Récurrences mahlériennes, suites automatiques, études asymptotiques

Philippe Dumas

Numéro d'ordre : 952 Deuxième édition 2009

THÈSE

PRÉSENTÉE

À L'UNIVERSITÉ BORDEAUX I

POUR OBTENIR

LE TITRE DE DOCTEUR EN MATHÉMATIQUES

PAR PHILIPPE DUMAS

RÉCURRENCES MAHLÉRIENNES, SUITES AUTOMATIQUES, ÉTUDES ASYMPTOTIQUES.

Soutenue le 2 Septembre 1993, devant le jury composé de :

Michel MENDÈS FRANCE	Président
Jean-Paul ALLOUCHE	Directeur de thèse
Jean BERSTEL	Rapporteur
Louis COMTET	
Philippe FLAJOLET	
Gérald TENENBAUM	Rapporteur

RÉCURRENCES MAHLÉRIENNES, SUITES AUTOMATIQUES, ÉTUDES ASYMPTOTIQUES.

Philippe Dumas

Projet Algorithmes
INRIA Rocquencourt BP 105
78153 Le Chesnay Cedex
France
Philippe.Dumas@inria.fr

Avant-propos

Il n'est guère de notion plus banale que la numération de position utilisée depuis quelque quarante siècles [44] pour coder les nombres entiers. Cependant cette structure si pauvre cache des trésors et la raison essentielle en est son ubiquité : nous employons tous cette notation et c'est souvent avec elle que nous exprimons les propriétés des nombres. Ainsi en arithmétique la preuve par neuf utilise-t-elle un calcul simple sur les écritures décimales ou encore, pour donner un exemple plus sophistiqué, un nombre comme trois cent cinquante mille deux cent cinquante six est somme de trois carrés d'entiers parce que son écriture binaire, 1010101100000110000, se termine par le bloc 011 suivi d'un nombre pair de 0. Cette richesse aura pour nous une source complémentaire, qui est la puissance d'une idée simple, la bissection. Diviser un problème en deux pour le traiter plus facilement est une idée fondamentale, qui est à la base des algorithmes *diviser pour régner*. Ainsi pour trier par ordre alphabétique la liste des passagers d'un avion, une méthode rapide consiste à séparer la liste en deux parties à peu près égales, à trier séparément chacune d'elles puis à fusionner ces deux demi-listes triées. Le nombre de comparaisons effectuées entre les noms des passagers dépend de l'écriture binaire du nombre de passagers.

La représentation des entiers fait intervenir la théorie des langages formels : un chiffre est une lettre d'un alphabet particulier et l'écriture d'un nombre est un mot sur cet alphabet. Les écritures d'entiers sont les mots qui ne commencent pas par un zéro. Comme le fait remarquer J. Berstel [12], chaque avancée de la théorie des langages s'est reflétée dans des concepts liés à la numération. On a ainsi vu fleurir les concepts d'ensemble reconnaissable de nombres, puis de suite automatique. Ces notions ont été illustrées par deux types d'exemples, soit directement liés à la numération, comme la suite de Thue-Morse qui donne la parité du nombre de 1 dans l'écriture binaire d'un entier, mais ils restent alors à l'intérieur de la théorie, soit des exemples exogènes comme les suites de pliage de papier, qui énumèrent les plis d'une bande de papier que l'on a pliée sur elle même un grand nombre de fois puis redépliée. Ces exemples sont tout à fait intriguants et excitants mais demeurent souvent cantonnés dans le domaine de la curiosité intellectuelle. La raison essentielle en est que les suites automatiques ne prennent qu'un nombre fini de valeurs ; elles permettent seulement de représenter des phénomènes dont la complexité surpasse légèrement celle des phénomènes périodiques.

La notion de suite B-régulière libère les suites automatiques des contraintes de finitude au prix d'un effort minime et rapidement compensé par un formalisme algébrique agréable. D'objets curieux, elles passent à un statut de concept utile que tout informaticien devra bientôt connaître, car la stratégie *diviser pour régner*, que nous évoquions plus haut, fait naturellement apparaître des suites 2-régulières. L'étude de ces suites se déroule comme un long fleuve tranquille et fait émerger une classe plus générale de suites, les suites mahlériennes, dont le prototype est la suite du nombre de partitions binaires, qui comptent le nombre de façons d'écrire un entier comme somme de puissances de deux. Celles-ci constituent véritablement le sujet de cette thèse. Elles nous ont attiré par leur aspect de prime abord déroutant, qui finalement s'ordonne sous l'effet de l'algèbre, et aussi par la variété des techniques employées dans leur analyse, qui vont d'arguments tout à fait élémentaires à des méthodes sophistiquées de théorie analytique des nombres. Nous toucherons ainsi à la théorie des langages, l'algorithmique, la combinatoire, l'arithmétique en employant l'algèbre linéaire, l'arithmétique des polynômes, l'analyse complexe et le calcul asymptotique. Notre thèse et notre plaisir sont en fait bien là, dans cette unité, dans ce passage, cette traduction d'une notion, d'un domaine à un autre, dans l'illustration d'un concept élevé par un exemple commun mais vu sous un jour nouveau.

Introduction

Cette thèse a pour objet l'étude d'une classe de séries entières solutions de certaines équations fonctionnelles linéaires, dites de Mahler. Une sous-classe importante est constituée des séries B-régulières qui sont liées à la numération en base B.

Les séries mahlériennes forment une algèbre stable par dérivation et contenant les fractions rationnelles, analogue des séries holonomes de l'algèbre différentielle. Pour celles-ci l'opérateur de base est la dérivation et pour les séries mahlériennes l'opérateur fondamental est la substitution de z^B à z, ce qui traduit en pratique une relative invariance d'échelle par rapport à la taille des structures concernées. Elles unifient plusieurs domaines. Elles apparaissent en effet en combinatoire dans des problèmes de comptage de mots ou dans l'énumération de partitions d'entiers contraintes. On les rencontre aussi en analyse d'algorithmes où fleurissent les récurrences *diviser pour régner*, pour lesquelles le principe même est de jouer sur un phénomène d'échelle. Enfin elles se réduisent aux séries algébriques si le corps de base est fini et l'entier B est la caractéristique du corps.

Ce dernier point, évident en lui même, est important car il ouvre la porte à toute la littérature sur les suites automatiques à valeurs dans un corps fini. Les séries génératrices de ces suites sont en effet algébriques sur le corps des fractions rationnelles, d'après le théorème de Christol, Kamae, Mendès France et Rauzy. L'extension des séries automatiques aux séries B-régulières, due à Allouche et Shallit, amène à reprendre le lien entre séries automatiques et séries algébriques. Les séries B-régulières sont la traduction des séries rationnelles en indéterminées non commutatives de la théorie des langages par l'intermédiaire de la numération en base B. À ce titre elles héritent de tout un appareillage algébrique plaisant et efficace, comme les représentations linéaires, la matrice de Hankel ou la condensée, analogue de la notion de densité pour les langages. Les séries B-régulières sont mahlériennes, comme nous l'avons déjà indiqué, et la réciproque est vraie moyennant une condition simple. Il en résulte que les récurrences *diviser pour régner* sont dans leur majorité B-régulières et cela fournit un grand champ d'application de cette notion.

L'étude des séries mahlériennes pose essentiellement deux problèmes : d'une part la résolution des équations mahlériennes, d'autre part l'asymptotique des coefficients des séries mahlériennes complexes. La résolution des équations de Mahler linéaires repose sur deux types de résultat ; d'abord le comportement des fractions rationnelles vis-à-vis de l'opérateur fondamental, qui structure les polynômes en arborescence et met en valeur le rôle particulier des polynômes cyclotomiques en caractéristique nulle ; ensuite l'arithmétique des opérateurs sous-jacents à ces équations, qui est assez similaire à l'arithmétique élémentaire des entiers. L'utilisation conjointe de ces deux outils permet de donner des méthodes effectives de calcul, par exemple pour obtenir les solutions rationnelles d'une telle équation. En ce sens ce travail s'inscrit dans le développement actuel du calcul formel qui tend à automatiser les calculs mathématiques classiques. Elle fournit aussi des résultats qualitatifs ; dans le cas complexe les séries mahlériennes définissent des fonctions méromorphes dans le disque unité.

L'analyse asymptotique des suites mahlériennes a déjà donné lieu à de nombreux travaux en

combinatoire ou en analyse d'algorithmes. Nous privilégions une approche globale en introduisant une classification qui donne un grand rôle aux séries B-régulières et aux produits infinis mahlériens. Les méthodes employées sont de deux types, élémentaires, ce qui permet de dégrossir les problèmes, ou sophistiquées comme en théorie analytique des nombres et ceci fournit des développements asymptotiques complets. Nous traitons en particulier un exemple dans son intégralité, généralisant ainsi un travail de De Bruijn sur les partitions B-aires, où l'on voit fonctionner la méthode du cercle dans un cadre inhabituel. Deux points émergent particulièrement : un comportement dominant des suites B-régulières lié aux valeurs propres d'une représentation linéaire et des fluctuations périodiques en échelle logarithmique cachées mais maintenant classiques pour les suites mahlériennes disons non triviales.

Le texte est structuré en trois parties et huit chapitres. La première partie (chapitres 1 à 3) porte sur l'algèbre des séries mahlériennes. La deuxième (chapitres 4 à 6) est consacrée aux séries B-régulières et la troisième (chapitres 7 et 8) concerne l'asymptotique des suites mahlériennes.

1. Dans le premier chapitre nous nous intéressons à des résultats techniques surtout utilisés aux chapitres 3 et 6, comme l'étude des périodes de fractions rationnelles sur un corps fini dans l'esprit du théorème de Berlekamp. Nous mettons ainsi en place l'opérateur fondamental, baptisé opérateur de Mahler, et les opérateurs de section, qui trient les coefficients d'une série suivant le résidu modulo B de l'indice et qui seront essentiels dans l'analyse des séries B-régulières.

2. L'arithmétique des opérateurs mahlériens est développée dans le chapitre 2. Une division euclidienne unilatérale permet un traitement similaire à l'arithmétique de notre enfance et les notions de pgcd ou de ppcm sont effectives. La non commutativité complique un peu la situation mais l'algèbre linéaire sauve la mise.

3. Le chapitre 3 donne les propriétés de clôture des séries mahlériennes, montre comment obtenir les séries formelles solutions d'une équation de Mahler à une précision donnée et enfin permet de déterminer des solutions sous formes closes. Les résultats saillants en sont l'existence d'un entier critique qui scinde la résolution en deux temps, d'abord un système linéaire en dimension finie puis une équation de point fixe ; l'effectivité des calculs autant pour les solutions approchées que pour les solutions closes ; des conséquences qualitatives avec par exemple un critère d'Eisenstein. Nous verrons aussi des produits infinis qui se réduisent à des fractions rationnelles comme l'identité d'Euler de la théorie des partitions.

4. Avec le chapitre 4 commence l'étude des séries B-régulières et la traduction des propriétés des séries rationnelles en indéterminées non commutatives. Il ne présente guère de surprise pour qui est familier de ces séries. Nous n'avons pas essayé d'être exhaustif mais plutôt de mettre en valeur le passage d'un type de séries à l'autre. Le point le plus frappant nous semble être la quantité d'exemples naturels qui viennent à l'esprit quand on étudie ces séries et nous n'avons pas hésité à donner une abondante illustration. Insistons cependant sur le fait qu'ici aussi beaucoup de calculs sont effectifs et ont d'ailleurs été programmé et exécuté avec l'aide du calcul formel.

