le problème (2) admet une unique solution, tandis que la proposition 2.11 nous dit que le problème (2') admet lui aussi une unique solution.

A la matrice A , à coefficients méromorphes sur D, et réguliers en 0 , on peut associer une matrice, toujours notée A, de $M_{n,n}\left(\mathbb{C}[[X]]\right)$; de cette façon, à un problème (2), on peut toujours associer un problème (2') ; l'un admet alors une solution U, l'autre une solution F, et il est clair que U est l'image de F par l'injection canonique de $\mathcal{M}_0$ (D) dans $\mathbb{C}[[X]]$: cela provient de la récurrence nécessairement satisfaite par les coefficients du développement en série entière de F, et de l'unicité.

Il faut tout de même constater que la situation n'est pas aussi claire dans le cas général, où $\mathcal{M}_0$ (D) est remplacé par $\mathcal{M}$ (D) et où $\mathbb{C}[[X]]$ est remplacé par $\mathbb{C}((X))$; dans cette situation, en effet, l'unicité n'est pas établie.

3 Singularités non polaires d'une solution au problème (1).

Soit U une fonction méromorphe sur Ω, à valeurs dans $\mathbb{C}^n$. Un point α de l'adhérence de Ω est dit singularité non polaire de U si U n'est pas prolongeable en une fonction méromorphe sur un voisinage de α. Par définition, une telle singularité appartient à la frontière de Ω. Nous noterons S(U) l'ensemble des singularités (sous-entendu : non polaires) de U, et R(U) le complémentaire de S(U) dans la frontière de Ω L'ensemble R(U) est donc constitué des points réguliers et des singularités polaires de U. Si $U = \left(u_1,\ldots,u_n\right)$, α est dans S(U) si, et seulement si, il existe i tel que $\alpha \in S\left(u_i\right)$.

Nous considérerons dans la suite un élément U de $\mathcal{M}_0(D)$, solution du problème (1). Les hypothèses sur la fonction F restent, dans ce paragraphe, celles du début du chapitre.

Lemme 1.

Soit A un ensemble non borné de réels. L'ensemble des b/a,où b décrit $\mathbb{Z}$ et a décrit A-{0}, est dense dans $\mathbb{R}$.

Preuve.

Soit x dans $\mathbb{R}$, et $\varepsilon > 0$. Il existe a, élément de A-{0}, tel que :

$$0 < \frac{1}{|a|} \leq \varepsilon.$$

Soit b dans $\mathbb{Z}$ tel que :

$$x \in [\frac{b}{a}, \frac{b+1}{a}[\quad \text{ou} \quad [\frac{b+1}{a}, \frac{b}{a}[, \text{ selon le signe de a.}$$

On a alors $\left| x - \frac{b}{a} \right| \leq \varepsilon$, donc le résultat.∎

Par exemple, si A est l'ensemble des puissances positives de 2, l'ensemble obtenu est celui des réels dyadiques.

Lemme 2.

Soit x un élément de Γ, cercle unité de $\mathbb{C}$. L'ensemble des racines p^k-ièmes de x est dense dans Γ.

Preuve.

Posons $x = e^{i\theta}$. Etant donnés y dans Γ et $\varepsilon > 0$, il existe k_0 tel que, pour $k \geq k_0$, l'on ait : $\left| e^{i\frac{\theta}{p^k}} - 1 \right| \leq \varepsilon$.

Par ailleurs, l'ensemble des p^k, où $k \geq k_0$, est non borné : l'ensemble des b/a, où b décrit $\mathbb{Z}$ et a décrit A-{0}, est donc dense dans $\mathbb{R}$, et son image par l'application $t \longmapsto e^{2i\pi t}$ est, elle aussi, dense dans G. Il existe donc un k, avec $k \geq k_0$, et un b dans $\mathbb{Z}$, tels que :

$$\left| e^{2i\pi \frac{b}{p^k}} - y \right| \leq \varepsilon.$$

On a donc, pour ces valeurs de k et de b :

$$\left| e^{i\frac{\theta}{p^k} + 2i\pi \frac{b}{p^k}} - y \right| \leq 2\varepsilon + \varepsilon^2.$$

Comme $e^{i\frac{\theta}{p^k} + 2i\pi \frac{b}{p^k}}$ est une racine p^k-ième de x, le résultat est démontré.∎

Lemme 3.

Soit $U \in \mathcal{M}(D)$. Alors :

$$\alpha \in R(\mu(U)) \iff \alpha^p \in R(U).$$

Preuve.

∴ Si $\alpha \in R(\mu(U))$, on peut prolonger $\mu(U)$ sur un voisinage Ω de α en une fonction méromorphe sur $D \cup \Omega$, notée ϕ. L'application $x \longmapsto x^p$ est biholomorphe d'un voisinage de α, que l'on peut supposer être Ω , sur le voisinage Ω^p de α^p . Notons $x \longmapsto \sqrt[p]{x}$ son application inverse et posons, pour x dans Ω^p, $\psi(x) = \phi(\sqrt[p]{x})$; ψ est méromorphe sur Ω^p. De plus, si $x \in D \cap \Omega^p$, on a $\sqrt[p]{x} \in D \cap \Omega$, et donc :

$$\phi(\sqrt[p]{x}) = \mu(U)(\sqrt[p]{x}) = U(x).$$

L'application ψ est bien un prolongement méromorphe de U sur le voisinage Ω^p de α^p.

∴ Si $\alpha^p \in R(U)$, notons ψ un prolongement méromorphe de U sur le voisinage Ω_1 de α^p , et posons, pour $x \in \sqrt[p]{\Omega_1}$:

$$\phi(x) = \psi(x^p).$$

La fonction ϕ est alors méromorphe sur $\sqrt[p]{\Omega_1}$. De plus, si $x \in D \cap \sqrt[p]{\Omega_1}$, on a :

$$x^p \in D \cap \sqrt[p]{\Omega_1}$$

et donc :

$$\psi\ (\ x^p\ ) = U(\ x^p\ ) = \mu(U)(x)\ ;$$

la fonction ϕ est bien un prolongement méromorphe de $\mu(U)$ sur le voisinage $\sqrt[p]{\Omega_1}$ de α .∎

Avant d'aborder le problème (1) lui-même, supposons un instant que U soit solution du problème (1') :

$$\mu(U) = G(x,U)\ ,$$

où G vérifie des hypothèses analogues à celles sur F. Cela sera possible dès que F, dans un certain cadre, sera inversible.

Proposition 4.2.

Soit U un élément de $\mathcal{M}$ (D) vérifiant :

$$\mu(U) = G(x,U)\ ,$$

où l'application $x \longmapsto G(x,Y)$ est méromorphe sur un voisinage du disque unité fermé, et où $Y \longmapsto G(x,Y)$ est entière. Alors :

$$R(U) = \varnothing \text{ ou } \Gamma\ .$$

Preuve.

Soit x dans S(U); et soit α tel que $\alpha^p = x$; le lemme 3 nous dit que α appartient à $S(\mu(U))$; il résulte immédiatement de (1') que α appartient à S(U) ; finalement, S(U) est stable par extraction de racine p-ième. Si S(U) est non vide, le lemme 2 nous dit que S(U) contient un sous-ensemble dense dans Γ . Comme S(U) est fermé, il est égal à Γ .∎

A présent, étudions le cas où $R(U) = \Gamma$.

Lemme 4.

Soit U un élément de $\mathcal{M}$ (D), tel que $R(U) = \Gamma$; U est alors prolongeable en une fonction méromorphe sur un voisinage de $D'\left(0,1\right)$.

Preuve.

L'ensemble des pôles de U dans D est fini, car, dans le cas contraire, il y aurait un point d'accumulation de tels pôles qui ne pourrait qu'être une singularité non polaire de U. Soit p un polynôme dont les zéros sont les pôles précédents, avec le même ordre de multiplicité que celui qu'ils ont comme pôles de U. Alors pU n'a pas de pôle dans D, et R(pU) est égal à R(U). On procède de même pour les

singularités polaires, en nombre fini, de U sur Γ. De cette façon, on est ramené au résultat sur les fonctions holomorphes.∎

Lemme 5.

Soient U un élément de $\mathcal{M}(\Gamma)$, et

$$G : \mathbb{C}\times\mathbb{C}^n \longrightarrow \mathbb{C}^n$$

$$(x,Y) \longmapsto G(x,Y)$$

une fonction méromorphe par rapport à x, entière par rapport à Y, tels que :

$$\forall\, x \in D \qquad U\left(x^p\right) = G(x, U(x)).$$

Si $R(U) = \Gamma$, la fonction U est prolongeable en une fonction méromorphe sur $\mathbb{C}$, vérifiant toujours l'égalité :

$$\forall\, x \in \mathbb{C} \qquad U\left(x^p\right) = G(x, U(x)).$$

Preuve.

D'après le lemme 4, il existe R>1 et une fonction V, méromorphe sur D(0,R), prolongeant U. De plus, $V\left(x^p\right)$ - G(x,V(x)) est méromorphe sur $D\left(0, \sqrt[p]{R}\right)$, et coïncide avec la fonction nulle sur D. On a donc :

$$\forall\, x \in D\left(0, \sqrt[p]{R}\right) \qquad V\left(x^p\right) = G(x, V(x)).$$

Supposons fausse la conclusion du lemme, et soit(W , Ω) un prolongement maximal de$\left(V,D(0,R)\right)$, "étoile de Mittag-Leffler " de $\left(V,D(0,R)\right)$. Il advient alors que Ω est différent de $\mathbb{C}$. Considérons alors un disque ouvert $D\left(0,\rho\right)$, de rayon maximal, inclus dans Ω, avec :

$R \leq \rho < +\infty$. On a donc :

$$\forall\, x \in D\left(0, \sqrt[p]{\rho}\right) \qquad W\left(x^p\right) = G(x, W(x)).$$

Soit α un complexe quelconque, de module ρ. Soit alors β vérifiant : $\beta^p = \alpha$.

L'application $x \longmapsto x^p$ *est biholomorphe d'un voisinage de* α, *noté* ω , *sur le* voisinage ω^p de α^p . Notons $x \longmapsto \sqrt[p]{x}$ son application inverse. Il n'est pas restrictif de supposer ω inclus dans $D\left(0,\rho\right)$, puisque : $|\beta| = \sqrt[p]{\rho}$ et donc $|\beta| < \rho$. Posons pour x dans ω^p :

$$W_1(x) = G\left(\sqrt[p]{x}\ ,\ W\left(\sqrt[p]{x}\right)\right).$$

Alors W_1 est méromorphe sur ω^p. En outre, si $x \in D(0,\rho) \cap \omega^p$, alors :

$\sqrt[p]{x} \in D\left(0, \sqrt[p]{\rho}\right) \cap \omega$, et donc :

$$W(x) = G\left(\sqrt[p]{x}\ .\ W\left(\sqrt[p]{x}\right)\right).$$

Finalement, W et W_1 coïncident sur $D(0,\rho) \cap \omega^p$. Il en résulte que l'on a pu prolonger W sur un voisinage de α , et ce pour tout α de module 1. Le lemme 4 entraîne que W est prolongeable en une fonction méromorphe sur un voisinage de $D'(0,\rho)$, ce qui est une contradiction.∎

Nous notons à présent $\mathbb{C}(x)$ le corps des fonctions fractions rationnelles sur un ouvert de $\mathbb{C}$, qui s'identifie à un sous-corps du corps des fonctions méromorphes sur cet ouvert.

Théorème 4.2.

Soit U une fonction méromorphe sur D, solution de l'équation (2):

$U = A\mu(U)$, où $A \in M_n(\mathbb{C}(x))$.

Si R(U) n'est pas vide, $U \in M_{n,1}(\mathbb{C}(x))$.

Preuve.

D'après le chapitre 3, nous pouvons supposer que $A \in GL_n(\mathbb{C}(x))$. En effet, il s'agit de montrer que chaque composante de U appartient à $M_{n,1}(\mathbb{C}(x))$. Si u est une telle composante, Vect $\{\mu^i(u)\}_{i\in\mathbb{N}}$ est un sous-espace vectoriel de l'espace engendré par les composantes de U ; un élément de R(U) appartiendra alors à R(v), pour tout v dans Vect $\{\mu^i(u)\}_{i\in\mathbb{N}}$. Il suffit alors de compléter u en une base de l'espace vectoriel précédent, pour obtenir une équation dans laquelle la matrice est inversible. Les lemmes 3 et 5 s'appliquent, puisque l'on peut réécrire (2) sous la forme :

$$\mu(U) = A^{-1}U.$$

Désignons toujours par U le prolongement méromorphe de U à $\mathbb{C}$ tout entier. On obtient :

$\forall\ x \in \mathbb{C}\quad U(x) = A(x)U(x^p)$, encore grâce au lemme 5.

∴ Soit $\rho > 1$ choisi pour que $D'(0,\rho)$ contienne tous les zéros de det(A(x)). Notons m le cardinal de l'ensemble de ces zéros, fixons un entier q tel que $p^q > m$, et supposons par l'absurde que U admette un pôle β tel que $|\beta| > \rho^{p^q}$. Notons s l'entier tel que :

$$\rho^{p^{s+1}} \geq |\beta| > \rho^{p^s}.$$

On a évidemment $s \geq q$.

Soit α une racine p-ième de β. L'égalité :

$$U(x^p) = A(x)^{-1} U(x)$$

montre α que est pôle de $A(x)^{-1}U(x)$. Si $s \geq 1$, on a : $|\alpha| > \rho$, et par conséquent α n'est pas pôle de $A(x)^{-1}$; c'est donc un pôle de U(x).

Par récurrence, les racines p-ièmes, p^2-ièmes,....,p^s-ièmes de β sont des pôles de U(x).

Mais les racines p^{s+1}-ièmes de β sont dans $D'(0,\rho)$, et sont des pôles de $A(x)^{-1}U(x)$; ceux-ci sont en nombre m dans ce disque. Or :

$$p^{s+1} \geq p^{q+1} > p^q \geq m.$$

Il y a donc une contradiction : tous les pôles de U sont de module inférieur ou égal à ρ^{p^k}. En particulier, l'ensemble des pôles de U est borné, et donc fini.

∴ Nous pouvons poser :

$$U(x) = \frac{1}{n(x)} V(x), \text{ où } V \text{ est entière et } n \text{ un polynôme. On a :}$$

$$V(x^p) = \frac{n(x^p)}{n(x)} A(x)^{-1} V(x) = B(x)V(x), \text{ où } B \in M_n(\mathbb{C}(x)).$$

Montrons que V est un polynôme. Pour cela, posons :

$$\|B\|_R = \sup_{R \leq |x| \leq R^p} \|B(x)\|, \text{ lorsque } R>1.$$

Ceci définit un réel dès que $R \geq \rho_1$, où ρ_1 est choisi de façon que B(x) ait tous ses pôles dans $D(0,\rho_1)$, et supérieur à 1.

De l'égalité $V(x^p) = B(x)V(x)$, on déduit :

$$\|V\|_{R^p} \leq \|B\|_R \|V\|_R \text{ ,et, par récurrence :}$$

$$\|V\|_{R^{p^k}} \leq \|B\|_R \|B\|_{R^p} \ldots \|B\|_{R^{p^{k-1}}} \|V\|_R .$$

A présent, comme $B \in M_n(\mathbb{C}(x))$, il existe un m dans $\mathbb{N}$ tel que :

$$\|B\|_R \leq R^m$$

pour tout R supérieur ou égal à ρ_1.

Donc, pour tout entier k :

$$||V||_{R^{p^k}} \leq R^{m+pm+\ldots+p^{k-1}m} ||V||_R \leq R^{p^k m} ||V||_p .$$

Considérons alors x et r tels que :

$$r \geq |x| \geq \rho_1,$$

puis k tel que :

$$\rho_1^{p^k} \leq |r| < \rho_1^{p^{k+1}}.$$

Dans ces conditions, on a :

$$||V(x)|| \leq ||V||_{\rho_1^{p^{k+1}}} \leq r^{pm} ||V||_{\rho_1},$$

d'où :

$$\sup_{\rho_1 \leq |x| \leq r} ||V(x)|| \leq r^{pm} ||V||_{\rho_1}.$$

Comme V est une fonction entière, on a aussi :

$$\sup_{|x| \leq r} ||V(x)|| = O(r^{pm}), \quad + \infty$$

et donc V appartient à $M_n(\mathbb{C}[x])$. ∎

Conséquences.

Soit u une fonction méromorphe sur le disque unité, solution d'une p-équation linéaire de Mahler sur $\mathbb{C}(x)$ que l'on écrit :

$$u = \sum_{k=1}^{m} a_k \mu^k(u), \text{ les } a_k \text{ étant dans } \mathbb{C}(x).$$

Supposons que u n'est pas dans $\mathbb{C}(x)$.

En associant à u le vecteur U, égal à :

$$\begin{bmatrix} u \\ \mu_p(u) \\ \vdots \\ \mu_p^{m-1}(u) \end{bmatrix},$$

et la matrice A, égale à :

$$\begin{bmatrix} a_1 a_2 \ldots a_m \\ 1\ 0 \ldots 0 \\ 0\ 1 \ldots 0 \\ \ldots\ldots \\ 0\ 0\ 1\ 0 \end{bmatrix},$$

on aboutit à l'équation vectorielle :

$$U = A\,\mu_p(U).$$

Le théorème 4.2 nous dit alors que S(U) est égal à Γ, ou encore que :

$$\bigcup_{i=0}^{m-1} S(\mu^i(u)) = \Gamma.$$

Supposons alors S(u) dénombrable. Le lemme 3 implique que les ensembles $S(\mu^i(u))$ sont eux aussi dénombrables, ce qui est une contradiction manifeste. En résumé, S(u) est non dénombrable. On pourrait d'ailleurs montrer de façon identique que la mesure linéaire de S(u) est strictement positive.

Il résulte de l'annexe 1 que u ne peut être une fonction élémentaire, et en particulier ne peut être algébrique sur $\mathbb{C}(x)$.

L'objet du paragraphe qui suit est d'obtenir des résultats plus précis sur les singularités non polaires de u.

4 Cas d'une équation scalaire.

Nous disons que Γ est frontière naturelle pour une fonction méromorphe sur le disque unité ouvert lorsque tous les points de Γ en sont singularités non polaires. Dans ce paragraphe, u est à valeurs complexes.

Lemme 1.

Soit u un élément de $\mathcal{M}(D)$; si Γ est frontière naturelle pour $\mu(u)$, Γ est alors aussi frontière naturelle pour u.

Preuve.

Puisque R(u) est vide, le lemme 3 du §3 nous dit que $R(\mu(u))$ l'est aussi.∎

Lemme 2.

Soit $(u_0,\ldots,u_{n-1})$ une famille libre sur $\mathbb{C}(x)$ d'éléments de $\mathcal{M}(D)$.

La famille $\left(\mu(u_0),\ldots,\mu(u_{n-1})\right)$ est libre sur $\mathbb{C}(x)$.

Preuve.

Considérons par l'absurde une relation de la forme :

$$\sum_{k=0}^{n-1} \lambda_k \, \mu\left(u_k\right) = 0,$$

où les λ_k sont dans $\mathbb{C}(x)$, et $\lambda_{n-1} = 1$, ce qui n'est pas restrictif.

Notons U_p l'ensemble des racines p-ièmes de 1. On a :

$$\forall\, x \in D \qquad \sum_{k=0}^{n-1} \lambda_k(x)\, u_k(x^p) = 0,$$

et donc :

$$\forall\, x \in D \quad \forall\, \omega \in U_p \qquad \sum_{k=0}^{n-1} \lambda_k(\omega x)\, u_k(x^p) = 0.$$

Par somme sur ω, il vient :

$$\forall\, x \in D \qquad \sum_{k=0}^{n-1} \nu_k(x)\, u_k(x^p) = 0.$$

où $\nu_k(x) = \sum_{\omega \in U_p} \lambda_k(\omega x)$.