5. Une série B-régulière est solution d'une équation mahlérienne non triviale et ceci fournit la matière du chapitre 5, dans lequel nous donnons un procédé de calcul d'une telle équation. Nous n'avons pas résisté au plaisir d'ajouter une preuve de ce résultat fondée sur la stabilité par les opérations rationnelles d'une classe d'opérateurs ; elle n'est certes pas effective mais met en valeur l'esprit de cette partie.

6. Le chapitre 6 a pour but d'établir une réciproque au résultat du chapitre 5. Nous exhibons un critère dont la condition essentielle stipule qu'un certain produit infini mahlérien est B-régulier. Ce critère permet de retrouver et de généraliser le théorème de Christol *et alii*, y compris à des

anneaux quotients de l'anneau des entiers. Il s'applique aussi dans le corps des complexes et s'étend à des séries vectorielles, ce qui permet de considérer des suites vérifiant une récurrence exprimée suivant le résidu modulo une puissance de B, comme il est fréquent dans la pratique. Le théorème de Christol *et alii* n'est ainsi plus confiné aux corps finis et dans cette nouvelle version s'applique par exemple à des suites de complexes ou des suites d'entiers réduite suivant un certain module.

7. Quelques idées générales sur l'asymptotique des suites mahlériennes sont exposées dans le chapitre 7. Une série mahlérienne s'écrit comme le quotient d'une série B-régulière et d'un produit infini mahlérien et B-régulier. Ceci permet d'établir une classification qui subdivise cette étude difficile en plusieurs sous-problèmes plus abordables. Le premier concerne les suites B-régulières, pour lesquelles nous établissons un lien assez fort entre l'ordre de croissance et le spectre d'une représentation linéaire. Nous montrons aussi que la série de Dirichlet associée à une telle suite se prolonge en une fonction méromorphe dans le plan complexe, dont les pôles sont assez bien localisés.

8. Le dernier chapitre est consacré à un exemple, un produit infini mahlérien, pour lequel nous donnons un développement asymptotique complet de la suite des coefficients. Ce développement fait voir une périodicité de nature arithmétique, évidente *a priori* car le produit infini est lié à un polynôme cyclotomique, mais aussi une périodicité plus cachée en rapport avec l'invariance d'échelle. Les techniques utilisées sont classiques en théorie des nombres, même si leur emploi est ici un peu exotique : transformation de Mellin, méthode de col, formule d'Euler-Maclaurin.

9. Enfin un ultime chapitre constitué uniquement de dessin est là pour réjouir notre aimable lecteur et lui fait apprécier sans effort les suites mahlériennes.

Une thèse est rarement le fruit d'un travail solitaire et il me faut dire ici ma reconnaissance.

Je suis tout simplement heureux que Michel Mendès France, Jean-Paul Allouche, Jean Berstel, Louis Comtet, Philippe Flajolet et Gérald Tenenbaum soient les membres du jury. Ils ont évidemment inspiré mon travail et rencontrer chacun d'eux est toujours un plaisir par l'amabilité sans faille dont ils font preuve. Je les remercie vivement de leur présence, spécialement Jean Berstel et Gérald Tenenbaum, qui ont accepté sans rechigner la tâche de rapporteur.

Mon cher directeur de thèse, Jean-Paul Allouche, a toujours su m'écouter et m'assister. Sa vision de la conquête des mathématiques, sur grand écran, est fascinante et il sait, grâce à son sens de l'anecdote, les mettre en valeur, trouver le point excitant, faire jaillir un rapprochement surprenant, ou espéré, toujours avec brio.

L'ambiance du projet Algorithmes de l'Inria a été un puissant stimulant et la qualité de ses membres, leur gentillesse bourrue m'ont grandement aidé à mener à bien ce travail. Je tiens à remercier particulièrement Virginie Collette, notre riante secrétaire, qui ne répugne jamais à remonter ses manches quand on a besoin d'elle et Bruno Salvy qui a fait preuve d'une patience remarquable pour m'apprendre les beautés technologiques de notre époque moderne.

Jeanne-Marie m'a supporté avec constance pendant que je courais les mathématiques et n'a rien négligé pour je réussisse cette entreprise. C'est bien d'elle que l'on peut dire « cette thèse n'existerait pas si ... »

Enfin Philippe Flajolet a eu un apport essentiel dans ce travail, autant par les idées qu'il m'a inspirées que par ses encouragements amicaux associés à la rigueur dont il est coutumier. Il m'a toujours poussé vers le haut et obligé à réfléchir sur l'intérêt et la place des notions rencontrées. Il imprègne son équipe, le projet Algorithmes, de cet esprit. Empruntant à Jean-Henry Fabre, il pourrait dire : « Les choses se passèrent ainsi. Nous étions cinq ou six : moi le plus vieux, leur maître, mais encore plus leur compagnon et leur ami ; eux jeunes gens à cœur chaleureux, à riante imagination, débordant de cette sève printanière qui nous rend si expansifs et si désireux

de connaître. Devisant de choses et d'autres, par un sentier bordé d'arbres bien enracinés, on allait collecter des résidus sur les lignes de pôles imaginaires, à l'espacement régulier source de comportements récurrents ; on allait franchissant des cols à l'abrupt relief voir si le terme dominant, juché tout là haut, l'emporterait bien sur ceux de la vallée. »

Et maintenant, en route vers ces hauteurs !

Première partie

Aspect algébrique

Les récurrences avec retard ou équations aux différences finies, comme la récurrence qui définit la suite de Fibonacci

$$F_n = F_{n-1} + F_{n-2},$$

sont bien connues en algèbre, en théorie des langages et en combinatoire [60, chap. 3][13, 21]. Par ailleurs les récurrences *diviser pour régner*, comme la récurrence

$$T_n = T_{\lfloor n/2 \rfloor} + T_{\lceil n/2 \rceil} + n - 1$$

qui donne le coût du tri-fusion dans le cas le pire, sont classiques en analyse d'algorithmes [36, 64]. Ces deux types de récurrence entrent dans une classe qui les englobe. Les séries génératrices ordinaires $f(z)$ des suites qu'elles définissent sont dans les deux cas solutions d'équations qui expriment une dépendance linéaire à coefficients polynomiaux entre $f(z)$, $f(z^2)$, $f(z^4)$, *etc.* Plus généralement de telles équations en $f(z)$, $f(z^B)$, $f(z^{B^2})$, ... sont dites mahlériennes en l'honneur de Kurt Mahler [50, 53, 51], qui a étudié dans les années 26-30 la transcendance de certaines fonctions analytiques dans le cas linéaire et non linéaire et vers 1940 l'asymptotique de certaines suites en liaison avec des équations de cette forme.

La voie naturelle pour aborder des équations fonctionnelles linéaires consiste à étudier d'abord les opérateurs linéaires sous-jacents. Ici deux types de propriétés sont fondamentales : d'une part le comportement sur les polynômes de l'opérateur de base, l'opérateur de Mahler, qui fait passer de $f(z)$ à $f(z^B)$; d'autre part l'arithmétique de ces opérateurs. L'action de l'opérateur de Mahler structure l'ensemble des polynômes irréductibles en forêt et confère un rôle particulier aux polynômes cyclotomiques. L'algèbre des opérateurs n'est pas commutative mais la relation de pseudo-commutativité $Mz = z^B M$ permet d'en normaliser l'écriture. De plus elle a la remarquable propriété de posséder une division euclidienne à gauche, ce qui permet de développer une arithmétique élémentaire, dans laquelle la linéarité pallie le manque de commutativité. Cette arithmétique montre qu'une série mahlérienne possède une équation de Mahler minimale. Elle permet d'obtenir des propriétés de clôture : les séries mahlériennes forment une algèbre stable par dérivation, qui contient les fractions rationnelles. Enfin elle ramène toute équation de Mahler à une forme équivalente dans laquelle le coefficient de $f(z)$ n'est pas nul.

La résolution des équations de Mahler peut être abordée de différents points de vue. On peut vouloir obtenir des solutions formelles à une précision fixée d'avance, par exemple à z^{100} près. Le point crucial est que la récurrence associée à l'équation fonctionnelle se scinde en deux. Il y a d'abord une partie basse pour laquelle un petit système linéaire permet de déterminer la dimension de l'espace des solutions. Ensuite la partie haute qui par simple dévidement fournit les termes successifs de la suite. L'obtention de la partie haute se fait par itération d'un opérateur contractant et cela peut fournir de jolis développements des solutions en séries de fractions rationnelles. Surtout ceci montre que les solutions formelles à coefficients complexes définissent des solutions méromorphes dans le disque unité. Dans l'espace des séries de Laurent, les résultats sont qualitativement les mêmes car la valuation des solutions est minorée *a priori*. Enfin l'obtention de solutions sous forme close est un problème naturel et important ; il est possible de déterminer les solutions rationnelles d'une équation de Mahler, voire certaines solutions qui s'écrivent sous forme d'un produit infini, ce qui fournit alors des facteurs du premier degré pour l'opérateur associé.

Chapitre 1

Opérateurs

Ce chapitre a un statut préparatoire. Les opérateurs linéaires qui y sont étudiés sont les outils algébriques que nous utiliserons sans cesse. Il s'agit d'une part de l'opérateur de Mahler, la substitution de z^B à z, et d'autre part des opérateurs de section, qui trient les coefficients d'une série suivant le résidu modulo B de leur indice.

Il est fondamental de déterminer leur action sur les polynômes et les fractions rationnelles car leur comportement sera la clé de nombreuses démonstrations. Ce chapitre est donc consacré à tirer ces questions au clair, essentiellement dans deux cas : soit les coefficients sont pris dans le corps des rationnels, soit ils sont dans un corps fini. Dans le premier cas on met en valeur l'importance des polynômes cyclotomiques et dans le second on étudie des propriétés de périodicité, ce qui est au fond la même idée. Dans ces deux situations on voit apparaître une structure arborescente qui permet de décrire l'action de l'opérateur de Mahler sur les polynômes irréductibles. Les résultats obtenus seront essentiellement utilisés dans l'étude des équations de Mahler au chapitre 3 et dans la recherche de critères de B-régularité au chapitre 6.

1.1 Objets de base

Dans tout le texte, la lettre B désigne un entier supérieur ou égal à 2. Cette lettre B abrège la locution base de numération et ceci apparaitra clairement dans la seconde partie.

Les êtres mathématiques que nous manipulerons le plus sont les séries formelles en une indéterminée z à coefficients dans un anneau commutatif $\mathbb{A}$,

$$f(z) = \sum_{n\geq 0} f_n\, z^n.$$

Elles forment une algèbre $\mathbb{A}[[z]]$ pour le produit de Cauchy $\times$, mais aussi pour le produit de Hadamard $\odot$,

$$f(z) \times g(z) = \sum_{n\geq 0} \sum_{k+l=n} f_k\, g_l\, z^n, \quad f(z) \odot g(z) = \sum_{n\geq 0} f_n\, g_n\, z^n.$$

La valuation de la série $f(z)$ est le premier entier $\omega(f)$ qui fournit un coefficient f_n non nul, avec la convention $\omega(0) = +\infty$. Muni de l'ultramétrique

$$(f, g) \longmapsto 2^{-\omega(f-g)}$$

$\mathbb{A}[[z]]$ est un espace complet [17].

À l'occasion nous utiliserons aussi l'algèbre des séries de Laurent formelles $\mathbb{A}[[z]][1/z]$. Dans le cas particulier où $\mathbb{A}$ est un corps $\mathbb{K}$, il s'agit du corps des fractions $\mathbb{K}\,(\!(z)\!)$ de l'anneau intègre $\mathbb{K}\,[[z]]$.

1.2 Opérateur de Mahler

À l'entier B est associé l'opérateur de Mahler M_B ou plus simplement M, défini par

$$Mf(z) = f(z^B).$$

Suivant les cas ce sera un opérateur sur les polynômes, les fractions rationnelles, les séries formelles, les fonctions analytiques ou méromorphes. Il est linéaire et injectif pour tout ce qui concerne l'aspect formel.

L'algèbre linéaire et l'arithmétique des polynômes sont les deux pierres angulaires des démonstrations dans ce travail et le comportement des polynômes par rapport à cet opérateur est un outil fondamental.

1.2.1 Comportement des polynômes

Nous nous plaçons d'abord dans un corps algébriquement clos $\mathbb{K}$ de caractéristique nulle ou première avec B. Avec cette hypothèse l'arithmétique des polynômes est équivalente à la gestion de multi-ensembles de $\mathbb{K}$, vus comme ensembles de racines des polynômes affectées de leur multiplicité et nous étudions donc les sous-ensembles du corps au regard de l'application $z \mapsto z^B$.

Définition 1. *Un sous-ensemble de $\mathbb{K}$ est B-stable, s'il est stable par l'élévation à la puissance B-ième.*

La structure des applications d'un ensemble fini dans lui-même est bien connue [21, p. 84].

Proposition 1. *Soit $\mathcal{N}$ un ensemble fini et ϕ une application de $\mathcal{N}$ dans lui-même. L'ensemble $\mathcal{N}$ est partitionné en un nombre fini de blocs $\mathcal{B}$ tels que la restriction de ϕ à $\mathcal{B}$ a pour graphe fonctionnel un cycle sur lequel sont éventuellement enracinés des arbres.*

Définition 2. *Un $\alpha \in \mathbb{K}$ est B-cyclique s'il appartient à un cycle pour l'application $z \mapsto z^B$, c'est-à-dire vérifie*

$$\alpha^{B^\ell} = \alpha.$$

Proposition 2. *Un élément de $\mathbb{K}$, qui est B-cyclique, est une racine de l'unité. Une racine de l'unité est B-cyclique si et seulement si son ordre est premier avec B.*

Démonstration. Supposons, en effet, que α est une racine de l'unité dont l'ordre est N (autrement dit, elle engendre le groupe des racines N-ièmes de l'unité).

Si N et B sont premiers entre eux, B est inversible modulo N et

$$B^{\phi(N)} \equiv 1 \bmod N,$$

donc α appartient à un cycle dont l'ordre divise $\phi(N)$.

Sinon, soit p un diviseur premier commun à N et B. S'il existait un ℓ tel que

$$N \mid B^\ell - 1,$$

p diviserait 1, donc α n'est pas B-cyclique. □

Définition 3. *La distance de $z \in \mathbb{K}$ à un cycle est la distance de z à un cycle dans le graphe fonctionnel de $z \mapsto z^B$. C'est un élément de l'ensemble ordonné $\mathbb{N} \cup \{+\infty\}$.*

1.2.2 Polynômes cyclotomiques

Dans la plupart des exemples que nous rencontrerons les polynômes sont à coefficients entiers. Parmi ceux-ci les polynômes cyclotomiques seront très utiles, car ils ont un comportement particulier au regard de l'opérateur de Mahler. Le corps de référence est donc ici le corps des rationnels.

Définition 4. *Nous notons Ω_a l'ensemble des racines de l'unité dans le corps $\mathbb{C}$ des nombres complexes dont l'ordre est a et $\Phi_a(z) \in \mathbb{Z}[z]$ le polynôme cyclotomique d'indice a, avec $\Phi_a(0) = 1$.*

Imposer $\Phi_a(0) = 1$, au lieu de la convention usuelle qui rend Φ_a unitaire, ne concerne en réalité que $\Phi_1(z) = 1 - z$. Le fait d'avoir $\Phi_a(0) = 1$ est plus adapté à l'usage que nous ferons des polynômes cyclotomiques. Comme on le sait [14, p. 363] [70, p. 551] les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$ et c'est pourquoi le corps de référence est ici $\mathbb{Q}$.

Rappelons que $\Phi_a(z)$ est le polynôme minimal des racines primitives a-ième de l'unité (les éléments de Ω_a). Il est donné par

$$\Phi_a(z) = \prod_{\alpha \in \Omega_a} (1 - \alpha z)$$

ou encore

$$\Phi_a(z) = \prod_{d|a} \left(1 - z^{a/d}\right)^{\mu(d)}$$

en notant μ la fonction de Möbius.

Les formules précédentes ne donnent pas un moyen de calcul efficace des polynômes cyclotomiques ; il vaut mieux utiliser

$$\Phi_{pa}(z) = \frac{\Phi_a(z^p)}{\Phi_a(z)}$$

si p est un nombre premier qui ne divise pas a, et

$$\Phi_a(z) = \Phi_{\sqrt{a}}\left(z^{a/\sqrt{a}}\right)$$

si on note $\sqrt{a}$ le radical de a, c'est-à-dire le nombre libre de carré $p_1 p_2 \dots p_k$ pour $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. En effet les racines de $\Phi_{\sqrt{a}}(z)$ sont les racines de l'unité (primitives) d'ordre $\sqrt{a}$, donc celles de $\Phi_{\sqrt{a}}(z^{a/\sqrt{a}})$ ont pour ordre, au sens de la théorie des groupes, $\sqrt{a} \times a/\sqrt{a} = a$ et sont au nombre de $\varphi(\sqrt{a}) \times a/\sqrt{a} = \varphi(a)$, d'où l'égalité.

Exemple 1 : Ainsi, avec $a = 600 = 2^3 \times 3 \times 5^2$, les égalités

$$\Phi_{600}(z) = \Phi_{30}(z^{20}),$$

et

$$\Phi_{30}(z) = \Phi_{6\times 5}(z) = \frac{\Phi_6(z^5)}{\Phi_6(z)} = \frac{1 - z^5 + z^{10}}{1 - z + z^2} = 1 + z - z^3 - z^4 - z^5 + z^7 + z^8,$$

donnent l'expression explicite

$$\Phi_{600}(z) = 1 + z^{20} - z^{60} - z^{80} - z^{100} + z^{140} + z^{160}.$$

Les polynômes cyclotomiques ont des propriétés remarquables sous l'action de l'opérateur de Mahler, comme il apparaît dans la proposition suivante.

Proposition 3. *Les seuls polynômes irréductibles, $\phi(z)$, de $\mathbb{Q}[z]$ tels que $\phi(z)$ divise $\phi(z^B)$ et $\phi(0) = 1$ sont les polynômes cyclotomiques $\Phi_a(z)$ où a est premier avec B.*

DÉMONSTRATION. Dire que $\phi(z)$ divise $\phi(z^B)$ c'est dire que l'ensemble des racines de $\phi(z)$ est B-stable. En particulier il contient des racines primitives a-ièmes de l'unité pour un entier a premier avec B. Comme les $\Phi_a(z)$ sont irréductibles, $\phi(z)$ est nécessairement un $\Phi_a(z)$, où a est premier avec B. □

Pour préciser le comportement des polynômes cyclotomiques par rapport à l'élévation à la puissance B, nous introduisons une définition.

Définition 5. *Soient a et b deux entiers non nuls, dont les factorisations sont respectivement*

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\gamma_1} \dots q_m^{\gamma_m},$$

$$b = p_1^{\beta_1} \dots p_k^{\beta_k} r_1^{\delta_1} \dots r_n^{\delta_n},$$

les nombres premiers $p_1, \dots, p_k, q_1, \dots, q_m, r_1, \dots, r_n$ étant distincts deux à deux et les α_i, β_i, γ_i, δ_i étant des entiers strictement positifs, alors

$$b' = r_1^{\delta_1} \dots r_n^{\delta_n}$$

est la partie de b étrangère à a.

Proposition 4. *Si a et B sont deux entiers naturels non nuls, alors le polynôme $\Phi_a(z^B)$ se factorise en polynômes irréductibles de $\mathbb{Q}[z]$ sous la forme*

$$\Phi_a(z^B) = \prod_{b|B'} \Phi_{aB/b}(z)$$

si B' désigne la partie de B étrangère à a.

DÉMONSTRATION. Nous partons de deux formules connues. Si a et B sont premiers entre eux

$$\Phi_a(z^B) = \prod_{b|B} \Phi_{aB/b}(z).$$

Si p est premier et ne divise pas a

$$\Phi_{p^\alpha a}(z) = \Phi_{pa}(z^{p^{\alpha-1}}).$$

□

EXEMPLE 2 : Avec $a = 10$ et $B = 60$, la partie de B étrangère à a vaut $B' = 3$, d'où l'égalité

$$\Phi_{10}(z^{60}) = \Phi_{200}(z)\Phi_{600}(z),$$

c'est-à-dire

$$1 - z^{60} + z^{120} - z^{180} + z^{240} = (1 - z^{20} + z^{40} - z^{60} + z^{80})(1 + z^{20} - z^{60} - z^{80} - z^{100} + z^{140} + z^{160}).$$

L'élévation à la puissance B induit sur l'ensemble des polynômes irréductibles $\phi(z)$ tels que $\phi(0) = 1$ une relation qui à chaque $\phi(z)$ associe les facteurs de $\phi(z^B)$ et ceux-ci sont d'ailleurs tous distincts. La relation réciproque est une application qui à un $\phi(z)$ associe le polynôme (irréductible) dont les racines sont les puissances B-ième des racines de $\phi(z)$. Comme Bradford et Davenport [15], nous pouvons dire que cette application est l'application graeffe$_B$.

Définition 6. *Si $\phi(z)$ est un polynôme à coefficients dans un corps commutatif,* graeffe$_B\phi(z)$ *est le résultant de $\phi(y)$ et $y^B - z$.*

Lemme 1. *Le coefficient dominant de* graeffe$_B\phi(z)$ *est le coefficient dominant de* $\phi(z)$ *élevé à la puissance* B.

Si le polynôme $\phi(z)$ *est à coefficients entiers et primitif, il en est de même de* graeffe$_B\phi(z)$.

DÉMONSTRATION. Il suffit d'ecrire, par exemple, le résultant comme un déterminant de Sylvester.

Pour le deuxième point, on raisonne par l'absurde en considérant le coefficient dominant modulo p, si p est un diviseur premier commun à tous les coefficients de graeffe$_B\phi(z)$. □

Le fait d'utiliser le corps des rationnels permet de préciser les choses. Dans ce cas il y a, d'après les deux propositions précédentes, deux types de polynômes irréductibles au regard de l'application graeffe$_B$: les cyclotomiques et les non cyclotomiques. Pour un polynôme non cyclotomique, ses images par les itérées de graeffe$_B$ sont toutes distinctes. Inversement ce polynôme est à la racine d'un arbre infini dont chaque noeud $\phi(z)$ a pour fils les facteurs irréductibles de $\phi(z^B)$. Un polynôme cyclotomique Φ_a, où a est premier avec B, est fixe par graeffe$_B$. Les facteurs irréductibles de $\Phi_a(z^B)$ sont les $\Phi_{aB/b}(z)$ où b divise B,; en particulier $\Phi_a(z)$ est lui-même un des facteurs de $\Phi_a(z^B)$ et les autres sont des $\Phi_{a'}$, où a' n'est pas premier avec B. Pour les polynômes cyclotomiques Φ_a où a n'est pas premier avec B le comportement est similaire à celui des polynômes non cyclotomiques, à la différence qu'en itérant un certaine nombre de fois graeffe$_B$ on trouve $\Phi_{a'}$ où a' est la partie de a étrangère à B et que la suite des itérés par graeffe$_B$ est donc stationnaire.

Il sera commode d'employer une terminologie imagée.