Or il existe ξ dans $\mathbb{C}(x)$ tel que : $\nu_k(x) = \xi(x^p)$; de plus, $\nu_{n-1}(x) = p$. Il vient donc :

$$\forall\, x \in D \qquad \sum_{k=0}^{n-1} \nu_k(x^p)\, u_k(x^p) = 0, \text{ soit encore :}$$

$$\sum_{k=0}^{n-1} \nu_k\, u_k = 0.$$

Comme $\nu_{n-1} = p$, il y a une contradiction.∎

Lemme 3.

Si u est un élément de $\mathcal{M}(D)$ tel que $\mu(u)$ soit un élément de $\mathbb{C}(x)$, alors u appartient à $\mathbb{C}(x)$.

Preuve.

Dire que u est dans $\mathbb{C}(x)$, c'est dire que la famille(1,u) est liée. Il s'agit donc du lemme 2.∎

Lemme 4.

Notons π_h la projection canonique de $\mathbb{N}^m$ sur $\mathbb{N}^h$ lorsque $\mathbb{N}^m = \mathbb{N}^h \times \mathbb{N}^{m-h}$.

Soit $\mathcal{A}$ un sous-ensemble de $\mathbb{N}^m$ vérifiant la propriété $(\mathcal{P})$ suivante :

$$(\mathcal{P}) \quad \forall\ h \in [1,m] \quad \forall \left(k_1,\ldots,k_{h-1}\right) \in \pi_{h-1}(\mathcal{A}) \quad \left\{k \in \mathbb{N} \left(k_1,\ldots,k_{h-1},k\right) \in \pi_h(\mathcal{A})\right\} \text{ est infini.}$$

Soit ω un ouvert non vide de $\mathbb{R}$. Il existe alors un réel θ et $(k_1,\ldots,k_m)$ dans $\mathcal{A}$ tels que les ensembles $p^{k_1}\theta+\mathbb{Z},\ldots,\ p^{k_m}\theta+\mathbb{Z}$, rencontrent tous ω.

Preuve.

Dans la suite, une écriture du type : 0,abcde... désignera le développement propre d'un réel de [0,1[en base p.

∴ Supposons tout d'abord que $\omega \cap]0,1[$ est non vide, et soit α dans $\omega \cap]0,1[$. Il existe q dans $\mathbb{N}$ tel que $\left[\alpha - \frac{1}{p^q}, \alpha + \frac{1}{p^q}\right]$ soit inclus dans ω. Si le début du développement de α est 0, $\alpha_1\alpha_2.....\alpha_q$, notons δ la chaîne de caractères : $\alpha_1\alpha_2.....\alpha_q$. On remarque que tous les réels dont le développement commence par 0,δ sont dans ω.

Appliquant l'hypothèse pour h égal à 1, on voit que $\pi_1(\mathcal{A})$ est infini.

Soit k_1 dans $\pi_1(\mathcal{A})$; tous les réels θ dont le développement commence par 0,00...0δ (avec k_1 zéros après la virgule) sont tels que $p^{k_1}\theta$, égal à 0,δ... , est dans ω.

Soit maintenant k_2, avec : $k_2 \geq k_1 + q$, tel que $\left(k_1, k_2\right)$ appartienne à $\pi_2(\mathcal{A})$.

Les réels θ dont le développement commence par 0,00...0δ00...0δ (avec k_1 zéros après la virgule, puis $(k_2 - k_1 - q)$ zéros après le premier δ) sont tels que $p^{k_1}\theta$ est dans ω, mais aussi tels que $p^{k_2}\theta$ appartienne à $\mathbb{Z}+\omega$.

Par récurrence, on construit $(k_1,\ldots,k_m)$ dans $\mathcal{A}$ *tel que, pour tout réel* θ dont le développement commence par :

0,00....0 δ0.... 0 δ 0.....δ0.....0δ, avec des blocs de k_1,
puis $k_2 - k_1 - q$,....., puis $k_m - k_{m-1} - q$ zéros,

les réels $p^{k_1}\theta$, $p^{k_2}\theta$,....., $p^{k_m}\theta$ appartiennent tous à $\mathbb{Z}+\omega$.

∴ Dans le cas général, on remarque que ω', égal à $\mathbb{Z}+\omega$, rencontre toujours $]0,1[$, et donc que l'on peut construire θ tel que :

$$p^{k_1}\theta\ ,\ p^{k_2}\theta\ ,\ .....,\ p^{k_m}\theta \text{ appartiennent tous à } \mathbb{Z}+\omega' = \mathbb{Z}+\omega. \blacksquare$$

Nous appuyant sur ces lemmes, nous allons démonter le théorème principal de ce paragraphe.

Théorème 4.3 (Antoine et Claudia).

Soit u une solution méromorphe sur D de l'équation :

$$\sum_{k=0}^{m} a_k\, \mu^k(u) = 0,$$

où les a_k sont dans $\mathbb{C}(x)$ et non tous nuls.

Si u n'appartient pas à $\mathbb{C}(x)$, le cercle unité est frontière naturelle pour u.

Preuve.

Choisissons m minimal ; d'après la proposition 2.9, a_0 est non nul ; de plus, d'après le théorème 3.2 , la famille $\left(u, \mu(u),..., \mu^{m-1}(u)\right)$ est une base du $\mathbb{C}(x)$-espace vectoriel $\mathcal{V}$ engendré par $\left\{\mu^k(u)\right\}_{k\in\mathbb{N}}$.

∴ Construisons un ensemble $\mathcal{A}$ vérifiant la propriété $(\mathcal{P})$ énoncée dans le lemme 4, et tel que, de plus :

$$\forall \left(k_1,...,k_m\right) \in \mathcal{A} \qquad \left(\mu^{k_1}(u),....,\mu^{k_m}(u)\right) \text{ soit libre.}$$

On suppose aussi : $m\geq 1$ (si m est nul, il n'y a rien à construire).

Posons : $\mathcal{A}_0 = \varnothing$ et $\mathcal{A}_1 = \mathbb{N}$; puisque u est non nul, la famille $\left(\mu^k(u)\right)$ est libre, quel que soit k.

Supposons construits, pour un q compris entre 0 et m-1, des ensembles $\mathcal{A}_0, \mathcal{A}_1,....., \mathcal{A}_q$ tels que, pour tout i compris entre 0 et q-1 :

→ $\mathcal{A}_i \subset \mathbb{N}^i$;

→ $\forall \left(k_1,...,k_i\right) \in \mathcal{A}_i \qquad \left\{k\in \mathbb{N} \ \left(k_1,...,k_i,k\right) \in \mathcal{A}_{i+1}\right\}$ est infini ;

→ $\forall \left(k_1,...,k_{i+1}\right) \in \mathcal{A}_{i+1} \qquad \left(\mu^{k_1}(u),....,\mu^{k_{i+1}}(u)\right)$ est libre.

Construisons alors $\mathcal{A}_{q+1}$, inclus dans $\mathbb{N}^{q+1}$. Soit $\left(k_1,...,k_q\right)$ dans $\mathcal{A}_q$, et posons :

$$\mathcal{E}(k_1,....,k_q) = \{k \in \mathbb{N} \quad (\mu^{k_1}(u),.....,\mu^{k_q}(u), \mu^{k}(u)) \text{ est libre}\}.$$

∴ Supposons, par l'absurde, que $\mathcal{E}(k_1,....,k_q)$ est fini. Puisque $(\mu^{k_1}(u),.....,\mu^{k_q}(u))$ est libre, on a, pour tous les k n'appartenant pas à $\mathcal{E}(k_1,....,k_q)$:

$$\mu^{k}(u) \in \text{Vect}(\mu^{k_1}(u),.....,\mu^{k_q}(u)) .$$

Cette condition est réalisée en particulier pour tous les k supérieurs à un certain l ; la famille $(\mu^{l}(u), \mu^{l+1}(u),....,\mu^{l+m-1}(u))$ est donc liée, car:

$$q \leq m-1.$$

Le lemme 2 implique alors que la famille (u, $\mu(u)$,..., $\mu^{m-1}(u)$ est liée, ce qui est une contradiction.

$\mathcal{E}(k_1,....,k_q)$ étant infini, posons :

$$\mathcal{A}_{q+1} = \bigcup_{(k_1,...,k_q) \in \mathcal{A}_q} \{(k_1,....,k_q,k) \quad k \in \mathcal{E}(k_1,....,k_q)\}.$$

L'ensemble $\mathcal{A}_{q+1}$ répond aux conditions imposées.

Au terme de la récurrence, l'ensemble $\mathcal{A}_m$,noté $\mathcal{A}$, vérifie les propriétés attendues.

∴ *Partant de l'hypothèse que u n'est pas une fraction rationnelle, nous raisonnons par l'absurde en supposant que R(u) est non vide.*

Appliquons le théorème 4.2 à un élément U de $M_{m,1}(\mathcal{M}(D))$, de composantes égales à u, $\mu(u)$,...,$\mu^{m-1}(u)$ (cf ch. 3) ; puisque U n'appartient pas à $M_m(\mathbb{C}(x))$, le cecle unité Γ est frontière naturelle pour U. En d'autres termes, tout point de Γ est singularité non polaire pour l'une des fonctions u, $\mu(u)$,..., $\mu^{m-1}(u)$, c'est-à-dire que :

$$R(u) \cap R(\mu(u)) \cap .....\cap R(\mu^{m-1}(u)) = \varnothing .$$

Considérons à présent l'ouvert ω., égal à $f^{-1}(R(u))$, où :

$$f : \mathbb{R} \to \mathbb{C}$$

$$t \longmapsto e^{it} .$$

L'ensemble $\frac{1}{2\pi}\omega$ est aussi un ouvert de $\mathbb{R}$, non vide par hypothèse. Le lemme 4, appliqué à l'ensemble $\mathcal{A}$ précédent, montre l'existence d'un réel θ et d'un élément $(k_1,...,k_m)$ de $\mathcal{A}$ tels que les ensembles $\theta p^{k_j} + \mathbb{Z}$ rencontrent tous l'ensemble $\frac{1}{2\pi}\omega$; posons : $z = e^{2i\pi\theta}$. On a :

$$z^{p^{k_j}} = e^{2i\pi\theta p^{k_j}}.$$

Or $2\pi\theta p^{k_j}$ appartient à $2\pi\mathbb{Z} + \omega$. Donc :

$$z^{p^{k_j}} \in f(\omega) = R(u).$$

Le lemme 3 du §3 entraîne que z est élément de $R\left(\mu^{k_j}(u)\right)$, et ce pour tous les j entre 1 et m ; d'où :

$$z \in R\left(\mu^{k_1}(u)\right) \cap .....\cap R\left(\mu^{k_m}(u)\right).$$

Comme $(\mu^{k_1}(u),...., \mu^{k_m}(u))$ est une base de $\mathcal{V}$, chacune des fonctions u, $\mu(u),...., \mu^{m-1}(u)$ est une combinaison linéaire, à coefficients dans $\mathbb{C}(x)$, d'éléments de cette famille, et par conséquent :

$$z \in R(u) \cap R\left(\mu(u)\right) \cap .....\cap R\left(\mu^{m-1}(u)\right).$$

Ceci est la contradiction souhaitée.∎

Corollaire 1.

Soit u, fonction méromorphe sur D, solution d'une équation de Mahler sur $\mathbb{C}(x)$. Si u n'appartient pas à $\mathbb{C}(x)$, u est transcendante sur $\mathbb{C}(x)$.

Preuve.

Une fonction méromorphe sur D, algébrique sur $\mathbb{C}(x)$, ne peut admettre le cercle unité comme ensemble de singularités non polaires [annexe].∎

Exemple.

Soit u la série génératrice d'une suite régulière sur $\mathbb{C}$, ou sur un sous-corps de $\mathbb{C}$. Nous savons que u est holomorphe sur D, comme on le constate en examinant la majoration des termes de la suite donnée dans le paragraphe suivant. Le corollaire 1 s'applique alors à cette situation.
Ce corollaire est à mettre en relation avec la proposition 1.4. On peut lui donner le statut formel suivant:

Corollaire 2.

Soit f un élément de $\mathbb{C}[[X]]$, vérifiant une équation linéaire de Mahler résoluble à droite sur $\mathbb{C}(X) \cap \mathbb{C}[[X]]$. Si f n'est pas dans $\mathbb{C}(X)$, f est transcendant sur $\mathbb{C}(X)$.

Preuve.

On écrit le problème matriciel associé à l'équation de Mahler, et l'on applique la remarque suivant la proposition 4.1. Il est en outre nécessaire de remarquer que l'algébricité d'un élément de $\mathcal{M}_0(D)$ sur $\mathbb{C}(x)$ équivaut à celle de l'élément de $\mathbb{C}[[X]]$ associé sur $\mathbb{C}(X)$. ∎

Le corollaire 2 peut s'interpréter en disant que l'extension $\mathbb{C}(X)(f)$ sur $\mathbb{C}(X)$ est transcendante pure.

Corollaire 3.

Soit U un élément de $M_{n,1}\left(\mathcal{M}(D)\right)$, solution de l'équation :

$$U = A\mu(U),$$

où A appartient à $M_n\left(\mathbb{C}(x)\right)$.

Les composantes de U qui ne sont pas dans $\mathbb{C}(x)$ admettent le cercle unité pour frontière naturelle, et sont toutes transcendantes sur $\mathbb{C}(x)$.

Preuve.

L'on sait en effet que les composantes de U vérifient toutes une équation de Mahler sur $\mathbb{C}(x)$.∎

5 Majoration des coefficients.

Soit U un élément de $M_{n,1}\left(\mathcal{M}_0(D)\right)$, solution de l'équation :

$$U = A\mu(U), \text{ où } A \in M_{n,n}\left(\mathcal{M}_0(D)\right).$$

D'après la proposition 4.2, la fonction U est holomorphe sur le disque $D\left(0,\rho_0\right)$, où ρ_0 est égal à min(1,d), d désignant la distance de 0 à l'ensemble des pôles de A.

Supposons que d est supérieur ou égal à 1; le rayon de convergence de la série entière précédente est alors supérieur ou égal à 1; s'il est strictement supérieur,

le théorème Antoine et Claudia nous dit que U appartient à $M_n(\mathbb{C}(x))$. Limitons-nous donc au cas où il est égal à 1.

Lorsque W est une fonction bornée sur $D'(0,\rho)$, où $\rho \in [0,1[$, nous noterons $||W||_\rho$ sa norme uniforme sur $D'(0,\rho)$. Nous avons :

$$||U||_\rho \leq ||A||_\rho \, ||U||_\rho \rho^k.$$

Soit à présent un réel r de [0,1[, et fixons un ρ quelconque dans [0,1[; si $r \geq \rho$, il existe un unique entier naturel j tel que :

$$r\rho^{j+1} \leq \rho < r\rho^j .$$

On a alors :

$$||U||_r \leq ||A||_r \, ||A||_{r\rho} \ldots\ldots ||A||_{r\rho^{j+2}} \, ||U||_{r\rho^{j+1}} \text{ et donc :}$$

$$||U||_r \leq ||A||_r \, ||A||_{r\rho} \ldots\ldots ||A||_{r\rho^{j+1}} ||U||_\rho ||A||_\rho^{\,2} .$$

Notons $v_k(r)$ le réel $\ln ||A||_{r\rho^k}$, et posons :

$$S_k = \sum_{i=0}^{k} v_i \ (r).$$

On a donc :

$$\ln\left(||U||_r \right) \leq S_{j+1} + \ln\left(||U||_\rho \right) + 2 \ln\left(||A||_\rho \right).$$

A présent, supposons que A est à coefficients dans $\mathbb{C}(x)$.

∴ Plaçons -nous dans l'hypothèse où il existe un entier strictement positif m et un réel r_0 tels que :

$$\forall \ z \in [r_0,1[\qquad ||A||_z \leq (1-z)^{-m}.$$

Lemme.

Si : $r\rho^k \geq r_0$, alors :

$$\sum_{i=0}^{k} v_i(r) \qquad \leq \quad -m \ln(1-r) - \frac{m}{\ln \rho} \int_h^{\rho^{k-1}h} \ln(1-e^y) \, \frac{dy}{y} ,$$

où l'on a posé : h = ln r.

Preuve.

On a :

$$v_i(r) \leq \ -m \ \ln\left(1 - r\rho^i \right).$$

Majorons la somme proposée en la comparant à l'intégrale de l'application ϕ :

$$t \longmapsto -m \ln\left(1 - r^{p^t}\right),$$

qui décroît sur $[0 , +\infty [$.

On obtient ainsi :

$$\sum_{i=0}^{k} v_i(r) \leq \phi(0) + \int_0^{k-1} \phi(t)\, dt .$$

Le changement de variable $p^t \ln r = y$ conduit à l'égalité :

$$\int_0^{k-1} \phi(t)\, dt = \frac{-m}{\ln p} \int_h^{p^{k-1}h} \ln(1-e^y)\, \frac{dy}{y},$$

où l'on a posé : $h = \ln r$.

Lorsque h tend vers 0, on a :

$$\int_h^{-\infty} \ln(1-e^y)\, \frac{dy}{y} = \int_h^{-1} \ln(-y)\, \frac{dy}{y} + O(1) , \text{ soit :}$$

$$\int_h^{-\infty} \ln(1-e^y)\, \frac{dy}{y} = -\frac{1}{2}[\ln(-h)]^2 + O(1).$$

Fixons ρ égal à r_0 ; si r est plus grand que r_0, on peut écrire :

$$\ln\left(\|U\|_r\right) \leq S_{j+1} + \ln\left(\|U\|_\rho\right) + 2\ln\left(\|A\|_\rho\right)$$

$$\leq -m \ln(1-r) - \frac{m}{\ln p} \int_h^{+\infty} \ln(1-e^y)\, \frac{dy}{y} + \ln\left(\|U\|_\rho\right) + 2\ln\left(\|A\|_\rho\right)$$

$$\leq -m \ln(1-r) + \frac{m}{2\ln p}[\ln(-h)]^2 + O(1), \text{ pour r tendant vers } 1^- .$$

Comme $h = \ln r$, on obtient :

$$\ln\left(\|U\|_r\right) = O((\ln(1-r))^2).$$

$\therefore$ Examinons à présent le cas où m est nul. La majoration :

$$\|U\|_r \leq \|A\|_r \|A\|_{rp} \ldots\ldots \|A\|_{rp^{j+2}} \|U\|_{rp^{j+1}}$$

devient alors :

$$\|U\|_r \leq a^{j+3} \|U\|_\rho,$$

où a est un majorant de $||A||_r$ pour $r < 1$. On suppose en outre : $a>1$.
Compte tenu des inégalités :

$$r^{p^{j+1}} \leq \rho < r^{p^j},$$

il vient :

$$p^j \leq \frac{\ln \rho}{\ln r},$$

et donc :

$$a^{j+3} \leq \exp\left(\left(\frac{1}{\ln p} \ln \frac{\ln \rho}{\ln r} + 3\right) \ln a\right),$$

d'où finalement :

$$||U||_r \leq C \frac{1}{(\ln r)^k},$$

avec :

$$C = ||U||_\rho \exp\left(\left(\frac{1}{\ln p} \ln \ln \rho + 3\right) \ln a\right),$$

$$\text{et } k = \frac{\ln a}{\ln p}.$$

En résumé :

<u>Proposition 4.3</u>

Soit U un élément de $M_{n,1}\left(\mathcal{M}_0(D)\right)$, solution de l'équation :

$$U = A\mu(U), \text{ où } A \in M_{n,n}\left(\mathbb{C}(x)\right).$$

On note d la distance de O à l'ensemble des pôles de A, avec, par convention, $d = +\infty$ si A n'a pas de pôle.