Définition 7. *Soient* ϕ *et* ψ *deux polynômes irréductibles distincts à coefficients dans un corps* $\mathbb{K}$, *tels que* $\phi(0) = 1$ *et* $\psi(0) = 1$ *; nous disons que* ψ *est fils de* ϕ *si* ψ *est un facteur de* $\phi(z^B)$, *c'est-à-dire si* $\phi =$ graeffe$_B\psi$, *et* ψ *est différent de* ϕ. *Un descendant de* ϕ *est un fils de* ϕ *ou un descendant d'un fils de* ϕ.

Théorème 1. *Le graphe de la relation « fils de » est une réunion d'arbres infinis. Si* $\mathbb{K} = \mathbb{Q}$, *les seuls éléments qui n'ont pas de père sont les polynômes cyclotomiques* Φ_a *où* a *est premier avec* B.

La comparaison de deux polynômes irréductibles ϕ et ψ à coefficients rationnels tels que $\phi(0) = 1$ et $\psi(0) = 1$ peut se faire comme suit. On commence par chasser les dénominateurs et rendre les polynômes primitifs. Plusieurs cas se présentent alors. D'abord les résultats de Bradford et Davenport [15] permettent de déterminer s'il s'agit de polynômes cyclotomiques et si c'est le cas leurs indices (mais la procédure est plutôt coûteuse), ce qui permet de les comparer. Si l'un est cyclotomique mais l'autre ne l'est pas, ils ne sont pas comparables. Ensuite si les deux sont non cyclotomiques et si leurs racines ne sont pas toutes de module 1, la méthode de Graeffe par exemple fournit les modules maximum et minimum de leurs racines. Si l'un des quotients des logarithmes des deux modules maximum ou minimum n'est pas une puissance de B, ou si la puissance de B n'est pas la même, les deux polynômes ne sont pas comparables. Sinon, l'exposant obtenu donne la distance, d, possible d'un polynôme à l'autre dans le graphe de la relation « fils de » et il suffit de vérifier que l'un est bien l'image par graeffe$_B^d$ de l'autre. En pratique, la simple recherche des modules maximum et minimum par la méthode de Graeffe fait déjà voir la relation entre les deux polynômes. Enfin si les deux polynômes ont toutes leurs racines de module 1 sans être cyclotomiques, leurs coefficients dominants ne sont pas égaux à ± 1, comme le montre le lemme qui suit, dû à Kronecker [57, p. 47]. Puisque le graeffe$_B$ d'un polynôme primitif est primitif, une égalité $\psi(z) =$ graeffe$_B^d\phi(z)$ impose la relation $\psi_m = \phi_n^{B^d}$ entre les coefficients dominants respectifs de ψ et ϕ. Ceci donne la valeur possible de d et il suffit de vérifier.

Proposition 5. *Le fait que deux polynômes de* $\mathbb{Q}[z]$ *soient liés par l'application* graeffe$_B$ *est algorithmiquement décidable.*

Lemme 2. *Soit f un polynôme unitaire irréductible de $\mathbb{Z}[z]$ non constant dont toutes les racines sont de module inférieur ou égal à 1, alors ou bien f est un polynôme cyclotomique ou bien toutes les racines de f sont de module strictement inférieur à 1.*

DÉMONSTRATION. Soient $d \geq 1$ le degré de f et $z_1, \ldots, z_d$ ses racines. Si f a comme racine une racine de l'unité, il est cyclotomique. Sinon supposons qu'il possède une racine de module 1, par exemple z_1. Pour tout $n > 0$, les z_i^n sont différents de 1 et l'entier $\prod_{1 \leq i \leq d} (z_i^n - 1)$ n'est pas nul. Comme tous les z_i^n sont à une distance de 1 plus petite que 2, l'inégalité

$$|z_1^n - 1| \geq \frac{1}{\prod_{1<i\leq d} |z_i^n - 1|} \geq \frac{1}{2^{d-1}},$$

contredit le fait que l'ensemble des puissances de z_1 est dense dans le cercle unité. □

EXEMPLE 3 : Prenons $\phi_1(z) = 1 + z^2 + z^3$ et $\phi_2(z) = 1 + 6\,z + 21\,z^2 - z^3$. Les racines, évaluées en flottants, sont respectivement

$$-1,465571232\,;\quad 0,2327856159 + 0,7925519925\,i\,;\quad 0,2327856159 - 0,7925519925\,i$$

et

$$21,28410791\,; -0,1420539549 + 0,1637195327\,i\,;\quad -0,1420539549 - 0,1637195327\,i$$

d'où les modules maximum et minimum respectifs

$$R_1 = 1.465571232\,;\quad r_1 := 0,8260313576$$

$$R_2 = 21,8410791\,;\quad r_2 = 0,2167565720.$$

Comme

$$\frac{\ln R_2}{\ln R_1} = 7,999999999\,;\quad \frac{\ln r_2}{\ln r_1} = 7,999999999$$

la seule possibilité est que

$$\phi_2 = \text{graeffe}_2^3 \phi_1$$

et il en est bien ainsi, car

$$\text{graeffe}_2(1 + z^2 + z^3) = 1 + 2\,z + z^2 - z^3,$$

$$\text{graeffe}_2(1 + 2z + z^2 - z^3) = 1 - 2\,z + 5\,z^2 - z^3,$$

$$\text{graeffe}_2(1 - 2z + 5z^2 - z^3) = 1 + 6\,z + 21\,z^2 - z^3.$$

1.2.3 Périodicité dans les corps finis

Nous montrerons, dans le chapitre 6, que certaines fractions rationnelles à coefficients dans un corps fini vivent dans un espace vectoriel de dimension finie. Ceci équivaut à dire qu'elles admettent toutes une même période pour la suite des coefficients de leur développement en série formelle.

Définition 8. *Soit g un polynôme à coefficients dans un anneau commutatif avec $g(0)$ inversible. Nous disons que g est périodique si la suite des coefficients de la série formelle $1/g$ est périodique. Une (respectivement la) période de g est alors une (resp. la) période de cette suite.*

Les deux propositions suivantes sont extraites du livre de Berlekamp [11].

Proposition. *Soit g un polynôme sur le corps $\mathbb{F}_q$, de caractéristique p, avec $g(0) \neq 0$. Si*

$$g = \prod_i g_i^{m_i},$$

où les g_i sont irréductibles de période T_i, la période de g est le ppcm *des T_i, multiplié par la première puissance de p supérieure ou égale à tous les m_i.*

Proposition. *Soit g un polynôme irréductible de période T sur $\mathbb{F}_q$ et n un nombre premier différent de la caractéristique p du corps.*

Si n divise T, chaque facteur irréductible de $f(z^n)$ a pour période nT.

Si n ne divise pas T, l'un des facteurs irréductibles de $f(z^n)$ a pour période T et les autres ont pour période nT.

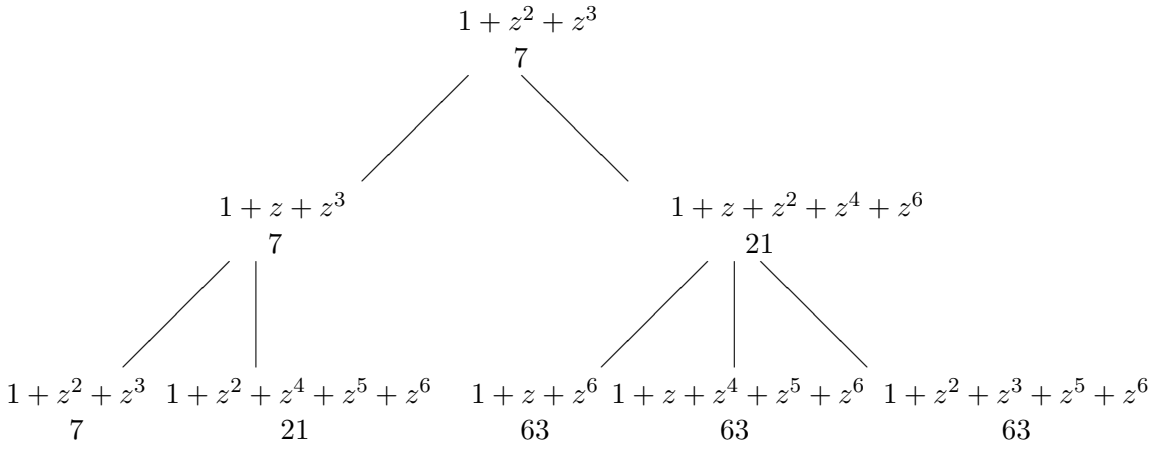

FIG. 1.1

Les relations de parenté entre les facteurs irréductibles de $g(z) = 1 + z^2 + z^3$, $g(z^3)$ et $g(z^9)$ dans le corps $\mathbb{F}_2$, montrent comment sont reliées leurs périodes. Si $h(z)$ a une période T multiple de 3, alors les facteurs de $h(z^3)$ ont tous pour période $3\,T$; par contre si T n'est pas divisible par 3, il y a exactement un facteur de $h(z^3)$ qui a pour période T, alors que les autres ont pour période $3\,T$. Nous remarquons aussi que 9 est une puissance de 3 congrue à une puissance de 2, la caractéristique, modulo 7, la période, et c'est pourquoi $g(z)$ est facteur de $g(z^9)$.

Une lecture attentive de la démonstration montre que cette dernière proposition peut être précisée et généralisée.

Corollaire 1. *Dans chaque cas les facteurs irréductibles de $g(z^n)$ sont distincts. De plus ils sont distincts de $g(z)$ sauf si n ne divise pas T et n est congru à une puissance de q modulo T et $g(z)$ est alors le facteur de période T de $g(z^n)$.*

Proposition 6. *Soit g un polynôme irréductible de période T sur $\mathbb{F}_q$ et n un entier premier avec la caractéristique p du corps. Si n a pour décomposition en facteur premier*

$$n = n_1^{\beta_1} \cdots n_I^{\beta_I} m_1^{\gamma_1} \cdots m_J^{\gamma_J},$$

les n_i divisant T et les m_j ne divisant pas T, les facteurs irréductibles de $f(z^n)$ sont tous distincts et ont pour période les

$$n_1^{\beta_1} \cdots n_I^{\beta_I} m_1^{\delta_1} \cdots m_J^{\delta_J} T,$$

avec $0 \leq \delta_j \leq \gamma_j$ pour $1 \leq j \leq J$. De plus toutes ces périodes apparaissent effectivement, celles pour lesquelles un δ_j est nul apparaissant exactement une fois.

DÉMONSTRATION. Par récurrence sur I et application répétée de la proposition précédente, le résultat est facilement atteint pour les entiers n dont les diviseurs premiers sont des diviseurs de T. De plus tous les polynômes irréductibles rencontrés sont différents. Ensuite une récurrence sur J, le cas précédent correspondant à $J = 0$, fournit le résultat général. Si la proposition est établie pour l'entier ν, soit m un nombre premier ne divisant ni T ni ν et différent de p. La proposition précédente appliquée de façon répétée aux facteurs irréductibles de $f(z^\nu)$ fait apparaître les périodes νT, $\nu m T$, $\cdots$, $\nu m^\gamma T$ pour les facteurs de $f(z^{\nu m^\gamma})$. De plus tous les facteurs de $f(z^{\nu m^\gamma})$ sont distincts. Si n n'est pas premier avec T (il existe des diviseurs premiers n_i), les périodes des facteurs irréductibles de $g(z^{n^\ell})$ sont de la forme

$$n_1^{\ell\beta_1} \cdots n_I^{\ell\beta_I} m_1^{\delta_1} \cdots m_J^{\delta_J} T,$$

avec $0 \leq \delta_j \leq \ell\gamma_j$ pour $1 \leq j \leq J$, ce qui fait que les facteurs des $g(z^{n^\ell})$, pris dans leur ensemble, sont tous distincts. Par contre si n est premier avec T, les facteurs dont la période est de la forme

$$m_1^{\delta_1} \cdots m_J^{\delta_J} T$$

avec au moins un δ_j nul ne sont pas nécessairement distincts. □

Corollaire 2. *Les facteurs irréductibles des polynômes $g(z)$, $g(z^n)$, $\cdots$, $g(z^{n^K})$ sont distincts sauf peut-être ceux de période*

$$m_1^{\delta_1} \cdots m_J^{\delta_J} T,$$

avec au moins un δ_j nul, dans le cas où n est premier avec T.