Si $d > 1$, il existe un réel k tel que :

$$||U||_r = O\left(\frac{1}{(1-r)^k}\right)$$

1^-

Si $d = 1$, on a :

$$\ln\left(\|U\|_r\right) = \underset{1^-}{O}\left([\ln(1-r)]^2\right).$$

Nous pouvons appliquer la proposition précédente en vue d'obtenir une majoration du coefficient u_n du développement en série entière de U. Partons de l'inégalité :

$$|u_n| \leq \inf_{r<1}\left\{\frac{1}{r^n}\|U\|_r\right\}.$$

Supposons tout d'abord que : d > 1, et prenons $r = 1-\frac{1}{n}$. Il vient :

$$u_n = \underset{+\infty}{O}\left(n^k\right).$$

Cette situation se présente en particulier lorsque (u_n) est une suite p-régulière.

Si l'on suppose que d est égal à 1, la majoration fournie par la proposition 4.3. nous donne :

$$\|U\|_r \leq \exp\left[M(\ln(1-r))^2\right], \text{ et donc :}$$

$$|u_n| \leq \exp\left[M(\ln(1-r))^2 - n \ln r\right].$$

En utilisant toujours : $r = 1-\frac{1}{n}$, on obtient :

$$|u_n| \leq \exp\left[M(\ln n)^2\right].$$

Chapitre 5.

La notion d'équation différentielle algébrique s'est naturellement introduite en suivant le courant de l'algébrisation de l'analyse que connut le dix-neuvième siècle. C'est la période qui, à la suite des travaux approfondis sur les équations algébriques, voit le calcul formel s'attacher à interpréter les identités, et autres équations différentielles, satisfaites par les fonctions de l'analyse classique ; ce n'est probablement pas un hasard complet si c'est à Liouville, l'un des inventeurs de Galois, que l'on doit des résultats déjà élaborés à ce sujet. La première fonction que l'on a démontrée être différentiellement transcendante est la fonction gamma [3] : il n'y a rien de surprenant à ce que l'on ait dû faire appel à cette fonction, puisque toutes les fonctions "élémentaires" vérifient une équation différentielle algébrique sur $\mathbb{C}(x)$. La preuve, en ce qui concerne la fonction gamma, repose sur l'équation fonctionnelle qu'elle vérifie.

Dans ce chapitre, nous nous consacrerons à la différentielle algébricité de solutions d'équations de Mahler, en premier lieu dans l'optique générale de ce travail, qui s'intéresse en particulier aux questions de transcendance, et aussi en vue de répondre à une question posée par Rubel [4], concernant une fonction qui se trouve vérifier une telle équation.

Il est bon de remarquer que les techniques "analytiques" du chapitre 4 ne permettent pas de montrer qu'une fonction, solution d'une équation de Mahler, est différentiellement algébrique sur $\mathbb{C}(x)$ au simple vu de ses singularités : il existe en effet des fonctions différentiellement algébriques qui admettent le cercle unité comme frontière naturelle [8]. Aussi bien, nous obtiendrons dans cette direction des résultats moins généraux.

La proposition 5.1 donne une condition nécessaire sur l'élément a d'un corps différentiel pour qu'une solution f de la p-équation de Mahler, linéaire et d'ordre un : $f = a\mu_p(f)$, soit différentiellement algébrique sur ce corps. Nous appliquerons ce résultat au cas où le corps différentiel est $\mathbb{C}(x)$, pour obtenir le résultat espéré : si f est différentiellement algébrique sur $\mathbb{C}(x)$, c'est elle même une fraction rationnelle (théorème 5.1). La difficulté technique principale vient du fait que, contrairement à la situation qui se présente dans le cas de la fonction gamma, il n'y a pas linéarité par rapport à la variable ; ceci contraint à un changement de variable, qui d'ailleurs motive le cadre du chapitre : celui des fonctions méromorphes. On ne dispose en effet pas nettement de cette possibilité dans le cadre général des séries formelles.

Une méthode de variation de la constante permet de généraliser le résultat précédent au cas d'équations affines, sous réserve qu'elles aient assez de solutions

(théorème 5.2). Quelques équations mahlériennes, algébriques, et surtout ad hoc, illustrent ces résultats.

Les résultats sur les équations différentielles algébriques qu'utilise ce chapitre sont regroupés dans les annexes 2 et 3.

1 Position du problème.

Le cadre général de ce chapitre est celui du chapitre 4. Le corps de base est donc $\mathbb{C}$. Les corps considérés seront des sous-corps de $\mathcal{M}(D)$, où D est un ouvert connexe de $\mathbb{C}$, qui en particulier pourra être égal à Δ, disque unité ouvert, ou à $\prod$, demi-plan des complexes de partie réelle strictement négative. On désignera par $\mathcal{K}$ un sous-corps différentiel de $\mathcal{M}(\Delta)$, p-mahlérien.

On considèrera aussi l'élément exp de $\mathcal{M}(\prod)$, défini de la manière usuelle.

Soit f un élément non nul de $\mathcal{M}(\Delta)$, solution de l'équation de Mahler d'ordre un sur $\mathcal{K}$ suivante :

$$f = a\ \mu_p(f).$$

Une autre relation vérifiée par f est :

$$\frac{f'}{f} = \frac{a'}{a} + px^{p-1}\frac{f'(x^p)}{f(x^p)},$$

et donc :

$$x\frac{f'}{f} = x\frac{a'}{a} + px^p\frac{f'(x^p)}{f(x^p)}.$$

Dans $\mathcal{M}(\prod)$, on a alors :

$$e^t\frac{f'(e^t)}{f(e^t)} = e^t\frac{a'(e^t)}{a(e^t)} + pe^{pt}\frac{f'(e^{pt})}{f(e^{pt})}.$$

Posons :

$$g = e^t\frac{f'(e^t)}{f(e^t)}.$$

C'est un élément de $\mathcal{M}(\prod)$, qui vérifie l'égalité :

$$(1) \qquad g(t) = pg(pt) + R_0(t),$$

où $R_0(t)$ est un élément de $\mathcal{K}\circ\exp$, égal à : $e^t\frac{a'(e^t)}{a(e^t)}$.

On pose : $S_0(x) = x\frac{a'(x)}{a(x)}$, de façon que : $R_0(t) = S_0(e^t)$.

Nous noterons $\mathcal{L}$ le corps $\mathcal{K}\circ\exp$. C'est un corps différentiel, stable par l'application .

$$\nu : h(t) \longmapsto h(pt).$$

L'application ν joue , vis-à-vis de $\mathcal{L}$, le même rôle que l'application μ vis-à-vis de $\mathcal{K}$.

Pour la commodité des écritures, nous préfèrerons le plus souvent, mais pas systématiquement, noter h^{ν} l'image de l'élément h de $\mathcal{M}(\prod)$ par ν .

On cherche à déterminer les éléments f de $\mathcal{M}(\Delta)$ qui sont différentiellement algébriques sur $\mathcal{K}$. On fait donc à présent l'hypothèse que f est différentiellement algébrique sur $\mathcal{K}$. Il en résulte que g est différentiellement algébrique sur $\mathcal{L}$.

2 Une condition nécessaire de différentielle algébricité.

Soit P, élément de $\mathcal{L}\left[Y_0,\ldots,Y_n\right]$, un polynôme minimal de g sur $\mathcal{L}$. On suppose en outre que P est normalisé. Nous disposons de l'égalité :

$$P\left(g,\ g',\ldots,\ g^{(n)}\right) = 0,$$

d'où aussi :

$$(2) \qquad P^{\nu}\left(g^{\nu},\ (g')^{\nu},\ldots,\ \left(g^{(n)}\right)^{\nu}\right) = 0.$$

Or, d'après l'égalité (1), on a :

$$g^{\nu} = \frac{1}{p}\left(g - R_0\right).$$

Il en résulte que, pour tout entier naturel k, on a :

$$\left(g^{\nu}\right)^{(k)} = \frac{1}{p}\left(g^{(k)} - R_k\right),$$

où l'on a posé :

$$R_k = R_0^{(k)}.$$

Par ailleurs, on a, évidemment :

$$\left(g^{\nu}\right)^{(k)} = p^k\left(g^{(k)}\right)^{\nu}.$$

On obtient finalement :

$$\left(g^{(k)}\right)^{\nu} = \frac{1}{p^{k+1}}\left(g^{(k)} - R_k\right).$$

Reportons ces égalités dans la relation de liaison (2) ; il vient :

$$P^{\nu}\left(\frac{1}{p}\left(g-R_0\right),\ldots,\ \frac{1}{p^{n+1}}\left(g^{(n)}-R_n\right)\right)=0.$$

Posons alors :

$$Q\left(Y_0,\ldots,Y_n\right)=P^{\nu}\left(\frac{1}{p}\left(Y_0-R_0\right),\ldots,\ \frac{1}{p^{n+1}}\left(Y_n-R_n\right)\right).$$

Il est clair que Q, qui est un élément de $\mathcal{L}\left[Y_0,\ldots,Y_n\right]$, est inférieur ou égal à P. Ces deux polynômes sont donc proportionnels ; soit :

$$\text{il existe } \lambda \text{ dans } \mathcal{L} \text{ tel que : } P^{\nu}\left(\frac{1}{p}\left(Y_0-R_0\right),\ldots,\ \frac{1}{p^{n+1}}\left(Y_n-R_n\right)\right)=\lambda P.$$

Lemme 1.

Soient $D_0,\ldots,D_n$ des opérateurs différentiels sur $L\left[Y_0,\ldots,Y_n\right]$ et d'ordre un, linéairement indépendants sur L, où L est un corps de caractéristique nulle, et P un élément non constant de $L\left[Y_0,\ldots,Y_n\right]$. Il existe alors une famille $\left(i_1,\ldots,i_k\right)$ d'éléments de [0,n] telle que $D_{i_1}\ldots D_{i_k}(P)$ soit un polynôme affine non constant.

Preuve.

Raisonnons par récurrence sur P.

∴ Supposons tout d'abord que, quel que soit i, $D_i(P)$ est constant. Dans ce cas, puisque la famille $\left(D_0,\ldots,D_n\right)$ est une base de l'espace vectoriel des opérateurs différentiels d'ordre un, quel que soit i, le polynôme $\frac{\partial P}{\partial Y_i}$ est constant. Il en découle immédiatement que P est affine.

∴ Dans le cas contraire, il existe un i tel que $D_i(P)$ n'est pas constant ; comme $D_i(P)$ est strictement plus petit que P, le résultat en suit.∎

Reprenons l'égalité :

$$P^{\nu}\left(\frac{1}{p}\left(Y_0-R_0\right),\ldots,\ \frac{1}{p^{n+1}}\left(Y_n-R_n\right)\right)=\lambda P.$$

Soit i un entier compris entre 0 et n ; appliquons à l'égalité précédente l'opérateur $\frac{\partial}{\partial Y_i}$; il vient :

$$\frac{1}{p^{i+1}}\frac{\partial P^{\nu}}{\partial Y_i}\left(\frac{1}{p}(Y_0-R_0),\ldots,\ \frac{1}{p^{n+1}}\ (Y_n-R_n)\right) = \lambda\frac{\partial P}{\partial Y_i}.$$

Cela signifie que le polynôme $\dfrac{\partial P}{\partial Y_i}$ satisfait une relation analogue à celle vérifiée par P, à ceci près que λ est remplacé par λp^{i+1}.

Par récurrence, on constate que tout polynôme $\dfrac{\partial^k P}{\partial Y_{i_1}\ldots\partial Y_{i_k}}$ vérifie une relation analogue, et ce quel que soit le k-uplet $(i_1,\ldots,i_k)$ d'éléments de [0,n].

Comme P n'est pas le polynôme nul, ce n'est pas un polynôme constant. On peut donc lui appliquer le lemme 1 ; notant S le polynôme $\dfrac{\partial^k P}{\partial Y_{i_1}\ldots\partial Y_{i_k}}$ correspondant, on obtient l'égalité :

$$S^{\nu}\left(\frac{1}{p}(Y_0-R_0),\ldots,\ \frac{1}{p^{n+1}}\ (Y_n-R_n)\right) = \delta S,$$

où est δ un élément de $\mathfrak{L}$.

Le polynôme S étant affine et non constant, on pose :

$$S(Y_0,\ldots,Y_n) = \sum_{i=0}^{n} s_i Y_i + s, \quad \text{avec l'un des } s_i \text{ non nul.}$$

L'égalité devient :

$$\sum_{i=0}^{n} \nu(s_i)\frac{1}{p^{i+1}}(Y_i-R_i) + \nu(s) = \delta\left(\sum_{i=0}^{n} s_i Y_i + s\right).$$

Il en résulte :

$$\forall\ i \in [0,n] \quad \frac{1}{p^{i+1}}\nu(s_i) = \delta s_i \qquad \text{et}$$

$$-\sum_{i=0}^{n} \nu(s_i)\frac{1}{p^{i+1}}R_i + \nu(s) = \delta\ s\ .$$

Lemme 2.

Soit c un complexe différent de 1. L'équation :

$$\nu(u) = cu$$

à l'inconnue u de $\mathfrak{L}$ n'admet que la solution nulle.

Preuve.

Il revient au même de montrer que l'équation : $\mu(w) = cw$ à l'inconnue w de $\mathcal{K}$ n'admet que la solution nulle. Cela résulte de la proposition 1.1.

Supposons alors qu'il existe deux indices i et j tels que s_i et s_j soient non nuls; on obtient, puisqu'alors δ est nécessairement non nul :

$$v\left(\frac{s_i}{s_j}\right) = p^{i-j}\,\frac{s_i}{s_j},$$

et ceci contredit le lemme 2.

Il existe donc exactement un indice, que l'on note k, tel que s_k soit non nul .

La condition nécessaire précédemment obtenue devient :

$$\frac{1}{p^{k+1}}\,v\left(s_k\right) = \delta\, s_k\,;\; -v\left(s_k\right)\frac{1}{p^{k+1}}\,R_k + v(s) = \delta\; s\,;$$

d'où, si l'on pose : $S = \frac{s}{s_k}$, on obtient :

$$-\frac{1}{p^{k+1}}\,R_k + v(S) = \frac{1}{p^{k+1}}\,S\,.$$

Revenant à $\mathcal{K}$, on parvient au résultat suivant :

Proposition 5.1.

Soient $\mathcal{K}$ un sous-corps différentiel p-mahlérien de $\mathcal{M}(\Delta)$, et f un élément non nul de $\mathcal{M}(\Delta)$, solution de l'équation de Mahler d'ordre un sur $\mathcal{K}$ suivante :

$$f = a\;\mu_p(f).$$

Posons : $S_0(x) = x\,\frac{a'}{a}$, et : $S_k(x) = x\,S'_{k-1}(x)$ pour k entier naturel non nul.

Si f est différentiellement algébrique sur $\mathcal{K}$, il existe un élément w de $\mathcal{K}$ et un entier naturel k tels que :

$$-\frac{1}{p^{k+1}}\,S_k + \mu(w) = \frac{1}{p^{k+1}}\;w\,.$$

Preuve.

Rappelons que : $R_k = R_0^{(k)}$. Or : $R_0(t) = S_0(e^t)$. Donc :

$$R_k(t) = R'_{k-1}(t) = \frac{d}{dt}\left(S_{k-1}(e^t)\right) = e^t\,S'_{k-1}(e^t) = S_k(e^t).$$

Ainsi, la relation :

$$-\frac{1}{p^{k+1}} R_k + \nu(S) = \frac{1}{p^{k+1}} S$$

devient :

$$-\frac{1}{p^{k+1}} S_k + \mu(w) = \frac{1}{p^{k+1}} \quad w, \text{ lorsque : } w(e^t) = S(t).\blacksquare$$

3. Cas où : $\mathcal{K} = \mathbb{C}(x)$.

Nous désignons ici par $\mathbb{C}(x)$ le sous-corps de $\mathcal{M}(\Delta)$ formé des fonctions fractions rationnelles sur Δ. Le degré d'une fraction rationnelle est la différence des degrés du numérateur et du dénominateur, lorsque elle est non nulle. On le pose égal à $-\infty$ si la fraction est nulle. On note $\mathbb{C}_d(x)$ le espace vectoriel formé des fractions rationnelles de degré inférieur ou égal à d, et de même pour $\mathbb{C}_d[x]$.

Lemme 1.

Soit $\mathcal{M}$ le sous-espace vectoriel de $\mathbb{C}(x)$ engendré par $\left\{\frac{1}{(x-\alpha)^n} \ , \ \alpha\in\mathbb{C}, n\in\mathbb{N}, n\geq 2\right\}$, et $\mathcal{S}$ le sous-espace vectoriel de $\mathbb{C}(x)$ engendré par $\left\{\frac{1}{x-\alpha} \ , \ \alpha\in\mathbb{C}\right\}$. Si d est un entier naturel, on dispose alors de la somme directe :

$$\mathbb{C}_d(x) = \mathcal{M}\oplus\mathcal{S}\oplus\mathbb{C}_d[x].$$

Preuve.

C'est l'expression du théorème de décomposition en éléments simples dans $\mathbb{C}(x)$.$\blacksquare$

Lemme 2.

Si d est un entier naturel, l'image par la dérivation de l'espace vectoriel $\mathbb{C}_d(x)$ est $\mathcal{M}\oplus\mathbb{C}_{d-1}[x]$.

Preuve.

Il suffit de regarder l'image par la dérivation de chacun des éléments simples de $\mathbb{C}(x)$.$\blacksquare$

Lemme 3.

L'espace vectoriel $\mathfrak{M}$ est stable par l'application :

$$R \longmapsto x^{p-1} R\left(x^p\right).$$

Preuve.

D'après le lemme 2, un élément R de $\mathfrak{M}$ est de la forme :

$R(x) = S'(x)$, où S appartient à $\mathbb{C}(x)$.

Donc: $x^{p-1} R\left(x^p\right) = x^{p-1} S'\left(x^p\right) = \frac{1}{p} \frac{d}{dx}\left(S\left(x^p\right)\right)$.

Puisque $S\left(x^p\right)$ appartient à $\mathbb{C}(x)$, le lemme 2, à nouveau, conclut.∎

Lemme 4.

L'espace vectoriel $\mathfrak{S}$ est stable par l'application :

$$R \longmapsto x^{p-1} R\left(x^p\right).$$

Preuve.

Soit α un élément de $\mathbb{C}$, et R, égal à $\frac{1}{x-\alpha}$, un élément de la base canonique de $\mathfrak{S}$. On a :

$$x^{p-1} R\left(x^p\right) = x^{p-1} \frac{1}{x^p-\alpha}.$$

Si α est nul, le calcul est immédiat ; dans le cas contraire, soit $R_p\left(\alpha\right)$, abrégé en R_p, l'ensemble des racines p-ièmes de α. On a :

$$x^{p-1} \frac{1}{x^p-\alpha} = \frac{1}{p} \sum_{\omega \in R_p} \frac{1}{x-\omega},$$

ce qui donne le résultat.∎

A présent, appliquons la proposition 5.1, et partons de l'égalité :

(1) $\quad S_k = p^{k+1} \mu(w) - w$, avec w dans $\mathbb{C}(x)$.

Nous allons montrer que, si la relation (1) est vraie pour un entier naturel non nul, noté encore k pour la simplicité, elle est vérifiée pour k-1.

Puisque : $S_k(x) = x\, S'_{k-1}(x)$, on a aussi :

$$S'_{k-1}(x) = \frac{1}{x} p^{k+1} w\left(x^p\right) - \frac{1}{x} w(x).$$

Puisque S_0 est de degré 0, il est clair, par recurrence, que S_k est aussi de degré 0. Posons : $z(x) = \frac{1}{x} w(x)$. On a :

$$S'_{k-1}(x) = x^{p-1} p^{k+1} z\left(x^p\right) - z(x).$$

Le degré de z est nécessairement strictement négatif ; car, s'il était positif ou nul, le degré du membre de droite serait strictement positif. Appelons z_1 le projeté de z sur $\mathfrak{M}$ parallèlement à $\mathfrak{S}$, z_2 son projeté sur $\mathfrak{S}$ parallèlement à $\mathfrak{M}$. Il vient :

$$S'_{k-1}(x) = x^{p-1} p^{k+1} z_1\left(x^p\right) - z_1(x) + x^{p-1} p^{k+1} z_2\left(x^p\right) - z_2(x).$$

Or, d'après le lemme 2, $S'_{k-1}(x)$ est dans $\mathfrak{M}$.

Grâce au lemme 3, l'élément $x^{p-1} p^{k+1} z_1\left(x^p\right) - z_1(x)$ est dans $\mathfrak{M}$, tandis que $x^{p-1} p^{k+1} z_2\left(x^p\right) - z_2(x)$ est dans $\mathfrak{S}$ d'après le lemme 4. Il en résulte :

$$S'_{k-1}(x) = x^{p-1} p^{k+1} z_1\left(x^p\right) - z_1(x).$$

Mais, d'après le lemme 2 encore, il existe un élément v de $\mathbb{C}(x)$ tel que : $z_1 = v'$; il découle de cela l'égalité :

$$S'_{k-1}(x) = p^k \frac{d}{dx}\left(v\left(x^p\right)\right) - v'(x), \text{ puis :}$$

$$S_{k-1}(x) = p^k v\left(x^p\right) - v(x) + c,$$

où c est dans $\mathbb{C}$.

Posons alors : $v_1 = v + \frac{c}{1-p^k}$. On obtient de suite :

$$S_{k-1}(x) = p^k v_1\left(x^p\right) - v_1(x),$$

ce qui était le but recherché.

Il résulte de cette récurrence qu'il existe une fraction rationnelle y de $\mathbb{C}(x)$ telle que :

$$S_0(x) = p\, y\left(x^p\right) - y(x),$$

soit encore, compte tenu de l'expression de S_0 :

$$(2) \qquad x \frac{a'}{a} = p\, y\left(x^p\right) - y(x).$$

Remarquons en outre que y n'a pas le pôle 0 ; en effet, dans le cas contraire, le membre de droite de (2) aurait le pôle 0, ce qui n'est pas le cas de son membre de gauche.

Notations.

Soit F un élément de $\mathbb{C}(x)$; nous noterons $F(n,\alpha)$ le coefficient de $\frac{1}{(x-\alpha)^n}$ dans la décomposition en éléments simples de F, de sorte que :

$$F(x) = \sum_{\alpha\in\mathbb{C},n\in\mathbb{N}^*} \frac{F(n,\alpha)}{(x-\alpha)^n}) + c,$$

où c appartient à $\mathbb{C}$. Ainsi, la famille des $F(n,\alpha)$ est à support fini.

Ecrivons d'autre part :

$$a(x) = \prod_{\alpha\in\mathbb{C}} (x-\alpha)^{m(\alpha)},$$

où $(m(\alpha))_{\alpha\in\mathbb{C}}$ est une famille à support fini d'éléments de$\mathbb{Z}$ Il vient alors, grâce à une dérivation logarithmique :

$$\frac{a'(x)}{a(x)} = \sum_{\alpha\in\mathbb{C}} \frac{m(\alpha)}{x-\alpha}, \text{ et donc :}$$

$$x\,\frac{a'(x)}{a(x)} = \sum_{\alpha\in\mathbb{C}} \frac{\alpha m(\alpha)}{x-\alpha} + d, \text{ où d est dans } \mathbb{C}.$$

Avec ces notations, l'égalité (2) devient :

$$\sum_{\alpha\in\mathbb{C}} \frac{\alpha m(\alpha)}{x-\alpha} + d = p \sum_{\alpha\in\mathbb{C},n\in\mathbb{N}^*} \frac{y(n,\alpha)}{(x^p-\alpha)^n} - \sum_{\alpha\in\mathbb{C},n\in\mathbb{N}^*} \frac{y(n,\alpha)}{(x-\alpha)^n} + (p-1)c,$$

soit encore, en projetant si $\mathfrak{M}\oplus\mathfrak{S}$ parallèlement à $\mathbb{C}[x]$:

$$(3) \qquad \sum_{\alpha\in\mathbb{C}} \frac{\alpha m(\alpha)}{x-\alpha} = p \sum_{\alpha\in\mathbb{C},n\in\mathbb{N}^*} \frac{y(n,\alpha)}{(x^p-\alpha)^n} - \sum_{\alpha\in\mathbb{C},n\in\mathbb{N}^*} \frac{y(n,\alpha)}{(x-\alpha)^n}.$$

Lemme 5.

Soit α un complexe non nul. On note R_p l'ensemble des racines p-ièmes de α Si n est un entier naturel non nul, on a :

$$\frac{1}{(x^p-\alpha)^n} = \sum_{\omega\in R_p} \left(\frac{\omega}{p\alpha}\right)^n \frac{1}{(x-\omega)^n} + \ldots\ldots,$$

les points de suspension désignant la partie polaire relative aux ordres de multiplicité inférieurs ou égaux à n-1.

Preuve.

Comme d'habitude, le coefficient de $\frac{1}{(x-\omega)^n}$ est égal à :

$$\left\{\left[\frac{d}{dx}\left((x^p-\alpha)^n\right)\right]_{x=\omega}\right\}^{-1}, \text{ soit : } \left(\frac{\omega}{p\alpha}\right)^n.\blacksquare$$

Nous montrerons à présent que, si n n'est pas égal à 1, et si α n'est pas nul, $y(n,\alpha)$ est nul. Pour cela, nous raisonnons par l'absurde, et nous considérons un entier n, supérieur ou égal à 2, minimal pour la propriété :

il existe un complexe non nul β tel que : $y(m,\beta) \neq 0$.

L'égalité (3) nous donne, par considération de la partie polaire d'ordre n, relative à tous les complexes non nuls, et par application du lemme 5 :

$$0 = p \sum_{\alpha\in\mathbb{C}^*} y(n,\alpha) \sum_{\omega^p=\alpha} \left(\frac{\omega}{p\alpha}\right)^n \frac{1}{(x-\omega)^n} - \sum_{\alpha\in\mathbb{C}^*} \frac{y(n,\alpha)}{(x-\alpha)^n}.$$

Examinons la partie polaire relative à un complexe non nul donné ; l'égalité précédente peut se réécrire :

$$0 = p \sum_{\beta\in\mathbb{C}^*} y(n,\beta) \sum_{\omega^p=\beta} \left(\frac{\omega}{p\beta}\right)^n \frac{1}{(x-\omega)^n} - \sum_{\alpha\in\mathbb{C}^*} \frac{y(n,\alpha)}{(x-\alpha)^n},$$

soit encore :

$$0 = p \sum_{\alpha \in \mathbb{C}^*} y(n,\alpha^p) \left(\frac{\alpha}{p\alpha^p}\right)^n \frac{1}{(x-\alpha)^n} - \sum_{\alpha \in \mathbb{C}^*} \frac{y(n,\alpha)}{(x-\alpha)^n}.$$

Il en résulte :

$$\forall\, \alpha \in \mathbb{C}^* \quad 0 = p\, y(n,\alpha^p) \left(\frac{\alpha}{p\alpha^p}\right)^n - y(n,\alpha).$$

Nous allons exploiter cette égalité à l'aide du lemme suivant :

Lemme 6.

Soient ϕ une application de $\mathbb{C}^*$ dans $\mathbb{C}$, à support fini, et un complexe k, vérifiant :

$$\forall\, \alpha \in \mathbb{C}^* \quad \phi(\alpha) = k\, \phi(\alpha^p).$$

L'application ϕ est alors nulle.

Preuve.

Soit x un complexe non nul ; il existe m tel que p^m soit strictement plus grand que le cardinal du support de ϕ. Soit α une racine p^m -ième de x, telle que $\phi(\alpha)$ soit nul ; puisque :

$$\phi(\alpha) = k^m\, \phi(\alpha^{p^m}) = k^m\, \phi(x) = 0,$$

on a de suite : $\phi(x) = 0$, le cas où k est nul étant trivial.∎

Appliquons le lemme 6 à l'égalité :

$$\forall\, \alpha \in \mathbb{C}^* \quad 0 = p\, y(n,\alpha^p) \left(\frac{\alpha}{p\alpha^p}\right)^n - y(n,\alpha)$$

qui s'écrit aussi :

$$\forall\, \alpha \in \mathbb{C}^* \quad \phi(\alpha) = k\, \phi(\alpha^p),$$

lorsque l'on a posé : $\phi(\alpha) = \dfrac{y(n,\alpha)}{\alpha^n}$ et $k = \dfrac{1}{p^{n-1}}$.

Puisque $\alpha \mapsto \dfrac{y(n,\alpha)}{\alpha^n}$ est à support fini, on a :

$\forall\, \alpha \in \mathbb{C}^* \quad y(n,\alpha) = 0$, ce qui est la contradiction souhaitée.

Exploitons à présent la relation (3), qui se présente, compte tenu du résultat précédent, sous la forme suivante :

$$\sum_{\alpha\in\mathbb{C}} \frac{\alpha m(\alpha)}{x-\alpha} = p \sum_{\alpha\in\mathbb{C}} \frac{y(1,\alpha)}{x^p-\alpha} - \sum_{\alpha\in\mathbb{C}} \frac{y(1,\alpha)}{x-\alpha},$$

et qui fournit la relation :

$$\forall\ \alpha \in \mathbb{C}^* \qquad \alpha m(\alpha) = y(1,\alpha^p)\ \frac{\alpha}{\alpha^p} - y(1,\alpha),$$

soit encore, en posant :

$\zeta(\alpha) = \dfrac{y(1,\alpha)}{\alpha}$, la relation :

$$\forall\ \alpha \in \mathbb{C}^* \qquad m(\alpha) = \zeta(\alpha^p) - \zeta(\alpha).$$

Lemme 7.

Soit ζ une application de $\mathbb{C}^*$ dans $\mathbb{C}$, à support fini, et ψ une application de $\mathbb{C}^*$ dans H, sous-groupe additif de $\mathbb{C}$. On suppose que :

$$\forall\ \alpha \in \mathbb{C}^* \qquad \psi(\alpha) = \zeta(\alpha^p) - \zeta(\alpha).$$

L'application ζ est alors à valeurs dans H.

Preuve.

Soit x un élément de $\mathbb{C}^*$. Il existe s tel que p^s soit strictement plus grand que le cardinal du support de ζ. Soit α une racine p^s -ième de x, telle que $\zeta(\alpha)$ soit nul ; on a :

$$\sum_{k=0}^{s-1} \psi(\alpha^{p^k}) = \sum_{k=0}^{s-1} \left(\zeta(\alpha^{p^{k+1}}) - \zeta(\alpha^{p^k})\right),$$

et donc :

$$\sum_{k=0}^{s-1} \psi(\alpha^{p^k}) = \zeta(x).$$

Le résultat en découle.∎

Le lemme 7 entraîne que l'application ζ est à valeurs dans $\mathbb{Z}$. Revenant à l'expression de la fraction rationnelle y, on obtient :

$$y(x) = \sum_{\alpha\in\mathbb{C}^*} \frac{\alpha\zeta(\alpha)}{x-\alpha} + c\,,$$

ou encore :

$$\frac{y(x)}{x} = -\sum_{\alpha\in\mathbb{C}^*} \frac{\alpha\zeta(\alpha)}{x(x-\alpha)} + \frac{d}{x}\,,$$

avec d élément de $\mathbb{C}$.

Par ailleurs : $\frac{1}{x(x-\alpha)} = \frac{1}{x-\alpha} - \frac{1}{x}$. Donc :

$$\frac{y(x)}{x} = -\sum_{\alpha\in\mathbb{C}^*} \frac{\zeta(\alpha)}{x-\alpha} + \frac{e}{x}.$$

Puisque est à valeurs entières, on constate que $-\sum_{\alpha\in\mathbb{C}^*} \frac{\zeta(\alpha)}{x-\alpha}$ est la dérivée logarithmique d'une fraction rationnelle :

$$-\sum_{\alpha\in\mathbb{C}^*} \frac{\zeta(\alpha)}{x-\alpha} = \frac{q'}{q}.$$

D'où , compte tenu de l'égalité (2) :

$$\frac{a'}{a} = p\frac{y(x^p)}{x} - \frac{y(x)}{x}$$

$$= \frac{p}{x}\frac{q'(x^p)}{q(x^p)} - \frac{q'(x)}{q(x)} + \frac{e}{x^p} - \frac{e}{x}$$

$$= \frac{d}{dx}\Big(q(x^p)\Big)/q(x^p) - \frac{q'(x)}{q(x)} + \frac{e}{x^p} - \frac{e}{x}.$$

Cette égalité implique en particulier que e est nul, puisque les pôles du membre de gauche sont simples. On obtient alors :

$$a(x) = \lambda\,\frac{q(x^p)}{q(x)}\,,$$

où λ est un complexe, et donc, en revenant à l'égalité initiale satisfaite par f :

$$f(x)\,q(x) = \lambda\; f(x^p)\,q(x^p).$$

On a déjà remarqué que cette égalité implique que λ est égal à 1, et que fq est une constante. Donc f est une fraction rationnelle.

Théorème 5.1.

Soient a un élément de $\mathbb{C}(x)$, et f un élément de $\mathcal{M}(\Delta)$ solution de l'équation :

$$f = a\ \mu_p(f).$$

Si f est différentiellement algébrique sur $\mathbb{C}(x)$, f appartient à $\mathbb{C}(x)$.

Illustration.

$\therefore$ Soit f un élément de $\mathcal{M}(\Delta)$, solution de l'équation (non linéaire) :

$$(4) \qquad f\ \mu^2(f) = a\ (\mu(f))^2\ ,$$

où a est un élément de $\mathbb{C}(x)$. Supposons f différentiellement algébrique sur $\mathbb{C}(x)$, et non nul. Soit : $g = \frac{\mu(f)}{f}$; g vérifie :

$$\mu(g) = a\ g\ ;$$

de plus, $\mu(f)$ est, comme f, différentiellement algébrique ; donc g l'est aussi et, par conséquent, g appartient à $\mathbb{C}(x)$. Comme f vérifie l'égalité :

$$\mu(f) = g\ f\ ,$$

f est aussi dans $\mathbb{C}(x)$.

Bien que l'équation (4) n'ait pas été étudiée stricto sensu, l'étude précédente montre qu'en réalité elle se ramène à deux équations d'ordre un. La proposition 4.1. nous dit que, si a(0) = 1, l'équation $\mu(g) = a\ g$ admet une droite de solutions, dont il est aisé de voir qu'elles ne s'annulent pas en 0 (sauf la solution nulle). Il en existe donc une à vérifier : g(0) = 1, et par conséquent l'ensemble des solutions f est une droite.

Dans le cas général, on peut utiliser la proposition 1.1, ou plutôt son analogue méromorphe, qui n'a pas été démontré mais qui relève aisément de la méthode du théorème 4.1. Nécessairement, si (4) admet une solution non nulle, on peut écrire :

$$a(x) = x^{\alpha}\ a_1(x)\ ,\ \text{avec} : a_1(0) = 1 \text{ et } \alpha \text{ multiple de } p-1.$$

On obtient ainsi :

$$g(x) = x^{\frac{\alpha}{p-1}} \phi(x), \qquad \text{avec } \phi(0) = 1.$$

Il est alors nécessaire que, à nouveau, p -1 divise $\frac{\alpha}{p-1}$. Les conditions sont alors suffisantes. En résumé :

Proposition 5.2.

Soit a un élément non nul de $\mathbb{C}(x)$, et l'équation à l'inconnue f dans $\mathcal{M}(\Delta)$:

(4) $\qquad f\ \mu^2(f) = a\ (\mu(f))^2$.

Pour que l'équation (a) admette une solution non nulle, il faut et il suffit que l'on puisse écrire :

$$a(x) = x^{\alpha}\, a_1(x)\,, \text{ avec : } a_1(0) = 1 \text{ et } \alpha \text{ multiple de } (p-1)^2.$$

L'ensemble des solutions est alors une droite.

De plus, les solutions sont, soit différentiellement transcendantes sur $\mathbb{C}(x)$, soit dans $\mathbb{C}(x)$.

∴ Considérons la fonction f définie par l'égalité :

$$f(x) = \prod_{k=0}^{+\infty} \left(1+x^{3^k}\right).$$

Ainsi, $f(x) = (1+x)\ f\left(x^3\right)$.

Si f était différentiellement algébrique, ce serait un élément de $\mathbb{C}(x)$, d'après le théorème 5.1. Notant alors d le degré de f, on obtiendrait : 2d = 1, ce qui est absurde.

Cette illustration répond à une question de Rubel [4].

4 Cas d'une équation affine d'ordre un.

Nous étudions dans ce paragraphe l'équation à l'inconnue f de $\mathcal{M}(\Delta)$:

(1) $\qquad f = a\ \mu(f) + b,$ où a et b sont donnés dans $\mathcal{M}(\Delta)$.

L'équation (1) peut se mettre sous la forme matricielle équivalente :

$$F = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \mu(F),$$

avec : $F = \begin{bmatrix} f \\ 1 \end{bmatrix}$.

Dans le cas particulier où a et b sont en fait dans $\mathcal{M}_0(\Delta)$, et où l'inconnue est en fait à rechercher dans $\mathcal{M}_0(\Delta)$, on constate que, suivant la proposition 4.1, il y a trois cas à étudier :

→ Si : a(0) = 1 et b(0) = 0, l'ensemble des solutions F est un plan de $\mathcal{M}_0\left(\Delta, \mathbb{C}^2\right)$. Il en résulte aisément que l'ensemble des solutions f est une droite affine de $\mathcal{M}_0(\Delta)$, dirigée par l'ensemble des solutions de l'équation :

$$(2) \qquad f = a\,\mu(f)\,.$$

→ Si : a(0) = 1 et b(0) ≠ 0, il est immédiat que l'ensemble des solutions f est vide.

→ Si : a(0) ≠1 , l'ensemble des solutions F est une droite de $\mathcal{M}_0\left(\Delta, \mathbb{C}^2\right)$. On voit alors facilement que l'ensemble des solutions f est un singleton de $\mathcal{M}_0(\Delta)$.

Remarque.

Notons au passage que l'étude de l'équation (1) dans le cadre de A((X)), en supposant cette fois a et b éléments de A((X)), relèverait du théorème 2.3. Par ailleurs, il découle de la proposition 2.11 une étude identique à la précédente lorsque a et b n'admettent pas le pôle 0.

Nous supposons désormais que a et b sont dans $\mathbb{C}(x)$, et qu'en outre l'équation (2) admet une solution non nulle, que l'on note f_0 . Cela sera réalisé en particulier sous la condition suffisante : a(0) = 1 et b(0) = 0.

Dans la suite, on note f une solution de l'équation (1) ; posant : $g = \frac{f}{f_0}$, on constate que g vérifie la relation :

$$(3) \qquad g = \mu(g) + c,$$

où c, égal à $\frac{b}{f_0}$, est un élément de $\mathbb{C}(x)(f_0)$.

Supposons à partir d'ici que f est différentiellement algébrique sur $\mathbb{C}(x)$; g l'est alors sur $\mathbb{C}(x)\left(f_0,f'_0,\ldots\right)$

Il en découle que $h = g\circ\exp$ est différentiellement algébrique sur $\mathbb{C}\left(\exp\right)\left(f_0\circ\exp,f'_0\circ\exp.,\ldots\right)$. Ce sous-corps différentiel de $\mathcal{M}_0(\Pi)$ est à présent noté $\mathfrak{H}$. Il est stable par ν .

La relation (3) devient :

$$(4) \qquad h = \nu(h) + d,$$

où d appartient à $\mathfrak{H}$.