Un petit raffinement du corollaire 1 permet de préciser comment $g(z)$ apparaît dans les $g(z^{n^k})$ si n est premier avec T et p.

Corollaire 3. *Supposons que n est premier avec la caractéristique p du corps $\mathbb{F}_q$ et avec la période T de $g(z)$. Alors $g(z)$ est facteur de $g(z^{n^k})$ si et seulement si n^k est congru à une puissance de q modulo T.*

EXEMPLE 4 : Le polynôme à coefficients dans $\mathbb{F}_2$, $g = 1 + z^2 + z^3$, est irréductible de période 7. Avec $n = 3$, qui est premier avec 7, le polynôme $g(z^3) = 1 + z^6 + z^9$, se factorise en $(1 + z + z^3)(1 + z + z^2 + z^4 + z^6)$. Le premier facteur est de période 7, puisque la décomposition de $1 - z^7$ est

$$1 - z^7 = (1 + z)(1 + z + z^3)(1 + z^2 + z^3)$$

et le second est de période 21 car

$$\Phi_{21}(z) = \frac{(z^{21} - 1)(z - 1)}{(z^3 - 1)(z^7 - 1)} = (1 + z + z^2 + z^4 + z^6)(1 + z^2 + z^4 + z^5 + z^6).$$

Ensuite

$$g(z^9) = 1 + z^{18} + z^{27} = (1 + z^3 + z^9)(1 + z^3 + z^6 + z^{12} + z^{18})$$

et

$$1 + z^3 + z^9 = (1 + z^2 + z^3)(1 + z^2 + z^4 + z^5 + z^6),$$

$$1 + z^3 + z^6 + z^{12} + z^{18} = (1 + z + z^4 + z^5 + z^6)(1 + z + z^6)(1 + z^2 + z^3 + z^5 + z^6).$$

Ces derniers facteurs, sauf $1 + z^2 + z^3$, sont de période 63 d'après la factorisation

$$\begin{aligned}\Phi_{63}(z) &= (z^{63} - 1)(z^3 - 1)/(z^9 - 1)(z^{21} - 1) \\ &= (1 + z + z^6)(1 + z^5 + z^6)(1 + z + z^2 + z^5 + z^6) \\ &\quad \times (1 + z + z^3 + z^4 + z^6)(1 + z + z^4 + z^5 + z^6)(1 + z^2 + z^3 + z^5 + z^6).\end{aligned}$$

La première puissance de 3 congrue à une puissance de 2 modulo 7 est 9 et nous ne sommes pas étonnés de voir réapparaître $g(z)$ comme facteur de $g(z^9)$. Une bonne façon de voir les choses (cf. figure 1.1) est de considérer l'arbre dont la racine est étiquetée par $g(z)$, dans lequel chaque nœud d'étiquette $h(z)$ a pour fils les nœuds étiquetés par les facteurs irréductibles de $h(z^3)$, ainsi que l'arbre obtenu en remplaçant chaque facteur par sa période.

1.3 Opérateurs de section

Parallèlement à l'opérateur de Mahler, nous introduisons les opérateurs de B-section, $S_{B,r}$ ou S_r $(0 \le r < B)$ définis sur l'espace des séries de Laurent $\mathbb{A}[[z]][1/z]$, par

$$S_{B,r} f(z) = \sum_n f_{Bn+r} z^n.$$

Ils sont évidemment liés à l'opérateur de Mahler puisque, pour toute $f(z) \in \mathbb{A}[[z]][1/z]$,

$$S_0 M f = f, \quad S_r M f = 0 \ \ (0 < r < B).$$

Leur propriété caractéristique est

$$f(z) = \sum_{0 \le r < B} z^r S_{B,r} f(z^B)$$

pour toute $f(z)$.

Si le corps de référence est algébriquement clos et si sa caractéristique est nulle ou ne divise pas B, on peut aussi exprimer les opérateurs de section par

$$S_r f(z^B) = \frac{1}{B z^r} \sum_{0 \le j < B} \omega^{-rj} f(\omega^j z)$$

où ω est une racine primitive B-ième de l'unité.

Lemme 3. *Les sections d'une fraction rationnelle à coefficients dans un corps dont la caractéristique est nulle ou ne divise pas B sont rationnelles. Les sections d'une fraction rationnelle $g(z)$ ont alors pour pôles un sous-ensemble des puissances B-ièmes des pôles de $g(z)$ et l'ordre d'un pôle α de $S_r g(z)$ est majoré par l'ordre maximum des racines B-ièmes de α, qui sont pôles de $g(z)$.*

DÉMONSTRATION. Dans une extension convenable, la formule précédente appliquée à

$$g(z) = \frac{1}{(z-\alpha)^k};$$

donne, en réduisant au même dénominateur,

$$S_r g(z^B) = \frac{1}{Bz^r} \sum_{0\le j<B} \omega^{-rj} \frac{1}{(\omega^j z - \alpha)^k} = \frac{\sum_{0\le j<B} \omega^{-rj} \prod_{\ell\neq j} (\omega^\ell z - \alpha)^k}{(z^B - \alpha^B)^k}.$$

Le numérateur et le dénominateur de cette fraction sont premiers entre eux car les racines du dénominateur annulent tous les termes de la somme qui figure au numérateur sauf un. Il en résulte que le dénominateur de la fraction $S_r g(z)$ est exactement $(z-\alpha^B)^k$. Ainsi $S_r g(z)$ s'écrit

$$\frac{a_1}{z-\alpha^B} + \cdots + \frac{a_k}{(z-\alpha^B)^k}$$

et, pour une fraction g ayant plusieurs pôles qui ont la même puissance B-ième, il faut additionner les différentes contributions, d'où la majoration indiquée sur l'ordre du pôle. □

À dire vrai il n'est pas indispensable d'utiliser un corps pour obtenir un résultat de cette nature. Supposons que $\mathbb{A}$ soit un anneau commutatif et notons E l'opérateur de décalage défini par

$$Ef(z) = \sum_n f_{n+1}\, z^n.$$

Dire qu'une série formelle $g(z)$ est une série rationnelle c'est dire que toutes ses décalées $E^k g(z)$ $(k \ge 0)$ demeurent dans un $\mathbb{A}$-module de type fini $\mathcal{G}$. C'est d'ailleurs ainsi que cette notion est définie en théorie des langages formels. D'après les égalités

$$ES_r = S_r E^B,$$

la série $S_r g(z)$ vit dans le module de type fini, image par S_r du module $\mathcal{G}$, et est donc rationnelle. Cependant la notion de pôle et *a fortiori* d'ordre d'un pôle n'a plus de sens ici.

Définition 9. *Si a et b sont deux entiers, b étant non nul, nous notons $a \div b$ le quotient dans la division euclidienne de a par b.*

Lemme 4. *Pour $f,\ g \in \mathbb{A}[[z]][1/z]$, les sections du produit de Cauchy fg s'écrivent*

$$S_r(fg) = \sum_{s+t\,\equiv\, r \bmod B} z^{(s+t)\div B} S_s(f) S_t(g)$$

DÉMONSTRATION. L'égalité

$$f(z) = \sum_{0\le r<B} z^r S_r f(z^B)$$

caractérise les images d'une série formelle $f(z)$ par les opérateurs de B-section. La formule résulte donc du développement du produit de deux séries formelles $f(z)$ et $g(z)$ en fonction de leurs sections,

$$\begin{aligned} f(z)g(z) &= \sum_{0\le s<B} z^s S_s f(z^B) \sum_{0\le t<B} z^t S_t g(z^B) \\ &= \sum_{0\le r<B} z^r \sum_{s+t\equiv r \bmod B} z^{[(s+t)\div B]B} S_s f(z^B) S_t g(z^B). \end{aligned}$$

□

Il convient de remarquer que l'exposant $(s+t) \div B$ ne peut prendre que les valeurs 0 ou 1, et que le seul cas où tous les exposants sont nuls est celui où $r = B-1$.

Chapitre 2

Arithmétique euclidienne non commutative

Les opérateurs linéaires sur les séries formelles,

$$f(z) \longmapsto c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}),$$

forment une algèbre non commutative. Ils sont essentiellement combinaisons de l'opérateur de Mahler, $M : f(z) \mapsto f(z^B)$, et de la multiplication par z. Ceux-ci ne commutent pas mais la relation de pseudo-commutativité

$$Mz = z^B M,$$

conduit à la forme normale $c_0(z) + c_1(z)\, M + \cdots + c_N(z)\, M^N$.

L'existence d'une division euclidienne, disons unilatérale, permet de développer sur ces opérateurs une arithmétique élémentaire. On obtient ainsi les propriétés usuelles pour le pgcd et le ppcm et des méthodes effectives de calcul. La non commutativité de cette algèbre d'opérateurs oblige à remplacer les arguments classiques par des méthodes d'algèbre linéaire. Cependant il n'y a pas de théorème raisonnable de factorisation.

2.1 Forme normale

L'algèbre des séries de Laurent $\mathbb{K}((z))$ à coefficients dans le corps commutatif $\mathbb{K}$ est un espace vectoriel et les endomorphismes de cet espace forment une algèbre dans laquelle nous distinguons d'une part l'opérateur de Mahler, M, défini par

$$Mf(z) = f(z^B),$$

et d'autre part les opérateurs de multiplication $\times_a$ par une fraction rationnelle donnée $a(z)$:

$$\times_a f(z) = a(z)f(z).$$

Le passage de $a(z)$ à $\times_a$ est un homomorphisme d'algèbre de $\mathbb{K}(z)$ dans $\mathrm{End}_{\mathbb{K}}(\mathbb{K}((z)))$, qui est injectif, et ceci permet d'identifier $\mathbb{K}(z)$ à son image. La sous-algèbre de $\mathrm{End}_{\mathbb{K}}(\mathbb{K}((z)))$ engendrée par les opérateurs de multiplication et M est donc $\mathbb{K}(z)[M]$ et le point crucial est la relation de pseudo-commutativité

$$Mz = z^B M.$$

Grâce à elle, tout élément de $\mathbb{K}(z)[M]$ s'écrit

$$\sum_{k=0}^{K} c_k(z)\, M^k$$

et cette écriture est unique. En effet une relation de dépendance linéaire, à coefficients polynomiaux,

$$\sum_{k=0}^{K} c_k(z)\, M^k = 0,$$

appliquée à $f(z) = z^{m+1}$, où m est le plus grand degré des éventuels c_k non nuls, fournit la nullité des c_k.

Proposition 7. *Tout élément de $\mathbb{K}(z)[M]$ s'écrit d'une unique façon sous la forme*

$$\sum_{k=0}^{K} c_k(z)\, M^k,$$

les $c_k(z)$ étant des fractions rationnelles.

Bien que M ne soit pas une indéterminée, cette unicité permet de parler du degré d'un élément $P(z, M)$ de $\mathbb{K}(z)[M]$.

Définition 10. *Le degré par rapport à M d'un opérateur $P = \sum_k c_k(z)\, M^k$ est le plus grand indice k tel que c_k soit non nul. Nous le noterons $\deg_M P$, avec la convention $\deg_M 0 = -\infty$.*

Le degré a toutes les propriétés que l'on peut attendre de lui et donne en particulier la proposition suivante par un argument classique.

Proposition 8. *L'algèbre $\mathbb{K}(z)[M]$ est sans diviseur de 0 et ses éléments inversibles sont les fractions rationnelles non nulles.*

2.2 Division et pgcd

L'arithmétique que nous allons développer s'appuie essentiellement sur le fait que l'algèbre $\mathbb{K}(z)[M]$ possède une division euclidienne.

Proposition 9. *Soient F et G deux éléments de $\mathbb{K}(z)[M]$, G étant non nul, il existe un unique couple (Q, R) d'éléments de $\mathbb{K}(z)[M]$ vérifiant*

$$F = QG + R$$

avec

$$R = 0 \ \ ou \ \ \deg_M R < \deg_M G.$$

Démonstration. Ceci se démontre comme pour la division euclidienne des polynômes. Précisément, si $F = f_n M^n + \cdots + f_0$ et $G = g_m M^m + \cdots + g_0$ avec f_n et g_m non nuls et $n \geq m$, le pas élémentaire de l'algorithme consiste à poser $Q_1 = \dfrac{f_n}{M^{n-m} g_m} M^{n-m}$ puis $F_1 = F - Q_1 G$. □

$$
\begin{array}{l|l}
z^4M^3+(1+z)M^2+zM+1 & (1+z)M+1 \\
\cline{2-2}
\dfrac{1+z-z^4+z^9+z^{10}}{1+z^9}M^2+zM+1 & \dfrac{z^4}{1+z^9}M^2+\dfrac{1+z-z^4+z^9+z^{10}}{(1+z^3)(1+z^9)}M+\dfrac{-1+2z^4-z^9+z^{13}}{(1+z)(1+z^3)(1+z^9)} \\
\dfrac{-1+2z^4-z^9+z^{13}}{(1+z^3)(1+z^9)}M+1 & \\
\dfrac{2+z+z^3-z^4+2z^9+z^{10}+z^{12}}{(1+z)(1+z^3)(1+z^9)} &
\end{array}
$$

FIG. 2.1
Une division euclidienne dans $\mathbb{Q}(z)[M]$ avec $B=3$.

EXEMPLE 5 : Prenons $B=3$, $F=(1-z)+zM+(1-z+z^2)M^2+z^4M^3$ et $G=1+(1+z)M$. La division euclidienne (cf. figure 2.1) donne l'égalité

$$(1+z)(1+z^3)(1+z^9)\left[z^4M^3+(1+z)M^2+zM+1\right]=$$
$$\left[(1+z)(1+z^3)z^4M^2+(1+z)(1+z-z^4+z^9+z^{10})M+(-1+2z^4-z^9+z^{13})\right]\left[(1+z)M+1\right]$$
$$+\left[2+z+z^3-z^4+2z^9+z^{10}+z^{12}\right].$$

EXEMPLE 6 : Si le quotient entier de ℓ par k est q, la division de $z^nM^\ell-1$ par z^pM^k-1 a pour quotient

$$z^{n-pB^{\ell-k}}M^{\ell-k}+z^{n-pB^{\ell-k}-pB^{\ell-2k}}M^{\ell-2k}+\cdots+z^{n-pB^{\ell-k}-\cdots-pB^{\ell-qk}}M^{\ell-qk}$$

et comme reste

$$z^{n-pB^{\ell-k}-\cdots-pB^{\ell-qk}}M^{\ell-qk}-1.$$

En particulier z^pM^k-1 divise $z^nM^\ell-1$ si et seulement si k divise ℓ et $n=p\dfrac{B^\ell-1}{B^k-1}$.

Comme dans le cas classique, le fait d'avoir un anneau euclidien amène immédiatement la principalité.

Théorème 2. *Les idéaux à gauche de $\mathbb{K}(z)[M]$ sont principaux.*

Définition 11. *Nous notons (P) l'idéal à gauche de $\mathbb{K}(z)[M]$ engendré par un opérateur P, l'ensemble des AP avec $A\in\mathbb{K}(z)[M]$.*

Cette notation ne créera pas d'ambiguïté car nous n'utiliserons jamais d'idéaux à droite.

Soient F et G deux éléments non nuls de $\mathbb{K}(z)[M]$, l'idéal $(F)+(G)$ étant principal s'écrit (D). Ceci montre que la paire $\{F,G\}$ possède des pgcd. Comme les éléments de $\mathbb{K}(z)$ sont les inversibles de $\mathbb{K}(z)[M]$, on peut supposer que

$$D=\sum_{k=0}^{N}c_k(z)\,M^k$$

avec des $c_k(z)$ qui sont des polynômes premiers entre eux dans leur ensemble. Ainsi D est déterminé à multiplication près d'un élément non nul de $\mathbb{K}$. Si le corps de référence est $\mathbb{Q}$, on peut même

se ramener à des polynômes à coefficients entiers premiers entre eux dans leur ensemble, ce qui détermine un pgcd à ± 1 près. L'algorithme d'Euclide permet de calculer un pgcd de deux éléments et de trouver une relation de Bézout, d'ailleurs minimale au sens des degrés. Cependant une relation de Bézout ne donne pas comme d'habitude une décomposition en somme directe du noyau d'un opérateur faute de commutativité.

Corollaire 4. *Deux opérateurs de* $\mathbb{K}(z)[M]$ *ont un* pgcd, *qui se calcule par l'algorithme d'Euclide.*

2.3 Ppcm

Le traitement du pgcd était immédiat mais la non commutativité complique un peu l'étude du ppcm et ce sont des arguments d'algèbre linéaire qui vont permettre d'obtenir les résultats classiques. Si F et G sont deux éléments non nuls de $\mathbb{K}(z)[M]$, l'idéal $(F) \cap (G)$ est principal et s'écrit (P), ce qui prouve l'existence de ppcm.

Exemple 7 : Aucun des deux opérateurs

$$F = 1 - \sum_{0 \le r < B} z^r M, \qquad G = \sum_{0 < r < B} z^r M$$

ne divise l'autre et un éventuel ppcm est de degré au moins 2. L'égalité

$$\left[\sum_{0<r<B} z^{rB} M\right]\left[1 - \sum_{0 \le r < B} z^r M\right] =$$

$$\left[z^{B-1}\frac{z^{B(B-1)}-1}{z^{B-1}-1}\frac{z-1}{z^B-1} - \sum_{0 \le r < B} z^{rB} M\right]\left[\sum_{0<r<B} z^r M\right],$$

montre qu'un ppcm est ce produit commun,

$$\sum_{0<r<B} z^{rB} M - \sum_{0<r<B} z^{rB} \sum_{0 \le r < B} z^{rB} M^2.$$

Il se pourrait très bien que le ppcm de deux éléments non nuls soit nul, car le produit ne nous fournit pas un évident multiple non nul comme il est d'usage.

Lemme 5. *Soient* F *et* G *deux éléments non nuls de* $\mathbb{K}(z)[M]$, *alors leur* ppcm *est non nul et de degré plus petit que* $\deg_M F + \deg_M G$.

Démonstration. Notons, pour abréger, $d_F = \deg_M F$ et $d_G = \deg_M G$. Pour d entier naturel, le $\mathbb{K}(z)$-espace vectoriel $\mathbb{K}(z)[M]_d$ constitué des opérateurs

$$E(z, M) = \sum_{0 \le k \le d} e_k(z) M^k$$

de degré inférieur ou égal à d, est de dimension $d + 1$. L'application

$$\begin{array}{ccc} \mathbb{K}(z)[M] & \longrightarrow & \mathbb{K}(z)[M] \\ U & \longmapsto & UF \end{array}$$

est $\mathbb{K}(z)$-linéaire. Elle envoie le sous-espace $\mathbb{K}(z)[M]_{d_F}$ dans le sous-espace $\mathbb{K}(z)[M]_{d_F+d_G}$ et elle est injective car il n'y a pas de diviseurs de 0 dans $\mathbb{K}(z)[M]$. Il en est de même pour l'application $V \mapsto VG$ et l'image de $\mathbb{K}(z)[M]_{d_G}$ par celle-ci. Comme la somme des dimensions des deux images dépasse strictement la dimension de $\mathbb{K}(z)[M]_{d_F+d_G}$, leur intersection n'est pas réduite à $\{0\}$. □

Proposition 10. *Si F et G sont deux éléments non nuls de $\mathbb{K}(z)[M]$, un* ppcm*, P, et un* pgcd*, D, de F et G vérifient*

$$\deg_M P + \deg_M D = \deg_M F + \deg_M G.$$

Démonstration. On peut supposer que $D = 1$, car $\text{ppcm}(\tilde{F}D, \tilde{G}D) = \text{ppcm}(\tilde{F}, \tilde{G})D$. Nous notons $P = XF = YG$ le ppcm de F et G puis $\mathcal{E}$ l'espace des opérateurs de degré strictement plus petit que celui de P et enfin $\mathcal{F} = (F) \cap \mathcal{E}$ et $\mathcal{G} = (G) \cap \mathcal{E}$. Le caractère minimal de P montre que $\mathcal{F} \cap \mathcal{G} = \{0\}$. Ensuite le fait que F et G sont premiers entre eux permet d'écrire une relation de Bézout

$$UF + VG = 1.$$

Si C est un élément de $\mathcal{E}$, cette égalité donne successivement

$$C = CUF + CVG,$$

puis en divisant CU par X, $CU = U_0 + SX$ avec $\deg U_0 < \deg X$ ou $U_0 = 0$, et enfin

$$C = U_0 F + V_0 G,$$

avec $V_0 = CV + SY$. La considération des degrés montre que $\deg V_0 < \deg Y$. Ainsi $\mathcal{E} = \mathcal{F} + \mathcal{G}$. Il est clair que $\dim \mathcal{F} = \deg X$ et $\dim \mathcal{G} = \deg Y$ et l'égalité $\mathcal{E} = \mathcal{F} \bigoplus \mathcal{G}$ fournit

$$\deg P = \deg X + \deg Y.$$

Cependant

$$\deg P = \deg X + \deg F = \deg Y + \deg G$$

d'où la conclusion attendue,

$$\deg P = \deg F + \deg G.$$

□

Après ce résultat théorique, venons en à une question pratique. Le calcul du ppcm ne peut se faire par la formule classique $P = FG/D$, qui n'est plus valable ici. On peut montrer qu'un ppcm de F et G, en supposant que F et G ont d'abord été ramenés dans $\mathbb{K}[z, M]$, est de la forme

$$P = \sum_{\substack{0 \le j \le \mu \\ 0 \le k \le d_F + d_G}} P_{j,k} z^j M^k,$$

en notant m_F et m_G les degrés de F et G comme polynômes en z et

$$\mu = (d_F + 1) B^{d_F} m_G + (d_G + 1) B^{d_G} m_F.$$

On peut donc chercher un ppcm de F et G en employant une méthode de coefficients indéterminés, mais ceci ne se ferait pas sans mal car l'équation $xy = u$ a une infinité de solutions (x, y) dans les fractions rationnelles. Nous préférons employer la méthode assez brutale suivante. D'abord on peut supposer que F et G sont à coefficients polynomiaux et premiers entre eux et nous notons toujours $d_F = \deg_M F$ et $d_G = \deg_M G$ puis $N = d_F + d_G$. D'après la proposition précédente les deux opérateurs ont un ppcm, P, dans les opérateurs de degré N. Cela suppose que

$$P = UF = VG$$

avec

$$U = \sum_k u_k(z) M^k, \quad V = \sum_\ell v_\ell(z) M^\ell,$$

U et V étant de degré $N - d_F$ et $N - d_G$. Pour déterminer ces $N + 2$ inconnues que sont les polynômes u_k et v_ℓ, nous écrivons que UF et VG coïncident sur 1, z, ..., z^{N+1}, *id est*

$$\sum_{k=0}^{N-d_F} u_k(z) M^k F z^j = \sum_{\ell=0}^{N-d_G} u_\ell(z) M^\ell G z^j, \qquad \text{pour } 0 \le j \le N+1.$$

D'après la proposition précédente, la matrice carrée, C_N, de ce système linéaire a pour noyau une droite.