Soit alors P un polynôme minimal de g sur $\mathfrak{H}$. On le suppose en outre normalisé, ce qui ne restreint pas notre propos. Par dérivation de la relation (4), on obtient :

$$(5) \qquad \forall\, m \in \mathbb{N} \quad h^{(m)} = p^m \left(h^{(m)}\right)^{\nu} + d^{(m)} .$$

De l'égalité :

$$P\left(h,h',\ldots,h^{(n)}\right) = 0$$

provient l'égalité :

$$P^{\nu}\left(h^{\nu},(h')^{\nu},\ldots,\left(h^{(n)}\right)^{\nu}\right) = 0,$$

puis, grâce à la relation (5), cette autre égalité :

$$P^{\nu}\left(h-d,\frac{1}{p}(h'-d'),\ldots,\frac{1}{p^n}\left(h^{(n)}-d^{(n)}\right)\right) = 0.$$

Nous disposons ainsi d'un nouveau polynôme à coefficients dans $\mathfrak{H}$, annulant la famille $\left(h^{(m)}\right)_{m\in\mathbb{N}}$. Son multidegré est inférieur ou égal à celui de P. On en déduit que les polynômes P et $P^{\nu}\left(Y_0-d,\frac{1}{p}\left(Y_1-d'\right),\ldots,\frac{1}{p^n}\left(Y_n-d^{(n)}\right)\right)$ sont proportionnels, la constante de proportionnalité étant dans $\mathbb{C}$, comme on le constate en consultant le coefficient dominant.

On applique alors le lemme 1 du §2, et la méthode qui le motive : il existe ainsi un polynôme affine et non constant S de $\mathcal{H}[Y_0,Y_1,...,Y_n]$, égal à :

$$\sum_{k=0}^{n} s_k Y_k + s,$$

et un complexe δ, tels que :

$$S = \delta\, S^{\nu}\left(Y_0-d,\frac{1}{p}\left(Y_1-d'\right),....,\frac{1}{p^n}\left(Y_n-d^{(n)}\right)\right),$$

c'est à dire encore :

$$\forall\ k \in [0,n]\ \ s_k = \frac{\delta}{p^k}\nu\left(s_k\right) \text{ et } \ s = \delta\,\nu(s) - \sum_{k=0}^{n} \frac{\delta}{p^k} d^{(k)}.$$

Grâce au lemme 2 du §2, on voit que tous les s_i sont nuls, sauf un au plus, et donc sauf un exactement. Notons k l'indice correspondant, pour lequel on a donc :

$\frac{\delta}{p^k} = 1$; on a par conséquent :

$$s = p^k\,\nu(s) - d^{(k)}.$$

Compte tenu de la relation (5), on a :

$$(6) \qquad s = p^k\,\nu(s) - h^{(k)} + p^k\,\nu\left(h^{(k)}\right).$$

Nous devons à présent examiner deux cas :

∴ *Cas où f_0 n'appartient pas à $\mathbb{C}(x)$.*

Examinons d'abord, pour la clarté, la situation où k est nul. La relation (6), qui s'écrit aussi :

$$s + h = \nu(s+h)$$

entraîne que s + h appartient à $\mathbb{C}$, et donc que h appartient à $\mathcal{H}$; par conséquent, g appartient à $\mathbb{C}(x)\left(f_0,f'_0,....\right)$; mais : $g = \frac{f}{f_0}$ Donc f appartient aussi

à $\mathbb{C}(x)\left(f_0, f'_0, \ldots\right)$, qui est, d'après le théorème 5.1, une extension différentielle transcendante pure de $\mathbb{C}(x)$. Puisque f est différentiellement algébrique sur $\mathbb{C}(x)$, f appartient à $\mathbb{C}(x)$.

Dans le cas général où k est un entier quelconque, la relation (6) s'écrit encore :

$$s + h^{(k)} = p^k \, v\left\{s + h^{(k)}\right\}.$$

Cette relation implique que, ou bien k est nul, éventualité déjà envisagée, ou bien $s + h^{(k)}$ est nulle, ce que nous supposons à présent. Il en résulte que $h^{(k)}$ appartient à $\mathfrak{H}$.

Or : $h = \dfrac{f \circ \exp}{f_0 \circ \exp}$. Posant : $\dfrac{1}{f_0 \circ \exp} = g_0$, il vient :

$$h^{(k)} = \sum_{i=0}^{k} \lambda_i \; g_0^{(i)} \; \left(f \circ \exp\right)^{(k-i)} \in \mathfrak{H}, \text{ et } \lambda_i \in \mathbb{N}.$$

Considérons la famille $\left(g_0^{(i)}\right)_{i \in \mathbb{N}}$.

C'est une base algébrique de $\mathbb{C}\left(\exp\right)\left(f_0 \circ \exp, f'_0 \circ \exp., \ldots\right)$, comme $\mathbb{C}\left(\exp\right)$-algèbre. Cela résulte du fait que, f_0 n'étant pas dans $\mathbb{C}(x)$, le théorème 5.1 nous dit que la famille $\left(f_0^{(i)}\right)_{i \in \mathbb{N}}$ est une base algébrique de $\mathbb{C}(x)\left(f_0, f'_0, \ldots\right)$, et donc que la famille :

$$\left(\left(f_0 \circ \exp\right)^{(i)}\right)_{i \in \mathbb{N}}$$

est une base algébrique de $\mathbb{C}\left(\exp\right)\left(f_0 \circ \exp, f'_0 \circ \exp., \ldots\right)$, comme $\mathbb{C}\left(\exp\right)$-algèbre.

L'égalité ci-dessus nous permet alors d'affirmer que $\lambda_k \, f \circ \exp$ appartient à $\mathbb{C}\left(\exp\right)$, donc que f appartient à $\mathbb{C}(x)$.

∴ *Cas où f_0 appartient à $\mathbb{C}(x)$.*

Nous nous appuyons toujours sur l'égalité (6). Les calculs s'inspirent alors de ceux que l'on a conduits dans le §3. Nous savons que, en tous cas, $s + h^{(k)}$

appartient à $\mathbb{C}$. Le corps $\mathcal{H}$ est à présent égal à $\mathbb{C}(\exp)$, et s y appartient. Donc $h^{(k)}$ appartient à $\mathbb{C}(\exp)$.

Rappelons l'égalité satisfaite par h :

(4) $\qquad h = v(h) + d,$

où d appartient à $\mathcal{H}$, et, avec les notations de début de paragraphe :

$d = c\circ\exp$, c étant un élément de $\mathbb{C}(x)$.

Posons alors : $c_0 = c$, et définissons c_k par la condition :

$c_k(e^t) = \frac{d^k}{dt^k}\left(c(e^t)\right)$; c_k appartient à $\mathbb{C}(x)$. De même, posons :

$g_0 = g$, et $g_k(e^t) = \frac{d^k}{dt^k}\left(g(e^t)\right)$.

Par dérivation, l'égalité (4) implique :

$g_k(e^t) = p^k\, g_k(e^{pt}) + c_k(e^t)$, c'est à dire :

$g_k(x) = p^k\, g_k(x^p) + c_k(x)$.

En outre, on obtient les relations récurrentes :

$g_k(x) = x\, g'_{k-1}(x)$; $c_k(x) = x\, c'_{k-1}(x)$,

grâce auxquelles on peut écrire, pour k plus grand que 1 :

(5) $\qquad g'_{k-1}(x) = p^k\ x^{p-1}\ g'_{k-1}(x^p) + c'_{k-1}(x)$.

Par ce qui précède, on sait que $h^{(k)}$ appartient à $\mathbb{C}(\exp)$, ou encore que g_k appartient à $\mathbb{C}(x)$. Il en résulte que $p^k\ x^{p-1}\ g'_{k-1}(x^p)$ est aussi dans $\mathbb{C}(x)$. Projetons alors l'égalité (5) sur $\mathcal{S}$ parallèlement à $\mathcal{M}\oplus\mathbb{C}[x]$. Si l'on appelle S la composante de g'_{k-1} sur $\mathcal{S}$, on a :

$S = p^k\ x^{p-1}\ S(x^p)$, à l'aide des lemmes 2, 3, 4. Posant : $T = x\, S(x)$, il vient :

$T = p^k\ \mu\,(T)$,

donc T = 0. Il découle de cela que g'_{k-1} est dans $\mathfrak{M} \oplus \mathbb{C}[x]$, c'est à dire, toujours par le lemme 2, que g_{k-1} appartient à $\mathbb{C}(x)$. Une récurrence permet alors de connaître que g_0 , qui n'est autre que g, est dans $\mathbb{C}(x)$. Le résultat suivant est ainsi démontré :

Théorème 5.2.

Soient a et b deux éléments de $\mathbb{C}(x)$. On suppose que l'équation :

$$f = a\,\mu(f) + b$$

admet dans $\mathcal{M}(\Delta)$ une solution non nulle.

Les solutions dans $\mathcal{M}(\Delta)$ de l'équation :

$$f = a\,\mu(f) + b$$

sont différentiellement transcendantes ou rationnelles.

Corollaire.

Soient a et b deux éléments de $\mathbb{C}(X)$, tels que : a(0) = 1 et b(0) = 0.

Les solutions dans $\mathbb{C}[[X]]$ de l'équation :

$$f = a\,\mu(f) + b$$

sont différentiellement transcendantes ou rationnelles.

Preuve.

Les hypothèses auxquelles répondent a et b font que l'équation : $f = a\,\mu(f)$ admet une solution non nulle. De plus, l'étude effectuée au début du §4 montre que, sous ces hypothèses, les solutions dans $\mathbb{C}[[X]]$ sont en bijection naturelle avec les solutions dans $\mathcal{M}_0(\Delta)$.∎

∴ *Exemple 1.*

Considérons, dans $\mathbb{C}((X))$, l'équation :

$$f^2 = a\,(\mu(f))^2 + b,$$

où a et b sont deux éléments de $\mathbb{C}(X)$ tels que : a(0) = 1 et b(0) = 0.

Une solution f de cette équation est alors algébrique, ou bien différentiellement transcendante sur $\mathbb{C}(X)$. Il suffit pour s'en convaincre de poser : $g = f^2$. Ce changement de fonction nous donne aussi la discussion sur le nombre de solutions.

∴ *Exemple 2.*

Considérons, dans $\mathbb{C}((X))$, l'équation :

$$f - (a+b)\mu(f) + a\mu(b)\mu^2(f) = c,$$

où a, b sont des éléments de $\mathbb{C}(X)$, n'ayant pas 0 pour pôle, tels que :

$$a(0) = b(0) = 1, \text{ et } c(0) = 0.$$

Soit f l'unique solution non nulle de cette équation, dans $\mathbb{C}[[X]]$.

Posons :

$$g = f - b\mu(f) \text{ ; on a : } g = a\,\mu(g) + c.$$

Supposons f différentiellement algébrique sur $\mathbb{C}(X)$; g l'est aussi, et donc g appartient à $\mathbb{C}(X)$. Mais g(0) vaut 0. Donc f appartient aussi à $\mathbb{C}(X)$.

Chapitre 6.

L'application μ de Mahler n'est pas sans rappeler la dérivation, notamment dans son action de décalage sur les polynômes en f et ses images successives ; d'un côté, l'application de Mahler agit plus simplement, puisque, par exemple, l'image ensembliste de f et celle de $\mu(f)$ coïncident (lorsque l'on se place dans un cadre fonctionnel). D'un autre côté, elle est plus compliquée en ce qui concerne l'algébricité : la dérivée (n+1)-ième d'une fonction vérifiant une équation différentielle algébrique d'ordre n est une fraction rationnelle en les dérivées d'ordres inférieurs ; la situation est différente lorsqu'il s'agit des images itérées par μ .

Nonobstant ces nuances, on peut constater une situation commune aux deux exemples, tant qu'il s'agit de propriétés générales : l'objet de ce chapitre est de faire ressortir l'analogie.

Du point de vue arithmétique, le seul résultat qui nous occupera ici est le théorème 6.1, qui montre que, par exemple, s'il est conjecturé que la série génératrice f d'une suite régulière sur $\mathbb{Q}$ prend souvent des valeurs transcendantes en des points algébriques [1], la famille des valeurs prises en les points a, a^p,...a^{p^k} ,... sera, en revanche, toujours algébriquement liée.

Dans ce chapitre, nous nous plaçons à nouveau dans le cadre du corps A((X)) des séries formelles sur le corps commutatif A ; la situation générale est donc celle du chapitre 2. Néanmoins, la théorie s'applique sans changement si l'on se place dans le cadre du corps des fonctions méromorphes sur un ouvert de $\mathbb{C}$ stable par $x \longmapsto x^p$; on utilisera cette remarque pour obtenir des illustrations.

1 Extensions mahlériennes.

La notion d'extension mahlérienne a été introduite dans le chapitre 2. Donnons-en à présent quelques exemples.

Exemple 1.

Soit f un élément de A((X)), solution d'une p-équation de Mahler linéaire d'ordre un sur le sous-corps p-mahlérien B de A((X)), et K = B(f) ; K est une extension p-mahlérienne de B, car c'est un corps, contenant K, et p-mahlérien, puisque $\mu_p(f)$ appartient à K.

Exemple 2.

Soit E un sous-ensemble de A((X)); le plus petit sous-ensemble stable par μ_p et contenant E est manifestement l'ensemble :

$$\bigcup_{n\in\mathbb{N}} \mu^n(E),$$

qui est aussi l'intersection de toutes les partiet de A((X)) contenant E et stables par μ .

Même si E est un corps contenant A, l'ensemble précédent n'est pas nécessairement un corps ; il engendre un sous-corps de A((X)), qui est lui p-mahlérien.

Par exemple, si E = {f}, le plus petit sous-corps p-mahlérien contenant f est le corps contenant A et engendré par $\{f,\mu(f),\ldots,\mu^k(f),..\}$, c'est à dire :

$$A\left(f,\mu(f),\ldots,\mu^k(f),..\right).$$

Une famille p-mahlérienne est une famille dont l'ensemble image est stable par μ_p.

Lemme.

Soit L une extension p-mahlérienne de K. L'ensemble des familles p-mahlériennes de L algébriquement libres sur K est inductif.

Preuve.

Soit $(F_i)_{i\in I}$ une famille totalement ordonnée de telles familles, et : $F = \bigcup_{i\in I} F_i$; il est clair que F est p-mahlérienne ; par ailleurs, dire que F n'est pas algébriquement libre, c'est dire qu'il existe une sous-famille finie algébriquement liée, et cette sous-famille est alors nécessairement une sous-famille de l'une des F_i.∎

Soit alors, grâce à ce lemme , F un élément maximal de l'ensemble de familles précédent, et L_0 le corps K(F) ; puisque K et F sont p-mahlériens, L_0 l'est aussi .

Considérons à présent un élément x de L_0-K ; supposons, par l'absurde, que la famille $(\mu^k(x))_{k\in\mathbb{N}}$ est algébriquement liée sur K.

Il existe donc un entier k tel que :

$$\mu^k(x) \text{ est algébrique sur le corps } K\left(x,\mu(x),\ldots,\mu^{k-1}(x)\right).$$

Comme x est dans K(F), il existe un élément P de $K(F_1)$ tel que :

$$x = P(F_1).$$

Ici, F_1 est une sous-famille finie de F, de la forme suivante :

$$\left(f_1,\ldots,\mu^{m_1}(f_1),\ldots..,f_q,\ldots,\mu^{m_q}(f_q)\right).$$

Il n'est en outre pas restrictif de supposer que f_1 intervient effectivement dans l'expression $P(F_1)$ et, quitte à faire une hypothèse de minimalité sur m_1, que $\mu^{m_1}(f_1)$ y figure.

Dans ces conditions, l'expression de $\mu^k(x)$ contient $\mu^{m_1+k}(f_1)$, tandis que cet élément ne figure pas dans l'expression de $x,\mu(x),...,\mu^{k-1}(x)$. Ceci peut se dire *autrement : si M est le corps :*

$$K\left(f_1,...,\mu^{m_1+k-1}(f_1),.....,f_q,...,\mu^{m_q+k}(f_q)\right),$$

alors $\mu^k(x)$ appartient à $M\left(\mu^{m_1+k}(f_1)\right)$, mais pas à M.

Par ailleurs, $\mu^k(x)$ est algébrique sur $K\left(x,\mu(x),...,\mu^{k-1}(x)\right)$, qui est inclus dans M. Donc l'élément $\mu^k(x)$ est algébrique sur M, et appartient à l'extension transcendante pure $M\left(\mu^{m_1+k}(f_1)\right)$ de M : il en résulte que $\mu^k(x)$ appartient à M, *ce qui est une contradiction.*

On a ainsi prouvé qu'aucun élément de L_0-K ne vérifie de p-équation de Mahler algébrique sur K, soit encore de relation :

$P\left(x,\mu(x),...,\mu^k(x)\right)= 0$, où P est un polynôme non nul de $K[X_0,.....,X_k]$.

Enonçons ce résultat sous une forme plus générale.

Proposition 6.1

Soit K un sous-corps p-mahlérien de A((X)), et F une famille d'éléments de A((X)), algébriquement libre sur K. Si un élément de K(F) vérifie une p-équation de Mahler algébrique sur K, il appartient à K.

Considérons maintenant un élément x de L. La famille $F\cup\left(\mu^k(x)\right)_{k\in\mathbb{N}}$ est une famille p-mahlérienne contenant F strictement, donc algébriquement liée sur K. Une relation de liaison algébrique concernant cette famille impliquera l'un des $\mu^k(x)$, faute de quoi la famille F serait algébriquement liée sur K. Il résulte de ceci que x vérifie une p-équation de Mahler sur K.

En bref, l'extension mahlérienne de L sur K a pu être décomposée en une extension de L_0 sur K, " μ-transcendante pure " en ceci qu'aucun élément de L_0-K ne vérifie d'équation de Mahler sur K, et une extension "μ-algébrique " de L sur L_0, en ce sens que tous les éléments de L vérifient une équation de Mahler algébrique sur L_0.

2 Exemple d'extension μ-transcendante pure de $\mathbb{C}(x)$.

Dans ce paragraphe d'exemples, le cadre sera celui du corps $\mathcal{M}(\mathbb{C})$, et $\mathbb{C}(x)$ joue le rôle de $\mathbb{C}(X)$.

Lemme 1.

Soit $(t_i)_{i\in I}$ une famille d'éléments de $\mathbb{C}(x)$ telle que la famille $(1)\cup(t_i)_{i\in I}$ soit linéairement libre sur $\mathbb{C}$. La famille $(e^{t_i})_{i\in I}$ est alors algébriquement libre sur $\mathbb{C}(x)$.

Preuve.

Supposons qu'il existe une relation de dépendance algébrique sur $\mathbb{C}(x)$ de la famille précédente. On peut manifestement réécrire cette relation sous la forme :

$$\sum_j P_j\, e^{\lambda_j(t_1,t_2,\dots)} = 0$$

où : P_j appartient à $\mathbb{C}[x]$, l'un des P_j est non nul, $\lambda_j(t_1,t_2,\dots)$ désigne une combinaison linéaire à coefficients entiers des t_i, ici numérotés 1,2,.. pour la lisibilité, et où λ_j est différent de λ_k (comme formes linéaires) dès que j est différent de k.

Parmi les relations de ce type, choisissons en une de longueur minimale, et telle que, disons, P_0 soit non nul. On obtient :

$$1 + \sum_{j\neq 0} \frac{P_j}{P_0}\, e^{\lambda_i-\lambda_0} = 0, \text{ ou encore :}$$

$$1 + \sum_{j\neq 0} R_j\, e^{\lambda_j-\lambda_0} = 0.$$

Dérivons cette égalité par rapport à x ; il vient :

$$\sum_{j\neq 0}\left(R'_j + R_j \frac{d}{dx}(\lambda_j-\lambda_0)\right) e^{\lambda_j-\lambda_0} = 0.$$

L'hypothèse de minimalité entraîne que, pour tout j non nul, on a :

$$\frac{R'_j}{R_j} = -\frac{d}{dx}(\lambda_j-\lambda_0).$$

Mais $\lambda_j-\lambda_0$ est une fraction rationnelle ; la décomposition en éléments simples des membres de gauche et de droite de l'égalité précédente montre que :

$$\frac{R'_j}{R_j} = -\frac{d}{dx}(\lambda_j-\lambda_0) = 0.$$

Ceci implique que :

$\lambda_j-\lambda_0 \in \mathbb{C}$, ce qui est en contradiction avec l'hypothèse.∎

Exemple.

Soit : $t_i = x^{p^i}$; la condition du lemme est clairement satisfaite ; il découle alors de la proposition 6.1 que :

$\mathbb{C}(x)\left(e^{x}, e^{x^{p}}, e^{x^{p^{2}}},\ldots\right)$ est une extension μ-transcendante pure de $\mathbb{C}(x)$.

Plus généralement :

Lemme 2.

Soit f un élément de $\mathbb{C}(x)$, non dans $\mathbb{C}$. La famille $(1)\cup\left(\mu^{i}(f)\right)_{i\in\mathbb{N}}$ est linéairement libre sur $\mathbb{C}$.

Preuve.

C'est la même démonstration que celle de la proposition 2.2.∎

On dispose alors d'autres extensions μ-transcendantes pures de $\mathbb{C}(x)$: tous les corps du type $\mathbb{C}(x)\left(e^{f(x)}, e^{f(x^{p})}, e^{f(x^{p^{2}})},\ldots\right)$, où f est une fraction rationnelle non constante.

3 Propriétés des extensions μ-algébriques.

Lemme 1.

Soit K un sous-corps p-mahlérien de A((X)), et f un élément de A((X)).
Les propriétés ci-dessous sont équivalentes :

(1)f vérifie une p-équation de Mahler algébrique sur K.
(2)$K\left(f,\mu(f),\ldots,\mu^{k}(f),..\right)$ est une extension μ -algébrique de K.
(3)$K\left(f,\mu(f),\ldots,\mu^{k}(f),..\right)$ a une dimension de transcendance finie sur K.
(4)Il existe une extension μ -algébrique de K contenant f

Preuve.

$\therefore$ (3) $\Rightarrow$ (4)

Il suffit de prendre pour extension $K\left(f,\mu(f),\ldots,\mu^{k}(f),..\right)$ elle-même ; en effet, si g appartient à $K\left(f,\mu(f),\ldots,\mu^{k}(f),...\right)$, la famille $\left(g,\mu(g),\ldots,\mu^{m}(g)\right)$ est algébriquement liée, lorsque l'on prend pour m la dimension de transcendance de $K\left(f,\mu(f),\ldots,\mu^{k}(f),..\right)$ sur K.

$\therefore$ (4) $\Rightarrow$ (2)

Si L est l'extension dont on suppose l'existence, elle contient f, et donc, étant p-mahlérienne, elle contient $K\left(f,\mu(f),\ldots,\mu^{k}(f),..\right)$, qui est donc elle-même μ -algébrique .

$\therefore$ (2) $\Longrightarrow$ (1) est évident.

$\therefore$ (1) $\Longrightarrow$ (3)

Par hypothèse, la famille $\left(f,\mu(f),...,\mu^k(f),..\right)$ est algébriquement liée ; soit donc n tel que la famille :

$\left(f,\mu(f),...,\mu^{n-1}(f)\right)$ soit algébriquement libre, et $\left(f,\mu(f),...,\mu^n(f)\right)$ soit algébriquement liée.

Posons : $L = K\left(f,\mu(f),...,\mu^{n-1}(f)\right)$; $L\left(\mu^n(f)\right)$ est algébrique sur L ; or $\mu^{n+1}(f)$ vérifie une équation algébrique sur $L\left(\mu^n(f)\right)$: il suffit pour s'en assurer d'appliquer μ à l'équation vérifiée par $\mu^n(f)$ sur L. Donc $L\left(\mu^n(f),\mu^{n+1}(f)\right)$ est algébrique sur L ; par une récurrence facile, on constate ainsi que $\left(f,\mu(f),...,\mu^{n-1}(f)\right)$ est une base de transcendance de $K\left(f,\mu(f),...,\mu^k(f),..\right)$ sur K.∎

Proposition 6.2.

(a) Si L est une extension μ -algébrique de K, et M est une extension μ -algébrique de L, alors M est une extension μ -algébrique de K.

(b) Si K est un sous-corps p-mahlérien de A((X)), l'ensemble K_p des éléments de A((X)) qui vérifient une p-équation de Mahler algébrique sur K est un sous-corps p-mahlérien de A((X)), qui est une extension μ -algébrique de K.

(c) Si K est un sous-corps différentiel de A((X)), p-mahlérien, K_p est un sous-corps différentiel de A((X)).

Preuve.

(a)Soit f un élément de M ; la famille $(f,\mu(f),...,\mu^n(f))$ est algébriquement liée sur L, donc sur un sous-corps $K\left(a_1,.....,a_q\right)$ de L.

Les corps $K\left(a_1,\mu(a_1),...,\mu^m\left(a_1\right),...\right)$, ...,$K\left(a_q,\mu(a_q),...,\mu^m\left(a_q\right),...\right)$ sont, d'après le lemme, de dimension de transcendance finie sur K. Il en découle que le corps K_1, égal à :

$$K\left(a_1,\mu(a_1),...,\mu^m\left(a_1\right),.....,a_q,\mu(a_q),...,\mu^m\left(a_q\right),...\right)$$

est, lui aussi, de dimension de transcendance finie sur K. Puisque K_1 est toujours p-mahlérien, le lemme assure que la dimension de transcendance de $K_1\left(f,\mu(f),...,\mu^m(f),...\right)$ sur K_1 est finie ; par transitivité, la dimension de transcendance de $K_1\left(f,\mu(f),...,\mu^m(f),...\right)$ sur K est finie, et a fortiori celle de $K\left(f,\mu(f),...,\mu^m(f),...\right)$ sur K. Le lemme 1 permet de conclure.

(b) et (c).Montrons par exemple que, si f et g vérifient une équation de Mahler sur K, f + g en vérifie aussi une. L'extension $K \subset K\left(f,\mu(f),\ldots,\mu^m(f),\ldots\right)$ est μ -algébrique.

Par ailleurs, puisque l'extension :

$$K \subset K\left(g,\mu(g),\ldots,\mu^m(g),\ldots\right)$$

est μ -algébrique , l'extension :

$$K\left(f,\mu(f),\ldots,\mu^m(f),\ldots\right) \subset K\left(f,\mu(f),\ldots,\mu^m(f),\ldots\right)\left(g,\mu(g),\ldots,\mu^m(g),\ldots\right)$$

l'est elle aussi.

D'après (a), l'extension : $K \subset K\left(f,\mu(f),\ldots,\mu^m(f),\ldots\right)\left(g,\mu(g),\ldots,\mu^m(g),\ldots\right)$ est encore μ-algébrique . Comme l'élément f+g appartient à $K\left(f,\mu(f),\ldots,\mu^m(f),\ldots\right)\left(g,\mu(g),\ldots,\mu^m(g),\ldots\right)$, on a le résultat. Le restant se montre à l'identique. ∎

Remarque.

On pourrait appeler K_p la clôture mahlérienne de K dans A((X)) ; bien entendu, K_p n'est pas "μ-clos ", en ce sens que certaines équations algébriques de Mahler n'ont pas de solutions dans A((X)). Néanmoins,K_p est "μ-clos " dans A((X)), ce qui résulte de la propriété (a) de la proposition 6.2.

Exemple.

Soit f la série génératice de la suite de Thue-Morse, solution de :

$$f = (1-x)\mu_2(f) \ .$$

Bien évidemment, f est μ_2-algébrique sur $\mathbb{C}(X)$; en fait, on peut éliminer x :

$$\frac{f}{\mu(f)} = 1-x \ ; \ \frac{\mu(f)}{\mu^2(f)} = 1-x^2 ; \text{ d'où :}$$

$$\left(1 - \frac{f}{\mu(f)}\right)^2 = 1 - \frac{\mu(f)}{\mu^2(f)} \ , \text{ ou encore :}$$

$$\mu^2(f))\ (\mu(f) - f)^2 = (\mu(f))^2\left(\mu^2(f) - \mu(f)\right),$$

égalité qui montre que f vérifie en fait une équation de Mahler algébrique à coefficients dans $\mathbb{C}$, et même entiers. Ce résultat est général :

Lemme 2.

A(X) est une extension μ-algébrique de A.

Preuve.

Il suffit, grâce à la proposition 6.2, de prouver que X vérifie une équation de Mahler algébrique sur A, ce qui est particulièrement évident. ∎

Lemme 3.

Soit σ l'application de $A[X_0,X_1,...,X_n,..]$ dans lui-même, homomorphisme d'anneaux qui, pour tout i, envoie X_i sur X_{i+1}.

Notons $(\mathfrak{M}_j)_{j\in[0,q]}$ une famille finie de monômes de $A[X_0,X_1,...,X_n,..]$, ordonnée de façon croissante selon le bon ordre lexicographique défini dans le chapitre 1.

Le polynôme :

$$\det\begin{bmatrix} \mathfrak{M}_0 & \mathfrak{M}_1 & \dots & \mathfrak{M}_q \\ \sigma(M_0) & \sigma(\mathfrak{M}_1) & \dots & \sigma(\mathfrak{M}_q) \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \sigma^q(\mathfrak{M}_0) & \sigma^q(\mathfrak{M}_1) & \dots & \sigma^q(\mathfrak{M}_q) \end{bmatrix}$$

n'est pas le polynôme nul.

Preuve.

Par récurrence sur q ; dans un développement par rapport à la dernière ligne, on observe que le terme de plus haut indice, et d'exposant le plus élevé, qui provient du terme $\sigma^q(\mathfrak{M}_q)$, est multiplié par un terme non nul, d'après l'hypothèse de récurrence.∎

Théorème 6.1

Soit f un élément de A((X)) vérifiant une équation de Mahler algébrique sur A(X) ; f vérifie alors une équation de Mahler dans le sous-corps premier de A.

Preuve.

D'après le lemme 1, on peut supposer que f vérifie une équation de Mahler algébrique sur A. La famille des monômes en $f,\mu(f),...,\mu^m(f),...$ est linéairement liée sur A ; soit, si l'on note $(M_i)_{i\in I}$ la famille finie de monômes concernée par la relation de liaison :

$$\sum_{i\in I}\lambda_i M_i = 0.$$

D'où, en appelant q+1 le cardinal de I :

$$\sum_{i\in I}\lambda_i\,\mu(M_i) = 0$$

.....

$$\sum_{i\in I}\lambda_i \mu^q(M_i) = 0.$$

Il en suit que le déterminant de la matrice :

$$\begin{bmatrix} M_0 & M_1 & \dots & M_q \\ \mu(M_0) & \mu(M_1) & \dots & \mu(M_q) \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \dots & \cdot \\ \mu^q(M_0) & \mu^q(M_1) & \dots & \mu^q(M_q) \end{bmatrix}$$

est nul.

Le lemme 3 entraîne alors le résultat.

Corollaire.

Soit f une fonction holomorphe sur D(0,r), satisfaisant une p-équation de Mahler algébrique sur $\mathbb{C}(x)$, et a un élément de D(0,r); la famille $\left(f\left(a^{p^k}\right)\right)_{k\in\mathbb{N}}$ est algébriquement liée sur $\mathbb{Q}$.

CHAPITRE 7

Un résultat célèbre de Cobham affirme que, si une suite est à la fois p-automatique et q-automatique, p et q étant deux entiers multiplicativement indépendants, elle est ultimement périodique. La généralisation de ce résultat, conjecturée par Loxton et van der Poorten, est la suivante : *si une série formelle à coefficients dans un corps A vérifie à la fois une p-équation de Mahler et une q-équation de Mahler, p et q étant multiplicativement indépendants, c'est une fraction rationnelle.*
En d'autres termes, avec les notations du chapitre 2 :

$$ML_p(A(X)) \cap ML_q(A(X)) = A(X).$$

Notons que cette conjecture implique le théorème de Cobham, ainsi que la généralisation du théorème de Cobham aux suites p-régulières conjecturée par Allouche et Shallit.

Le résultat que nous obtenons est en réalité de portée beaucoup plus limitée : nous considérons un élément φ de $\mathbb{C}((X))$ vérifiant une p-équation de Mahler d'ordre un sur $\mathbb{C}(X)$, et aussi une q-équation de Mahler d'ordre un sur $\mathbb{C}(X)$. Nous montrons alors que φ est dans $\mathbb{C}(X)$ (théorème 8.1). Il faut noter que p et q sont supposés un peu plus que multiplicativement indépendants, à savoir premiers entre eux. Pour la clarté du propos, on prend $p = 2$ et $q = 3$.

Langages et notations.

Une application $f : A \to B$ est dite *presque nulle* si l'ensemble

$$supp(f) = \{a \in A \ f(a) \neq 0\}$$

est fini ; $supp(f)$ est appelé *support de f*.
Si A est un sous-ensemble de $\mathbb{C}$, et k un entier naturel. On note

$$A^{1/k} = \{x \in \mathbb{C} \ \ x^k \in A\}.$$

Si $A = \{a\}$, on notera plus brièvement $a^{1/k}$ cet ensemble. On désignera aussi par A^k l'image de A par $x \mapsto x^k$.
Soient à présent deux fractions rationnelles a et b telles que

$$a(0) = b(0) = 1,$$

et une fonction φ, méromorphe sur le disque unité ouvert, telle que $\varphi(0) = 1$, et vérifiant de plus les deux équations de Mahler suivantes :

$$\varphi(x^3) = a(x)\varphi(x) \qquad (1)$$
$$\varphi(x^2) = b(x)\varphi(x) \qquad (2)$$

On désire montrer que φ est elle aussi une fraction rationnelle.

Posons

$$a(x) = \prod_{\alpha \in \mathbb{C}^*} (x - \alpha)^{f(\alpha)},$$

où $f : \mathbb{C}^* \to \mathbb{Z}$ est presque nulle.
De même, posons $b(x) = \prod_{\alpha \in \mathbb{C}^*} (x - \alpha)^{g(\alpha)}$.
Gr ce à la proposition 1.3, on obtient :

$$\forall \alpha \in \mathbb{C}^* \qquad f(\alpha^2) - f(\alpha) = g(\alpha^3) - g(\alpha).$$

Grâce à cette relation, nous allons prouver l'existence d'une application $h : \mathbb{C}^* \to \mathbb{Z}$, presque nulle, telle que :

$$f(\alpha) = h(\alpha) - h(\alpha^3)$$

La proposition 1.3, à nouveau, nous permettra alors d'en déduire que φ est une fraction rationnelle.

1. Construction de h sur le complémentaire de l'ensemble des racines de 1.

Lemme 1. *Soit $S = \{x \in \mathbb{C}^*,\ x$ non racine de l'unité$\}$ et F un sous-ensemble fini de S. Alors :*

$$\{(k,l) \in \mathbb{N}^2 \quad F^{2^\ell} \cap F^{3^k} \neq \emptyset\} \text{ est fini.}$$

Preuve :
Notons I l'ensemble précédent; si $(k,\ell) \in I$, il existe $y_{k,\ell} \in F^{2^\ell} \cap F^{3^k}$, donc il existe $\alpha_{k,\ell}$ et $\beta_{k,\ell}$ dans F tels que :

$$y_{k,\ell} = \alpha_{k,\ell}^{2^\ell} = \beta_{k,\ell}^{3^k}.$$

On définit ainsi une application :

$$I \to F \times F$$
$$(k,\ell) \mapsto (\alpha_{k,\ell},\ \beta_{k,\ell})$$

Montrons qu'elle est injective, ce qui suffira. Soit :

$$\alpha_{k,\ell} = \alpha_{k',\ell'} = \alpha\ ;\ \beta_{k,\ell} = \beta_{k',\ell'} = \beta.$$

On a : $\alpha^{2^\ell} = \beta^{3^k}$; $\alpha^{2^{\ell'}} = \beta^{3^{k'}}$ et donc :

$$\alpha^{2^\ell . 3^{k'}} = \alpha^{2^{\ell'} . 3^k}$$

Or α n'est pas racine de 1 ($\alpha \in F \subset S$). Donc : $2^{\ell - \ell'} = 3^{k-k'}$, soit $\ell = \ell'$ et $k = k'$.

Nous pouvons à présent poser :

$$\forall \alpha \in S \quad h(\alpha) = \sum_{k=0}^{+\infty} f(\alpha^{3^k})$$

Ceci a un sens, car $k \mapsto \alpha^{3^k}$ est injective, et donc $f(\alpha^{3^k}) = 0$ pour k assez grand. De plus, $h(S) \subset \mathbb{Z}$ évidemment.
Soit $\alpha \in S$. Alors $\alpha^3 \in S$, et donc :

$$h(\alpha^3) = \sum_{k=0}^{+\infty} f(\alpha^{3^{k+1}}) = h(\alpha) - f(\alpha)$$

Montrons que $h : S \to \mathbb{Z}$ est presque nulle.
Notons $A = [\ \mathrm{supp}(f) \cup \mathrm{supp}(g)] \cap S$; A est fini.

Lemme 2. $\left[\bigcup_{k\in\mathbb{N}} A^{\frac{1}{2^k}}\right] \cap \left[\bigcup_{\ell\in\mathbb{N}} A^{\frac{1}{3^\ell}}\right]$ *est fini.*

Preuve : L'ensemble considéré est égal à :

$$\bigcup_{(k,\ell)\in\mathbb{N}^2} (A^{\frac{1}{2^k}} \cap A^{\frac{1}{3^\ell}})$$

Si (k,ℓ) est tel que $A^{\frac{1}{2^k}} \cap A^{\frac{1}{3^\ell}} \neq \emptyset$, il existe x, y dans A tels que $x = \omega^{2^k}$; $y = \omega^{3^\ell}$, où $\omega \in A^{\frac{1}{2^k}} \cap A^{\frac{1}{3^\ell}}$. D'où : $x^{3^\ell} = y^{2^k}$, et $(k,\ell) \in I$ (avec la notation du lemme 1).

Finalement :

$$\bigcup_{(k,\ell)\in\mathbb{N}^2} (A^{\frac{1}{2^k}} \cap A^{\frac{1}{3^\ell}}) = \bigcup_{(k,\ell)\in I} (A^{\frac{1}{2^k}} \cap A^{\frac{1}{3^\ell}})$$

Or, A étant fini, $A^{\frac{1}{2^k}}$ est lui aussi fini. Le résultat en découle.

Pour montrer que h est presque nulle, il suffit donc de montrer que, si $\alpha \notin [\bigcup_{k\in\mathbb{N}} A^{\frac{1}{2^k}}] \cap [\bigcup_{\ell\in\mathbb{N}} A^{\frac{1}{3^\ell}}]$, alors $h(\alpha) = 0$. Supposons par exemple que $\alpha \notin \bigcup_{k\in\mathbb{N}} A^{\frac{1}{2^k}}$.

Cela signifie que, quel que soit k dans $\mathbb{N}$, $\alpha^{2^k} \notin A$, donc que $f(\alpha^{2^k}) = 0$. Notons que l'hypothèse entraîne :

$$\forall k \in \mathbb{N} \quad f(\alpha^{3^k}) - f(\alpha^{2.3^k}) = g(\alpha^{3^k}) - g(\alpha^{3^{k+1}})$$

et donc que :

$$\begin{aligned} h(\alpha) - h(\alpha^2) &= \sum_{k=0}^{+\infty} [f(\alpha^{3^k}) - f(\alpha^{2.3^k})] \\ &= \sum_{k=0}^{+\infty} [g(\alpha^{3^k}) - g(\alpha^{3^{k+1}})] \\ &= g(\alpha) \end{aligned}$$

puis $h(\alpha^{3^k}) = 0$ pour k assez grand.