Exemple 8 : Avec $B = 2$, les deux opérateurs $F = zM^2$, $G = z - M$ sont premiers entre eux. Ici $N = 3$ et la matrice du système est

$$C_3 = \begin{bmatrix} z & z^2 & z-1 & z^2-1 & z^4-1 \\ z^5 & z^{10} & 0 & 0 & 0 \\ z^9 & z^{18} & z^3-z^4 & z^6-z^8 & z^{12}-z^{16} \\ z^{13} & z^{26} & z^4-z^6 & z^8-z^{12} & z^{16}-z^{24} \\ z^{17} & z^{34} & z^5-z^8 & z^{10}-z^{16} & z^{20}-z^{32} \end{bmatrix}$$

Elle a un noyau de dimension 1, engendré par le vecteur

$$(\ u_0 \quad u_1 \quad -v_0 \quad -v_1 \quad -v_2\ ) = (\ z^5 \quad -1 \quad 0 \quad 0 \quad -z^2\ ).$$

Il lui correspond les deux opérateurs

$$U = z^5 - M, \quad V = z^2 M^2,$$

et le ppcm cherché,

$$(z^5 - M)(zM^2) = z^2M^2(z - M) = z^6M^2 - z^2M^3.$$

Un ppcm de zM^2 et $z - M$ est donc $z^4M^2 - M^3$.

Si l'on cherche, par curiosité, des solutions dans l'espace des opérateurs de degré inférieur ou égal à 4, on utilise la matrice

$$C_4 = \begin{bmatrix} z & z^2 & z^4 & z-1 & z^2-1 & z^4-1 & z^8-1 \\ z^5 & z^{10} & z^{20} & 0 & 0 & 0 & 0 \\ z^9 & z^{18} & z^{36} & z^3-z^4 & z^6-z^8 & z^{12}-z^{16} & z^{24}-z^{32} \\ z^{13} & z^{26} & z^{52} & z^4-z^6 & z^8-z^{12} & z^{16}-z^{24} & z^{32}-z^{48} \\ z^{17} & z^{34} & z^{68} & z^5-z^8 & z^{10}-z^{16} & z^{20}-z^{32} & z^{40}-z^{64} \\ z^{21} & z^{42} & z^{84} & z^6-z^{10} & z^{12}-z^{20} & z^{24}-z^{40} & z^{48}-z^{80} \\ z^{25} & z^{50} & z^{100} & z^7-z^{12} & z^{14}-z^{24} & z^{28}-z^{48} & z^{56}-z^{96} \end{bmatrix}$$

et le noyau de C_4 admet pour base les 2 vecteurs

$$(\ u_0 \quad u_1 \quad u_2 \quad -v_0 \quad -v_1 \quad -v_2 \quad -v_3\ ) = (\ z^5 \quad -1 \quad 0 \quad 0 \quad 0 \quad -z^2 \quad 0\ ),$$

qui donne à nouveau

$$U = z^5 - M, \quad V = z^2 M^2,$$

mais aussi le vecteur

$$(\ u'_0 \quad u'_1 \quad u'_2 \quad -v'_0 \quad -v'_1 \quad -v'_2 \quad -v'_3\ ) = (\ z^{15} \quad 0 \quad -1 \quad 0 \quad 0 \quad -z^{12} \quad -z^4\ ),$$

qui fournit

$$U' = z^{15} - M^2, \quad V' = z^{12}M^2 + z^4M^3$$

et un multiple commun

$$(z^{15} - M^2)zM^2 = (z^{12}M^2 + z^4M^3)(z - M) = z^{16}M^2 - z^4M^4.$$

Celui-ci est bien un multiple du ppcm :

$$z^{16}M^2 - z^4M^4 = z^4(z^8 + M)(z^4M^2 - M^3).$$

Il est possible de définir la notion de valuation comme nous avons définie celle de degré et nous laissons au lecteur le soin de prouver le résultat suivant.

Proposition 11. *Si F et G sont deux éléments non nuls de $\mathbb{K}(z)[M]$, un* ppcm *de F et G a pour valuation le maximum des valuations de F et G.*

2.4 Factorisation

Malgré quelques défauts, les résultats obtenus jusqu'ici sont très similaires à ceux de l'arithmétique élémentaire. Cependant il ne peut y avoir de théorème de factorisation raisonnable. En effet les factorisations en produit $A_\ell \cdots A_1$ ne correspondent pas à l'arithmétique que nous avons développé et les décompositions de la forme $\text{ppcm}(A_1, \ldots, A_\ell)$ n'existent généralement pas.

Exemple 9 : Avec $B = 2$, les seules écritures de

$$A = (1 - zM)z^2M = z^2M - z^5M$$

sous forme de produit sont

$$A = [c(z) - zc(z^2)M] \frac{z^2}{c(z)} M,$$

où $c(z)$ est une fraction rationnelle non nulle. Les opérateurs M, z^2M et $z^2/c(z)M$ sont associés, mais pas $1 - zM$ et $c(z) - zc(z^2)M$, à moins que $c(z) = c(z^2)$, ce qui signifie que c est dans le corps de base. De plus A n'est pas ppcm de $1 - zM$ et z^2M, puisqu'un ppcm est $M - z^2M$. Une factorisation de A en accord avec les notions définies plus haut devrait fournir un égalité de la forme

$$(A) = (P) \cap (Q).$$

En effet, A n'est pas irréductible puisqu'il est divisible par M. Il ne peut pas avoir plus de deux facteurs puisqu'il est de degré 2. Hélas, le seul facteur disponible est M et nous ne pouvons obtenir une égalité entre idéaux qui exprime que A est réductible.

Les seules factorisations possibles consistent en des produits au sens usuel, mais ceci n'est pas compatible avec l'arithmétique définie plus haut : un produit de facteurs premiers entre eux n'est pas un ppcm des facteurs.

2.5 Interpolation

La détermination de l'idéal annulateur du sous-espace des polynômes de degré inférieur ou égal à n permet de rendre homogènes les équations de Mahler à second membre polynomial.

Proposition 12. *Il existe un unique opérateur $A \in \mathbb{K}(z)[M]$ de degré inférieur ou égal à n, qui prend des valeurs données $b_0, b_1, \ldots, b_n \in \mathbb{K}(z)$ sur $1, z, \ldots, z^n$.*

Démonstration. L'opérateur cherché est de la forme

$$A = \sum_{k=0}^{n} a_k M^k,$$

et l'interpolation se traduit par le système

$$\sum_{k=0}^{n} a_k(z) z^{B^k j} = b_j(z), \quad j = 0, \cdots, n$$

dont la matrice est

$$D_n = \left(z^{B^k j}\right)_{0\leq j,k\leq n}.$$

C'est une matrice de Vandermonde et son déterminant est

$$\Delta_n = \prod_{0\leq k<\ell\leq n} \left(z^{B^\ell} - z^{B^k}\right) \neq 0,$$

d'où la proposition. □

Corollaire 5. *Notons, pour k et n entiers naturels,*

$$A_k = z^{(B-1)k} - M$$

et

$$P_n = \mathrm{ppcm}(A_0, \cdots, A_n).$$

Alors P_n est un opérateur de degré $n+1$ donné par

$$P_n = M^{n+1} - \sum_{k=0}^{n} \prod_{\ell\neq k} \frac{z^{B^{n+1}} - z^{B^\ell}}{z^{B^k} - z^{B^\ell}}\, M^k.$$

Démonstration. La démonstration précédente, appliquée au système dans lequel les seconds membres sont les $M^{n+1}z^j$, permet de calculer P_n. □

Proposition 13. *Un opérateur $A \in \mathbb{K}(z)[M]$, qui s'annule sur $\mathbb{K}[z]_n$, est un multiple de P_n.*

Démonstration. L'opérateur A_k engendre l'annulateur de z^k, donc l'annulateur de $\mathbb{K}[z]_n$ est engendré par le ppcm des A_k, $0 \leq k \leq n$. □

Chapitre 3

Équations de Mahler linéaires

Les équations fonctionnelles de la forme

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z)$$

sont les équations de Mahler linéaires. Il existe de nombreux exemples de telles équations et même d'équations plus générales liées aux questions de transcendance [39, 46], mais ces équations sont très rarement étudiées en elles-même. On trouve dans le travail de Kuczma [47, 48] des indications assez précises pour le cas $N = 1$, mais relativement superficielles dès que $N \geq 2$.

Les séries solutions de ces équations sont les séries mahlériennes. Elles forment une algèbre close par les lois usuelles et par dérivation, tout comme les séries holonomes de Stanley, Lipshitz et Zeilberger [65, 49, 72], et constituent le cadre de cette thèse.

Les résultats d'arithmétique permettent de supposer que l'équation a un coefficient $c_0(z)$ non nul sans introduire de solutions parasites et même fournissent un moyen effectif de calculer une telle équation équivalente. On peut aussi imposer que le second membre $b(z)$ soit nul si l'équation proposée a un second membre mahlérien. Cependant ceci n'est guère utile en pratique car on préfère diminuer l'ordre de l'équation, quitte à augmenter la taille du second membre.

Pour ce qui est des séries formelles, la résolution numérique se fait en deux temps : d'abord par un système linéaire fini, qui détermine la dimension de l'espace des solutions, puis par itération, et ceci permet de montrer que les séries entières obtenues ont un rayon de convergence non nul. Le traitement s'étend d'ailleurs aux équations,

$$c_0(z)f(\phi_0(z)) + c_1(z)f(\phi_1(z)) + \cdots + c_N(z)f(\phi_N(z)) = b(z),$$

baptisées ici équations de Mahler linéaires générales, et fournit des résultats qualitativement similaires. Dans celles-ci les $\phi_k(z)$ sont des séries formelles, ou des fonctions analytiques au voisinage de 0, de valuation supérieure ou égale à 2, sauf $\phi_0(z)$ qui est réversible.

La recherche des solutions sous forme close, en particulier de solutions rationnelles ou sous forme de produits infinis, est une question naturelle qui permet de donner de jolies formules comme

$$1 = \sum_{k\geq 0} \frac{(-1)^k z^{2^k-1}\left(1-z^{2^k}\right)\left(1+2\,z^{2^k}\right)}{(1-2\,z^2)(1-2\,z^4)\cdots(1-2\,z^{2^{k+1}})},$$

$$1-(1-z)\prod_{k\geq 0}\left(1-z^{2^k}\right) = 2\sum_{k\geq 0}\left[z^{2^k}\prod_{k\geq j}\left(1-z^{2^j}\right)\right].$$

Elle amène à déterminer les produits infinis mahlériens qui se réduisent à des fractions rationnelles commme

$$\prod_{k\geq 0} \frac{1}{p(z^{10^k})} = 1 + z + z^2,$$

si $p(z) = 1 - z + z^3 - z^4 + z^6 - z^7 + z^9 - z^{11} + z^{12} - z^{14} + z^{15} - z^{17} + z^{18}$.