Il en résulte que :

$$\forall k \in \mathbb{N} \quad h(\alpha) = h(\alpha^{2^k})$$

Or il existe k tel que $h(\alpha^{2^k}) = 0$; sinon, pour tout k, $h(\alpha^{2^k}) \neq 0$ et donc, d'après la définition même de h, il existe ℓ (dépendant de k) tel que $f(\alpha^{2^\ell 3^\ell}) \neq 0$. Mais $k \mapsto \alpha^{2^k 3^\ell}$ est injective, donc supp (f) est infini, ce qui est contradictoire. Finalement, on a bien $h(\alpha) = 0$.

2. Construction de h sur l'ensemble des racines de 1.

Montrons tout d'abord deux lemmes.

Lemme 3. *Soit* $M = \sum_{x \in \mathbb{C}^*} |f(x)|$, *et* x *un élément de* $\mathbb{C}^*$, p *un élément de* $\mathbb{N}$. *Alors*

$$\forall n \in \mathbb{N} \quad 2^n[f(x) + f(x^3) + \cdots + f(x^{3^{p-1}})] =$$

$$= \alpha_n + \sum_{k=0}^{n-1} 2^k \left\{ \sum_{\omega \in (x^{3^p})^{\frac{1}{2^{n-k}}}} g(\omega) - \sum_{\omega \in x^{\frac{1}{2^{n-k}}}} g(\omega) \right\},$$

où $|\alpha_n| \leq Mp$.

Preuve : Soit $\omega \in x^{\frac{1}{2^n}}$. On a, successivement :

$$f(\omega^2) - f(\omega) = g(\omega^3) - g(\omega)$$

$$\cdots$$

$$f(\omega^{2^n}) - f(\omega^{2^{n-1}}) = g(\omega^{2^{n-1}3}) - g(\omega^{2^{n-1}})$$

et donc :

$$f(x) - f(\omega) = \sum_{k=0}^{n-1} \left[g(\omega^{2^k 3}) - g(\omega^{2^k}) \right]$$

Sommons ces égalités pour ω décrivant $x^{\frac{1}{2^n}}$. On obtient :

$$2^n f(x) - \sum_{\omega \in x^{\frac{1}{2^n}}} f(\omega) = \sum_{k=0}^{n-1} \sum_{\omega \in x^{\frac{1}{2^n}}} [g(\omega^{2^k \cdot 3}) - g(\omega^{2^k})]$$

Clairement : $|\sum_{\omega \in x^{\frac{1}{2^n}}} f(\omega)| \leq M$. De plus, pour $k \in [0, n-1]$:

$\sum_{\omega \in x^{\frac{1}{2^n}}} g((\omega^{2^k})^3) = 2^k \sum_{\omega \in x^{\frac{1}{2^{n-k}}}} g(\omega^3)$. On a donc :

$$2^n f(x) = \varepsilon_n + \sum_{k=0}^{n-1} 2^k \left\{ \sum_{\omega \in x^{\frac{1}{2^{n-1}}}} [g(\omega^3) - g(\omega)] \right\},$$

avec $|\varepsilon_n| \leq M$.

L'application :

$$x^{\frac{1}{2^j}} \to (x^3)^{\frac{1}{2^j}}$$
$$\omega \mapsto \omega^3$$

est bijective. Il suffit, vu la cardinalité, de montrer qu'elle est injective. Or :

$$\omega_1^3 = \omega_2^3 \text{ avec } \omega_1^{2^j} = \omega_2^{2^j} \Rightarrow \left(\frac{\omega_1}{\omega_2}\right)^3 = 1 \text{ et } \left(\frac{\omega_1}{\omega_2}\right)^{2^j} = 1, \text{ donc } \omega_1 = \omega_2.$$

Finalement, on peut réécrire :

$$2^n f(x) = \varepsilon_n + \sum_{k=0}^{n-1} 2^k \left\{ \sum_{\omega \in (x^3)^{\frac{1}{2^{n-k}}}} g(\omega) - \sum_{\omega \in x^{\frac{1}{2^{n-k}}}} g(\omega) \right\}$$

Appliquons cette égalité à x, $x^3, \cdots, x^{3^{p-1}}$, et sommons :

$$2^n[f(x) + f(x^3) + \cdots + f(x^{3^{p-1}})] = \alpha_n + \sum_{k=0}^{n-1} 2^k \left(\sum_{\omega \in (x^{3^p})^{\frac{1}{2^{n-k}}}} g(\omega) - \sum_{\omega \in x^{\frac{1}{2^{n-k}}}} g(\omega) \right)$$

avec $|\alpha_n| \leq pM$.

Lemme 4. *Soit $R = \{x \in \mathbb{C}^*,\ x$ racine de l'unité $\}$, et F un sous-ensemble fini de R. Alors :*

$$\bigcup_{n \in \mathbb{N}} F^{2^n} \text{ est un ensemble fini}$$

Preuve : Si $F = \{x\}$, alors $\bigcup_{n \in \mathbb{N}} F^{2^n}$ est incluse dans le sous-groupe de $\mathbb{C}^*$ engendré par x, qui est fini. Le résultat général en découle.

Notons $B = [\text{supp}\,(f) \cup \text{supp}\,(g)] \cap R$; B est fini, et donc, d'après le lemme 4 : $\bigcup_{n \in \mathbb{N}} B^{2^n}$ est fini.

Soit à présent $\alpha \in R$. Puisque $\bigcup_{p \in \mathbb{N}} \alpha^{\frac{1}{3^p}}$ est infini, il existe donc

$$x \in \bigcup_{p \in \mathbb{N}} \alpha^{\frac{1}{3^p}} \setminus \bigcup_{n \in \mathbb{N}} B^{2^n}.$$

Posons :

$$h(\alpha) = -[f(x) + \cdots + f(n^{3^{p-1}})], \text{ où } x^{3^p} = \alpha$$

Il convient de vérifier que cette définition ne dépend que de α, pas de (x, p). Soit donc $y \notin \cup B^{2^n}$ tel que $y^{3^q} = \alpha$. D'après le lemme 3 :

$$2^n[f(x) + \cdots + f(x^{3^{p-1}})] = \alpha_n + \sum_{k=0}^{n-1} 2^k \left(\sum_{\omega \in \alpha^{\frac{1}{2^{n-k}}}} g(\omega) - \sum_{\omega \in x^{\frac{1}{2^{n-k}}}} g(\omega) \right)$$

Mais, si $\omega \in x^{\frac{1}{2^{n-k}}}$, $\omega^{2^{n-k}} = x \Rightarrow \omega \notin B \Rightarrow g(\omega) = 0$.
Donc :

$$2^n[f(x) + \cdots + f(x^{3^{p-1}})] = \alpha_n + \sum_{k=0}^{n-1} 2^k \left(\sum_{\omega \in \alpha^{\frac{1}{2^{n-k}}}} g(\omega) \right)$$

De même :

$$2^n[f(y) + \cdots + f(y^{3^{q-1}})] = \beta_n + \sum_{k=0}^{n-1} 2^k \left(\sum_{\omega \in \alpha^{\frac{1}{2^{n-k}}}} g(\omega) \right)$$

Donc :

$$|2^n\{[f(x) + \cdots + f(x^{3^{p-1}})] - [f(y) + \cdots + f(y^{3^{q-1}})]\}| \leq M(p+q),$$

et ce quel que soit n. Donc, faisant tendre n vers $+\infty$, on obtient l'égalité souhaitée. h étant ainsi définie, h est clairement à valeurs entières. Soit $\alpha \notin \bigcup_{n \in \mathbb{N}} B^{3^n}$, qui est un ensemble fini (lemme 4). Soit x et p tels que $x^{3^p} = \alpha$. S'il existe $k \leq p-1$ tel que $x^{3^k} \in B$, alors $x^{3^p} \in B^{3^{p-k}}$, donc $\alpha \in B^{3^{p-k}}$, ce qui est exclu. Donc : $f(x) = f(x^3) = \cdots = f(x^{3^{p-1}}) = 0$, soit $h(\alpha = 0)$.

Enfin, si $h(\alpha) = -[f(x) + \cdots + f(x^{3^{p-1}})]$, alors :

$$h(\alpha^3) = -[f(x) + \cdots + f(x^{3^p})].$$

En effet, $x^{3^p} = \alpha \Rightarrow x^{3^{p+1}} = \alpha^3$, et $x \notin \cup B^{2^n}$. Donc $(x, p+1)$ permet effectivement de définir $h(\alpha^3)$. D'où :

$$h(\alpha) - h(\alpha^3) = f(x^{3^p}) = f(\alpha)$$

Nous pouvons donc énoncer le résultat suivant.

3. Le résultat.

Théorème 8.1. *Soient A un corps de caractéristique nulle, a et b des éléments de $A(X)$, p et q deux entiers premiers entre eux.*
Si φ, élément de $A((X))$, vérifie les équations de Mahler:

$$\mu_p(\varphi) = a\varphi;\ \mu_q(\varphi) = b\varphi,$$

alors φ appartient à A.

Preuve :
Supposons tout d'abord A algébriquement clos. La démonstration précédente montre le résultat, tout au moins lorsque 0 n'est pas pôle ou zéro de a et b, et lorsque φ est de valuation 0. Mais la proposition 1.1 permet de se ramener à ce cas.

Dans le cas général, soit K un corps algébriquement clos contenant A. Alors φ appartient à $K(X)$; mais, comme φ appartient à $A((X))$, φ appartient nécessairement à $A(X)$ d'après une remarque déjà faite.

Annexe 1.

Fonctions élémentaires.

Pour ce qui concerne les notions de base relatives aux fonctions élémentaires, nous renvoyons à [10].

Dans cette annexe, D désigne un ouvert connexe (non vide) de $\mathbb{C}$, et $\mathcal{M}(D)$ le corps des fonctions méromorphes sur D, à valeurs complexes, muni de sa structure habituelle de corps différentiel. Si u est un élément de $\mathcal{M}(D)$, on notera R(u) l'ensemble des points de l'adhérence de D au voisinage desquels u est prolongeable en une fonction méromorphe ; le complémentaire de R(u) dans l'adhérence de D est noté S(u) ; c'est un sous-ensemble de la frontière de D, et il y est fermé.

Les trois lemmes qui suivent étudient dans quelle mesure on augmente l'ensemble des points singuliers d'une fonction lorsque l'on en prend l'exponentielle (lemme 1), lorsque l'on en prend le logarithme (lemme 2), et dans quelle mesure on augmente l'ensemble des points singuliers de plusieurs fonctions lorsque l'on considère la solution d'une équation algébrique dont elles sont les coefficients (lemme 3).

Pour indiquer qu'un point α n'est pas pôle d'une fonction méromorphe u, on notera :

$$u(\alpha) \neq \infty .$$

Le dérivé topologique d'un ensemble E, c'est-à-dire l'ensemble de ses points d'accumulation, est noté E'.

Lemme 1.

Soient u, dans $\mathcal{M}(D)$, et v, dans $\mathcal{M}(D)-\{0\}$, des fonctions telles que : $u' = \frac{v'}{v}$.

Alors : $R(u) \subset R(v)$.

Preuve.

Soit α dans R(u), et (u_1, Ω) un prolongement méromorphe de u à un voisinage ouvert de α . Posons :

$$v_1 = \exp(u_1).$$

Alors : $u'_1 = \frac{v'_1}{v_1}$; il en résulte que $\frac{v'}{v}$ et $\frac{v'_1}{v_1}$ coïncident sur D, donc qu'il existe λ dans $\mathbb{C}$ tel que :

$$v = \lambda v_1 \text{ sur D.}$$

Ainsi, la fonction λv_1 est un prolongement méromorphe de v sur Ω.∎

Lemme 2.

Soient u, dans $\mathcal{M}(D)-\{0\}$, et v, dans $\mathcal{M}(D)$, des fonctions telles que : $v' = \frac{u'}{u}$
L'ensemble $R(u) \cap S(v)$ n' a pas de point d'accumulation dans R(u).

Preuve.

Supposons au contraire que α, élément de R(u), soit un point d'accumulation de l'ensemble $R(u) \cap S(v)$. Soit alors (u_1, Ω) un prolongement méromorphe de u et considérons une boule ω, fermée, centrée en α, et incluse dans Ω ; si u_1 s'annulait en une infinité de points de ω, u_1 serait alors identiquement nulle sur ω, donc sur Ω, et u avec elle. Pour des raisons analogues, u_1 ne peut avoir une infinité de pôles dans ω.

Puisque $R(u) \cap S(v) \cap \omega$ est infini, il existe un point β de cet ensemble tel que : $u_1(\beta) \neq 0$ et $u_1(\beta) \neq \infty$. Soit à présent ω_1 un voisinage de β sur lequel u_1 n'a ni zéro ni pôle ; il existe une fonction v_1, holomorphe sur ω_1, telle que :

$$v'_1 = \frac{u'_1}{u_1}.$$

Or, sur $D \cap \omega_1$, qui est non vide puisque β appartient à S(v), on a :

$$v'_1 = \frac{u'_1}{u_1} = \frac{u'}{u} = v',$$

et par conséquent $v_1 - v$ est constante sur $D \cap \omega_1$. En retranchant cette constante à v_1, on obtient sur $D \cap \omega_1$ une fonction holomorphe prolongeant v, ce qui contredit le fait que β appartient à S(v).∎

Lemme 3.

Soient $u_0, u_1, \ldots, u_{m-1}$, v, des éléments de $\mathcal{M}(D)$ tels que :

$$v^m + u_{m-1}v^{m-1} + \ldots + u_1 v + u_0 = 0.$$

De plus, on suppose que le polynôme $X^m + u_{m-1}X^{m-1} + \ldots + u_1 X + u_0$ est séparable, comme élément de $\mathcal{M}(D)[X]$.

Dans ces conditions, l'ensemble $\bigcap_{i=0}^{m-1} R(u_i) \cap S(v)$ n'a pas de point d'accumulation dans $\bigcap_{i=0}^{m-1} R(u_i)$.

Preuve.

Soit, par l'absurde, α un tel point ; considérons un ouvert Ω tel que, quel que soit i, (w_i, Ω) soit un prolongement méromorphe de (u_i, D) ; l'ensemble des pôles des fonctions w_i est discret.

Par ailleurs, le polynôme $X^m + u_{m-1}X^{m-1} + ... + u_1X + u_0$, noté P, a un discriminant non identiquement nul ; son prolongement méromorphe à Ω , noté δ, donné par ceux des u_i, a lui aussi un ensemble de pôles qui est discret. De plus, δ ne s'annule qu'en un ensemble discret de Ω, grâce à un argument déjà employé dans le lemme 2 . La réunion des différents ensembles précédents est encore discrète.

Elle n'est donc pas égale à $\bigcap_{i=0}^{m-1} R(u_i) \cap S(v)$, ce qui signifie qu'il existe un point β appartenant à l'ensemble précédent qui ne soit pôle d'aucun des w_i, et qui ne soit pas zéro de δ ; cette condition est alors vérifiée dans un voisinage ω_1 de β.

D'après le théorème des fonctions implicites holomorphes, il existe une boule ouverte ω_2, centrée en β , incluse dans ω_1, sur laquelle le polynôme P admette exactement m racines holomorphes $v_1, ..., v_m$.

Puisque β est dans S(v), $\omega_1 \cap D$ est non vide ; soit z_0 un élément de $\omega_1 \cap D$; puisque $v(z_0)$ est solution de l'équation, à l'inconnue complexe x :

$$x^m + u_{m-1}(z_0)\, x^{m-1} + ... + u_1(z_0)\, x + u_0(z_0) = 0,$$

$v(z_0)$ est égal à l'un des $v_i(z_0)$. Il en résulte, à nouveau grâce au théorème des fonctions implicites holomorphes, que v et v_i coïncident sur un voisinage de z_0, donc sur $\omega_1 \cap D$; cela entraîne que v admet un prolongement holomorphe sur un voisinage de β. Pourtant, β appartient à S(v).∎

Théorème.

Soit t un élément de $\mathcal{M}(D)$ qui soit une fonction élémentaire (sur $\mathbb{C}(x)$). Il existe un entier n tel que :

$$(S(t))^{(n)} = \varnothing .$$

Preuve.

Appelons hauteur d'une fonction élémentaire la longueur minimale d'une chaîne d'extensions de l'un des trois types fondamentaux nécessaire pour

l'atteindre. Les fonctions élémentaires de hauteur 0 étant les fractions rationnelles, le résultat est bien vrai pour n = 0.

Supposons-le vrai pour les hauteurs inférieures ou égales à n, et soit t une fonction élémentaire de hauteur n+1. Il existe une extension élémentaire L de $\mathbb{C}(x)$, dont tous les éléments sont de hauteur inférieure ou égale à n, et un élément v de $\mathcal{M}(D)$, de l'une des trois formes fondamentales sur L, tels que t appartienne à L(v). Montrons tout d'abord que :

$$(S(v))^{(n+1)} = \varnothing .$$

∴ *Premier cas : il existe u dans L tel que* $u' = \frac{v'}{v}$.

Le lemme 1 assure que : R(u) ⊂ R(v), c'est-à-dire que : S(v) ⊂ S(u). Dans ce cas, on a évidemment : $(S(v))^{(n)} = \varnothing$.

∴ *Deuxième cas : il existe u dans L- {0} tel que* $v' = \frac{u'}{u}$.

D'après le lemme 2, R(u) ∩ S(v) n' a pas de point d'accumulation dans R(u), ce qui peut encore s'écrire :

$$\Big(R(u) \cap S(v)\Big)' \subset S(u).$$

Or :

$S(v) = (R(u) \cap S(v)) \cup (S(u) \cap S(v))$; donc :

$(S(v))' = (R(u) \cap S(v))' \cup (S(u) \cap S(v))'$; soit :

$(S(v))' \subset S(u) \cup (S(u))'$.

Comme S(u) est fermé, on a : $(S(v))' \subset S(u)$, ce qui entraîne le résultat.

∴ *Troisième cas : v est algébrique sur L.*

Soit $X^m + u_{m-1}X^{m-1} + ... + u_1X + u_0$ le polynôme minimal de v sur L ; c'est un polynôme irréductible, comme élément de L[X]. Puisque L est de caractéristique nulle, ce polynôme est séparable.

D'après le lemme 3, $\left(\bigcap_{i=0}^{m-1} R(u_i) \cap S(v)\right)'$ est inclus dans la réunion des $S(u_i)$.

On a :

$$S(v) = \left(\bigcap_{i=0}^{m-1} R(u_i) \cap S(v)\right) \cup \left(\bigcup_{i=0}^{m-1} S(u_i) \cap S(v)\right), \text{ puis :}$$

$$(S(v))' = \left(\bigcap_{i=0}^{m-1} R(u_i) \cap S(v)\right)' \cup \left(\bigcup_{i=0}^{m-1} S(u_i) \cap S(v)\right)', \text{ soit :}$$

$$(S(v))' \subset \bigcup_{i=0}^{m-1} S(u_i) \cup \left(\bigcup_{i=0}^{m-1} S(u_i) \cap S(v)\right)', \text{ ou encore :}$$

$$(S(v))' \subset \bigcup_{i=0}^{m-1} S(u_i) \cup \left(\bigcup_{i=0}^{m-1} S(u_i)\right)' = \bigcup_{i=0}^{m-1} S(u_i).$$

Il vient alors :

$$(S(v))^{(n+1)} \subset \left(\bigcup_{i=0}^{m-1} S(u_i)\right)^{(n)} = \bigcup_{i=0}^{m-1} (S(u_i))^{(n)} = \varnothing .$$

Pour conclure, puisque t est dans L(v), on constate que les points singuliers de t appartiennent à une réunion finie d'ensembles dont les dérivés (n+1)-ièmes sont vides.∎

Annexe 2.

Ordre sur $K[X_0,\ldots,X_n,\ldots]$.

Nous considérons ici l'anneau des polynômes à une infinité dénombrable d'indéterminées sur un corps commutatif K. Pratiquement, on pourra se limiter à $K[X_0,\ldots,X_n]$, avec dans ce cas pour seul inconvénient d'avoir à spécifier n.

Nous avons déjà vu [ch.1] comment munir d'un ordre lexicographique l'ensemble des monômes X^α, notation désignant, *lorsque* α *est égal au* $(n+1)$-uplet $(\alpha_0,\alpha_1,\ldots,\alpha_n)$, le monôme $X_0^{\alpha_0} X_1^{\alpha_1} \ldots X_n^{\alpha_n}$. Cet ordre lexicographique est un bon ordre sur l'ensemble des monômes de $K[X_0,\ldots,X_n,..]$. Les monômes sont d'autant plus grands que les variables d'indices plus élevés ont des exposants plus grands.

Maintenant, un polynôme peut s'écrire, de façon unique, comme combinaison linéaire de monômes rangés dans l'ordre décroissant. A ce polynôme, on peut ainsi associer la famille des monômes affectés d'un coefficient non nul. Il ne s'agit alors pas d'une identification (sauf sur le corps à deux éléments!) puisque, par exemple, $X_0 + X_0^2$ d'une part, $X_0 - X_0^2$ d'autre part, sont associés à la même famille. On peut munir la famille de ces familles de monômes de l'ordre lexicographique associé à l'ordre sur les monômes, toujours en partant du monôme le plus élevé. Nous disposons ainsi d'une relation réflexive et transitive sur $K[X_0,\ldots,X_n,..]$, notée $\leq$. Par exemple :

$$X_1^2 + X_1 + X_0 \leq X_1^2 + X_1 X_0 ;$$

$$X_1^2 \leq X_3 ;$$

$$X_0 + X_0^2 \leq X_0 - X_0^2 ;$$

$$X_0 - X_0^2 \leq X_0 + X_0^2 ;$$

$$0 \leq 1.$$

Si l'on note $\simeq$ la relation d'équivalence associée à ce préordre, on obtient l'ordre strict associé à $\leq$ grâce la définition :

$P < Q$ lorsque : $P \leq Q$ et non($P \simeq Q$).

Proposition 1.

Soit $\mathcal{E}$ un sous-ensemble non vide de $K[X_0,...,X_n,..]$; $\mathcal{E}$ admet un plus petit élément.

Preuve.

Posons $h(\mathcal{E}) = \min \{ n \in \mathbb{N} \quad \mathcal{E} \cap K[X_0,...,X_{n-1}] \neq \varnothing \}$. Bien entendu, K est identifié à l'espace des polynômes en aucune variable. Montrons le résultat par récurrence sur $h(\mathcal{E})$. Il est clair si $h(\mathcal{E})$ est nul. Supposons le vrai pour : $h(\mathcal{E}) = m$.

Lorsque : $h(\mathcal{E}) = m+1$, soit :

$$\mathcal{F} = \mathcal{E} \cap K[X_0,...,X_m].$$

Il suffit évidemment de monter que $\mathcal{F}$ admet un plus petit élément. Parmi les éléments de $\mathcal{F}$, considérons ceux de degré en X_m minimal, qui forment un ensemble $\mathcal{G}$. Notons d ce degré. Les éléments P de $\mathcal{G}$ s'écrivent :

$$\sum_{i=0}^{d} P_i \, X_m^i$$

où les P_i sont dans $K[X_0,...,X_{m-1}]$. La notation P_i renvoie à la dépendance par rapport à P. Choisissons (hypothèse de récurrence) P tel que :

$$P_d = \min \{ Q_d \quad Q \in \mathcal{G} \},$$

puis, en notant $\mathcal{G}_d$ l'ensemble des polynômes Q de $\mathcal{G}$ tels que Q_d soit égal à P_d ,un polynôme R tel que :

$$R_{d-1} = \min \{ Q_{d-1} \quad Q \in \mathcal{G}_d \},$$

et ainsi de suite. On construit ainsi un plus petit élément de $\mathcal{G}$, donc de $\mathcal{F}$.∎

Bien que la relation ≤ ne soit qu'une relation de préordre, on peut raisonner par récurrence sur les éléments de $K[X_0,...,X_n,..]$ de la façon habituelle, à condition de ne pas oublier qu'une propriété peut être vraie pour un polynôme sans être vraie pour les polynômes équivalents.

On peut, pour appliquer le raisonnement par récurrence, utiliser la proposition suivante:

Proposition 2.

Si P est un élément non nul de $K[X_0,...,X_n,..]$, et m un entier naturel, on a :

$$\frac{\partial P}{\partial Y_m} < P.$$

Preuve.

Si P est un monôme, le résultat est clair. Dans le cas général, il suffit de constater que le plus grand monôme affecté d'un coefficient non nul est lui-même strictement diminué.∎

Annexe 3.

Extensions différentielles.

1 .Corps différentiels.

Soit K un corps. On appelle dérivation sur K une application additive de K dans lui-même, notée ' ,vérifiant :

$$\forall\ (u,v) \in K^2 \quad (uv)' = u'v + uv' .$$

Les formules habituelles sont vérifiées :

→ formule de Leibniz sur le produit ;

→ dérivée d'un quotient : $\left(\frac{u}{v}\right)' = \frac{u'v - uv'}{v^2}$;

→ dérivée logarithmique : si $u = \prod u_i$, alors : $\frac{u'}{u} = \sum \frac{u_i}{u_i}$.

Les éléments de L dont la dérivée est nulle forment un sous-corps C de L, appelé corps des constantes. La dérivation est alors C-linéaire.

Si L est le corps des fonctions méromorphes sur l'ouvert connexe D de $\mathbb{C}$, son corps des constantes est (identifié à) $\mathbb{C}$.

Si K est un corps quelconque, on dispose sur K(X) de la dérivation canonique, dont le corps des constantes est, en caractéristique nulle, le corps K lui-même.

Soit $K \subset L$ une extension différentielle, c'est-à-dire une extension de corps différentiels, la dérivation de L prolongeant celle de K. Si P appartient à $K[X_1, ..., X_n]$, et si $(x_1, ..., x_n)$ est une famille de L^n, on vérifie la formule :

$$\{P(x_1, ..., x_n)\}' = P'(x_1, ..., x_n) + \sum_{i=1}^{n} \frac{\partial P}{\partial X_i}(x_1, ..., x_n)\ x_i'$$

Ici, P' désigne le polynôme obtenu à partir de P en en dérivant les coefficients.

2 Différentielle algébricité.

Soit $K \subset M$ une extension différentielle. Tous les éléments considérés sont dans M.

On dit que la famille $(x_i)_{i\in I}$ est différentiellement liée sur K si la famille :

$$(x_i)_{i\in I} \cup (x_i')_{i\in I} \cup \ldots.$$

est algébriquement liée sur K. En d'autres termes, il existe une relation de dépendance algébrique non triviale, à coefficients dans K, entre les dérivées des x_i. Dans le cas d'un seul élément x, on dira que x est différentiellement algébrique sur K. Dans le cas contraire, on parlera de famille différentiellement

libre, ou d'élément différentiellement transcendant. On rencontre aussi, dans ce cas, la teminologie " élément hypertranscendant".

Proposition 1.

Soient $K \subset M$ une extension différentielle de corps de caractéristique nulle, et x un élément de M. Les propriétés ci-dessous sont équivalentes :

(1) x est différentiellement algébrique sur K.;

(2) il existe un entier naturel p tel que :

$$x^{(p+1)} \in K\left(x, \ldots, x^{(p)}\right) ;$$

(3) il existe un entier naturel p tel que :

$$K\left(x^{(k)}\right)_{k\in\mathbb{N}} \subset K\left(x, \ldots, x^{(p)}\right) ;$$

(4) la dimension de transcendance de $K\left(x^{(k)}\right)_{k\in\mathbb{N}}$ sur K est finie;

(5) x appartient à une extension différentielle de K, de dimension de transcendance sur K finie.

Dans la suite, les corps K,L,M sont de caractéristique nulle, et seront tous stable par la dérivation, sauf mention du contraire.

Proposition 2.

Sous les hypothèses de la proposition 1, il existe un plus petit polynôme unitaire annulant la famille $\left(x^{(k)}\right)_{k\in\mathbb{N}}$. Ce polynôme est unique.

Remarquons que le polynôme précédent, que l'on qualifiera de polynôme minimal de x sur K, n'est en général pas un générateur de l'idéal de $K[X_1, \ldots, X_n, \ldots]$ formé des polynômes annulant la famille $\left(x^{(k)}\right)_{k\in\mathbb{N}}$.

Exemple.

Si $K = \mathbb{C}$, et $M = \mathcal{M}(\mathbb{C})$, le polynôme minimal de sin est :

$$P(X_0,X_1) = X_0^2 + X_1^2 - 1.$$

Il ne divise pas $X_2 - X_0$.

Proposition 3.

Soit x un élément de M, différentiellement algébrique sur L, lui-même extension différentiellement algébrique de K. Alors x est différentiellement algébrique sur K.

Proposition 4.

Soit ∂K l'ensemble des éléments de M qui sont différentiellement algébriques sur K. Alors ∂K est un corps, extension différentielle de K.

Supposons à présent que nous disposions, dans le corps M, extension différentielle du corps K, d'un élément ϕ et d'un monomorphisme de M dans M, qui à l'élément x associe l'élément $x\circ\phi$, et qui vérifie de plus :

$$(x\circ\phi)' = x'\circ\phi.\phi' .$$

Bien entendu, cette application fait allusion à la composition, dans le cadre formel, ou bien fonctionnel.

Proposition 5.

Notons $K\circ\phi$ l'ensemble image de K par $x \longmapsto x\circ\phi$. Si x est différentiellement algébrique sur K, alors $x\circ\phi$ est *différentiellement algébrique sur* $K\circ\phi$ $\left(\phi^{(k)}\right)_{k\in\mathbb{N}}$.

En particulier, si ϕ est aussi différentiellement algébrique sur K, alors $x\circ\phi$ est différentiellement algébrique sur $K\circ\phi$

Proposition 6.

Soit $K \subset M$ une extension différentielle de corps , où M est de la forme :

$$K\left(b_i^{(k)}\right)_{i\in I,k\in\mathbb{N}} ,$$

la famille $\left(b_i^{(k)}\right)_{i\in I,k\in\mathbb{N}}$ étant algébriquement libre.

Notons ∂K l'ensemble des éléments de M qui sont différentiellement algébriques sur K. Alors :

$$\partial K = K.$$

Questions.

Chapitre 2.

Soit A un corps. Le théorème 2.1 nous fournit les sous-corps p-mahlériens de A(X), c'est-à-dire les sous-corps de A(X) stables par la substitution de X^p à X, *tout au moins lorsque la caractéristique de A ne divise pas p.* L'étude pourrait être faite sans hypothèse de caractéristique, et ne semble pas soulever de problème.

En revanche, l'étude des sous-algèbres p-mahlériennes de A(X) semble conduire à des situations plus diverses ; il semble intéressant de les caractériser.

Cette étude peut être généralisée de plusieurs points de vue : que se passe-t-il si A n'est qu'une algèbre ? Quelle situation a-t-on lorsque B est un sous-corps p-mahlérien de A((X)) ? La réponse est évidente si, par exemple, B ne contient pas d'élément non dans A vérifiant une équation algébrique de Mahler sur A.

Le théorème 2.2 ne permet pas de résoudre complètement une équation de Mahler linéaire sur le A, lorsque A n'est pas intègre.

Le théorème 2.3 est notablement insuffisant pour décrire les rapports entre solutions dans $\mathbb{C}((X))$ et celles qui sont dans $\mathcal{M}(D)$; cela est dû au fait que la dépendance de la solution vis-à-vis de la condition initiale n'est pas précisée. Une telle étude serait souhaitable en vue du transfert de résultats obtenus analytiquement à la situation des séries formelles.

Chapitre 3.

*Le chapitre 3 pose davantage de questions qu'il n'en résout.*Le théorème 3.1 caractérise matriciellement, en faisant intervenir des séries parasites, les *séries génératrices de suites p-régulières. Il conviendrait de caractériser, tout* d'abord dans le cas d'un corps, ces fonctions génératrices, à l'aide du générateur, *normalisé par la condition d'être primitif,* de l'idéal annulateur de $A(X)[\mathfrak{m}]$. On peut conjecturer que ces générateurs seront caractérisés par le fait que leur coefficient b_0 est solution d'une équation de Mahler résoluble à droite.

L'étude de $B[\mathfrak{m}]$ devrait permettre d'établir des rapports plus nets entre *équations linéaires et équations homographiques.*

Sur $\mathfrak{R}(B)$, on doit en premier lieu se poser la question de la recherche de ses inversibles, question posée par Allouche et Shallit déjà dans le cas où B est A[X]. Outre les questions standard de l'algèbre commutative, on aimerait savoir si $\mathfrak{R}(B)$ est stable par le produit de Hadamard.

Chapitre 4.

Les questions qui se posent, dans le prolongement du théorème Antoine et Claudia, relèvent de l'étude d'une fonction méromorphe sur le disque unité ouvert au voisinage des points du cercle.En fait, en relation avec le chapitre 1 et le corollaire 2 suivant le théorème 4.2, on aimerait étendre le résultat de *transcendance à un corps quelconque, de caractéristique nulle.*

Chapitre 5.

La conjecture générale est la suivante : si A est de caractéristique nulle, les éléments de $ML_p(A[X])$ sont différentiellement transcendants sur A[X], ou dans A[X]. L'extension porte dans deux directions : vers la généralité du corps de base, c'est-à-dire vers un substitut de l'exponentielle, mais surtout, vers l'ordre de l'équation considérée, qui devient quelconque.

Chapitre 6.

En relation avec [14], on se pose la question de déterminer des classes d' équations de Mahler algébriques sur $\mathbb{C}(x)$, dont les éléments sont, soit dans $\mathbb{C}(x)$, soit transcendants sur $\mathbb{C}(x)$.

Par exemple : si f vérifie une équation algébrique de Mahler sur $\mathbb{C}(x)$ résolue en f, et si f est entière sur $\mathbb{C}$, est-elle polynomiale ?

Chapitre 7.

La conjecture de Loxton et van der Poorten est intacte ; en fait, pour que les techniques utilisées puissent s'appliquer au cas général, il faudrait pouvoir répondre à la question : si A, B sont dans $GL_{n,n}\left(\mathbb{C}(x)\right)$, et vérifient : $A(x)\,B(x^2) = B(x)\,A(x^3)$, peut on en déduire que A est μ_2-conjuguée à une matrice triangulaire par blocs.?

Questions générales.

Les chapitres 4 et 5 permettent d'obtenir des classes de fonctions méromorphes transcendantes, ou encore des familles de fonctions algébriquement indépendantes, afin éventuellement d'appliquer les méthodes développées en [13]. Peut-on répondre ainsi à la conjecture d'Allouche et Shallit sur la transcendance des valeurs prises par une fonction p-régulière aux inverses des nombres entiers ? Peut-on obtenir l'indépendance algébrique des valeurs prises en un point algébrique par les dérivées successives d'une fonction qui vérifie une équation de Mahler d'ordre un à coefficients rationnels ?

Références bibliographiques.

[1] J.-P. Allouche et J. Shallit, *The ring of k-regular sequences*, Theoret. Comput. Sci., 98 (1992), 163-197.

[2] P. Dumas, *Les séries formelles B-régulières*, Preprint, (1991).

[3] O. Hölder, *Mémoire sur la fonction gamma*, Math. Ann., (1887), 1-13.

[4] L. A. Rubel, *Some research problems about algebraic differential equations, part II*, Preprint, (l'article au même titre *"Part I"* est paru aux Trans. Amer. Math. Soc., 280 (1983), 43-52).

[5] S. Lang, *Algebra*, Addison-Wesley Publishing Company, 1965.

[6] J.-P. Allouche, B. Randé, L. Thimonier, *Fonctions génératrices transcendantes engendrées par automates*, Lecture Notes in Computer Science, n° 294, Stacs 88, 1988, 170-183.

[7] J. H. Loxton et A. J. van der Poorten, *A class of hypertranscendental functions*, Aequationes Mathematicae, 16 (1977), 93-106.

[8] L. A. Rubel, *A survey of transcendentally transcendental functions*, Amer. Math. Monthly, 96 (1989), 777-788.

[9] P. Dolbeault, *Analyse complexe*, Masson, 1990

[10] B. Randé, *Primitives élémentaires*, Revue de Mathématiques Spéciales, 1983-84, 375-381.

[11] P. Borwein, *Hypertranscendence of the functional equation* $g(x^2) = (g(x))^2 + cx$, Proc. Amer. Math. Soc., 107 (1989), 215-221.

[12] J. H. Loxton et A. J. van der Poorten, *On algebraic functions satisfying a class of functional equations*, Aequationes Mathematicae, 14, (1976), 413-420.

[13] F. Gramain, M. Mignotte, M. Waldschmidt, *Valeurs algébriques de fonctions analytiques*, Acta Arith., 47, (1986), 97-121.

[14] R. Louboutin, *Solutions analytiques d'une équation fonctionnelle*, Cr. Acad. Sci. Paris, Sér. I, t.311, (1990),.291-293.

[15] K. Nishioka, *New approach in Mahler's method*, J. reine angew. Math., 407 (1990), 202-210.

[16] J. H. Loxton et A. van der Poorten, *Transcendance and algebraic independence by a method of Mahler*, in Transcendence Theory: Advances and Applications, eds. A. Baker and D. W. Masser, Academic Press, London and New York, 1977.

[17] A. Cobham, *Uniform tag sequences*, Math. Systems Theory, 6 (1972), 164-192.

[18] A. Cobham, *On the base-dependence of sets of numbers recognizable by finite automata*, Math. Systems Theory, 3 (1969), 186-192.

[19] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France 108 (1980), 401-419.

[20] M. Dekking, M. Mendès France et A. J. van der Poorten, *FOLDS!*, Math.Intell., 4 (1982), 130-138, 173-181, 190-195.

[21] J.-P. Allouche, *Automates finis en théorie des nombres*, Expo. Math., 5, (1987) , 239-266.

RÉSUMÉ.

Le concept de suite p-régulière, introduit par Allouche et Shallit, généralise celui de suite p-automatique. La série génératrice d'une telle suite est considérée, tantôt comme une série formelle, tantôt comme une fonction holomorphe (dans le cas complexe); elle vérifie une équation fonctionnelle linéaire, dite *de Mahler*. Ce travail étudie ces équations fonctionnelles de façon générale, pour les appliquer au cas particulier des suites p-régulières.

Le cadre formel est celui des chapitres 1, 2 et 3. On y étudie certaines structures mahlériennes. Le chapitre 4 montre la transcendance des solutions non rationnelles, par l'étude de leurs singularités. On étend ainsi un résultat bien connu dans le cas automatique. Le chapitre 5, répondant à une question posée par Rubel, montre que, dans un cas, les solutions non rationnelles sont différentiellement transcendantes (ou *hypertranscendantes*). Le chapitre 7, reprenant des méthodes bien connues, s'appuie sur le chapitre 4 pour établir la transcendance des valeurs prises, s'intéressant ainsi à une question posée par Allouche et Shallit. Le chapitre 8 montre un résultat très partiel en direction d'une conjecture de Loxton et van der Poorten. Le chapitre 6 esquisse une étude dans le cas non linéaire.

Mots-clés.
Équations fonctionnelles, équations de Mahler, suites p-régulières, suites p-automatiques, transcendance, hypertranscendance.