3.1 Propriétés de clôture.

Toutes les séries utilisées ici sont des séries formelles à coefficients dans un corps commutatif $\mathbb{K}$.

Définition 12. *Une série de Laurent* $f(z) = \sum_{n=n_0}^{+\infty} f_n z^n$, $n_0 \in \mathbb{Z}$, *est* B*-mahlérienne si elle satisfait une équation de Mahler homogène*

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = 0$$

à coefficients des fractions rationnelles $c_0, \ldots, c_N$ *non toutes nulles.*

Evidemment on peut supposer que les $c_k(z)$ sont des polynômes mais la définition précédente met l'accent sur le fait que $f(z)$, $f(z^B)$, …, $f(z^{B^N})$ forment une famille liée dans le $\mathbb{K}(z)$-espace vectoriel $\mathbb{K}((z))$. Ceci est à rapprocher de l'étude des séries D-finies ou holonomes, dont les dérivées successives engendrent un espace de dimension finie sur les fractions rationelles.

Le fait que $\mathbb{K}[z, M]$ soit principal à gauche implique tout de suite l'existence d'une équation minimale pour une série mahlérienne, dont l'ordre fournit la dimension de l'espace engendré par les $f(z^{B^k})$ sur $\mathbb{K}(z)$. En effet les opérateurs qui s'annulent sur une série mahlérienne $f(z)$ forment un idéal à gauche, qui est principal et est engendré par un opérateur P. L'équation $P(z, M)h(z) = 0$ est une équation minimale de $f(z)$ et le quotient $\mathbb{K}(z)[M]/(P)$ est isomorphe, comme $\mathbb{K}(z)$-espace vectoriel, à $\mathbb{K}(z)[M]_{<d}$, l'espace des opérateurs de degré strictement inférieur à $d = \deg P$, et à l'espace engendré par les $f(z^{B^k})$ dans $\mathbb{K}((z))$.

Définition 13. *Une équation minimale d'une série mahlérienne* $f(z)$ *est un générateur de l'idéal à gauche des opérateurs de* $\mathbb{K}[z, M]$ *qui s'annulent sur* $f(z)$.

Il sera commode d'employer la convention suivante pour éviter des formulations par cas.

Définition 14. *Une suite* (f_n) *à valeurs dans un anneau est étendue des entiers aux rationnels par la valeur 0,*

$$f_x = \begin{cases} f_n & \text{si } x = n \in \mathbb{N}, \\ 0 & \text{sinon.} \end{cases}$$

En particulier $(f_{n/B})$ est la suite qui vaut f_k si $n = kB$ est multiple de B et 0 sinon.

Au lieu d'exprimer la définition d'une série mahlérienne sur la série formelle, on peut l'énoncer en termes de récurrence sur ses coefficients. Or les deux opérateurs de base sur les séries, la multiplication par z et la substitution par z^B,

$$f(z) \longmapsto z\,f(z), \quad f(z) \longmapsto f(z^B),$$

se traduisent immédiatement dans l'espace des suites par l'opérateur de décalage et l'opérateur d'homothétie sur les indices,

$$(f_n) \longmapsto (f_{n-1}), \quad (f_n) \longmapsto (f_{n/B}).$$

Définition 15. *Une suite (f_n) est B-mahlérienne si elle satisfait une relation de récurrence*

$$\sum_\ell c_{0,\ell}\, f_{n-\ell} + \sum_\ell c_{1,\ell}\, f_{(n-\ell)/B} + \cdots + \sum_\ell c_{N,\ell}\, f_{(n-\ell)/B^N} = 0$$

avec les scalaires $c_{k,\ell}$ non tous nuls, c'est-à-dire si sa série génératrice est mahlérienne.

Théorème 3. *L'espace des séries B-mahlériennes possède les propriétés de stabilité suivantes :*

1. *les fractions rationnelles sont mahlériennes ;*
2. *si $f(z) \in \mathbb{K}((z))$ satisfait une équation de Mahler*

$$c_0(z)f(z) + c_1(z)f(z^B) + \ldots + c_N(z)f(z^{B^N}) = b(z),$$

   dont le second membre $b(z)$ est une série mahlérienne, alors $f(z)$ est une série mahlérienne ;
3. *si $f(z)$ est mahlérienne, il en est de même de $f(z^B)$;*
4. *les séries mahlériennes forment un sous-espace vectoriel du $\mathbb{K}$-espace vectoriel $\mathbb{K}((z))$ et même du $\mathbb{K}(z)$-espace vectoriel $\mathbb{K}((z))$;*
5. *si f et g sont deux séries mahlériennes, il en est de même de leur produit de Cauchy $f \times g$;*
6. *si f est une série mahlérienne, sa série dérivée f' est aussi mahlérienne.*

Démonstration. Le premier, le deuxième et le troisième points sont évidents. Pour le premier, il suffit d'écrire

$$r(z) = \frac{r(z)}{r(z^B)}\, r(z^B).$$

Pour le second, on multiplie à gauche l'équation avec second membre par un opérateur qui annule $b(z)$ et pour le troisième on multiplie à gauche l'équation par M.

Pour le quatrième, il suffit de remarquer que le ppcm de deux opérateurs qui s'annulent respectivement sur deux séries mahlériennes s'annule sur leur somme.

En ce qui concerne le produit de Cauchy, on écrit les équations vérifiées par $f(z)$ et $g(z)$ sous la forme

$$f(z^{B^K}) = \sum_{k=0}^{K-1} a_k(z) f(z^{B^k}), \quad g(z^{B^L}) = \sum_{k=0}^{L-1} b_k(z) f(z^{B^k})$$

et on constate ainsi que tous les produits $f(z^{B^k})g(z^{B^\ell})$, $k \geq 0$, $\ell \geq 0$, vivent dans le sous-espace engendré par les $f(z^{B^k})g(z^{B^\ell})$ avec $0 \leq k < K$, $0 \leq \ell < L$. Comme celui-ci est de dimension au plus KL, le produit fg vérifie une équation d'ordre au plus KL.

Enfin si f est solution de

$$c_0(z)f(z) + c_1(z)f(z^B) + \ldots + c_N(z)f(z^{B^N}) = 0,$$

alors sa dérivée f' vérifie

$$c_0(z)f'(z) + Bz^{B-1}c_1(z)f'(z^B) + \ldots + B^N z^{B^N-1}c_N(z)f'(z^{B^N}) =$$
$$- \Big(c_0'(z)f(z) + c_1'(z)f(z^B) + \ldots + c_N'(z)f(z^{B^N})\Big)$$

et le second membre est mahlérien, ce qui fait que f' est mahlérienne. □

Si le corps est de caractéristique nulle, on peut parler de primitive. Cependant une primitive de série mahlérienne n'est pas nécessairement mahlérienne.

EXEMPLE 10 : La série à coefficients rationnels

$$\ln \frac{1}{1-z} = \sum_{n\geq 1} \frac{z^n}{n},$$

dont la dérivée est mahlérienne puisque rationnelle, n'est pas mahlérienne.

Supposons qu'elle satisfasse une relation de dépendance

$$c(z) + \sum_{k=0}^{N} c_k(z) \ln \frac{1}{1-z^{B^k}} = 0$$

dans laquelle $c(z)$ et les $c_k(z)$ sont des polynômes. *A priori* cette égalité est formelle, mais elle a aussi un sens du point de vue analytique, si z est une variable complexe de module strictement plus petit que 1. L'évaluation de la limite du membre gauche en un point ζ qui est une racine B^N-ième de l'unité sans être une racine B^{N-1}-ième de l'unité, montre que le polynôme $c_N(z)$ est divisible par le polynôme $(z^{B^N}-1)/(z^{B^{N-1}}-1)$ car seul le dernier terme est susceptible d'avoir une limite infinie. Il en résulte que dans une telle relation le polynôme $c_N(z)$ est soit nul soit de degré non nul.

Si la série est mahlérienne, on peut tenir le raisonnement suivant. Partant de 1, qui forme une famille libre, on adjoint successivement $\ln(1-z)^{-1}$ (celle-ci n'est pas rationnelle et la famille est encore libre), $\ln(1-z^B)^{-1}$, *etc*, jusqu'au premier N telle que la famille soit liée, c'est-à-dire vérifie une relation

$$c(z) + \sum_{k=0}^{N} c_k(z) \ln \frac{1}{1-z^{B^k}} = 0$$

avec $c_N \neq 0$. On impose à c et aux c_k d'être des polynômes, puis on dérive, ce qui donne après simplification par le produit des $1-z^{B^k}$, $0 \leq k \leq N$,

$$C(z) + \sum_{k=0}^{N} c_k'(z) \ln \frac{1}{1-z^{B^k}} = 0$$

et c_N' n'est pas nul d'après notre remarque. Ceci permet de fabriquer une équation d'ordre plus petit en combinant les deux précédentes et contredit la minimalité de N. Ainsi $\ln(1-z)^{-1}$ n'est pas mahlérienne.

Le même raisonnement permet de prouver que les $1/(1-z)^\alpha$ avec α réel positif non entier ne sont pas mahlériennes.

Le produit de Hadamard de deux séries mahlériennes n'est généralement pas mahlérien.

EXEMPLE 11 : La série génératrice du nombre de partitions binaires

$$b(z) = \prod_{k\geq 0} \frac{1}{1-z^{2^k}}$$

est évidemment mahlérienne et il en est de même de

$$f(z) = \sum_{k\geq 0} z^{2^k}.$$

Si le produit de Hadamard

$$a(z) = b(z) \odot f(z) = \sum_{k\geq 0} b_{2^k}\, z^{2^k}$$

est mahlérien, la suite des coefficients vérifie une relation de récurrence de la forme

$$a_n = c_{0,1}\, a_{n-1} + c_{0,2}\, a_{n-2} + \cdots + c_{1,0}\, a_{n/2} + c_{1,1}\, a_{(n-1)/2} + \cdots .$$

En prenant pour n une puissance de 2 et en remarquant que les a_{n-1}, a_{n-2}, $a_{(n-1)/2}$, *etc* sont alors nuls, on constate que la suite (b_{2^k}) est solution d'une récurrence avec décalage

$$b_{2^k} = c_{1,0}\, b_{2^{k-1}} + c_{2,0}\, b_{2^{k-2}} + \cdots$$

et est donc rationnelle. Ceci est incompatible avec le fait que $\ln b_{2^k}$ a une croissance en k^2 [23].

3.2 Solutions formelles

Le fait que l'opérateur de Mahler soit local, c'est-à-dire utilise une substitution qui laisse 0 invariant, permet une approche formelle que nous allons abondamment utiliser.

La donnée est une équation de Mahler linéaire

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z)$$

et les solutions $f(z)$ sont ici des séries formelles de $\mathbb{K}[[z]]$ ou $\mathbb{K}((z))$. Les coefficients c_k sont des fractions rationnelles, l'entier N vaut au moins 1 et le coefficient $c_N(z)$ n'est pas nul. Le second membre est au choix une fraction rationnelle ou une série formelle. En multipliant au besoin l'équation par un dénominateur commun des c_k nous pouvons supposer que ceux-ci sont des polynômes.

3.2.1 Réduction au cas $c_0 \neq 0$

Nous allons montrer que l'on peut ramener l'équation proposée à une équation équivalente dans laquelle le coefficient $c_0(z)$ est non nul.

En appliquant les opérateurs de B-section aux deux membres de l'équation, plusieurs fois s'il le faut, l'équation est transformée en un système d'équations de Mahler, toutes d'ordre strictement plus petit que N et ayant toutes un coefficient c_0 non nul, à moins que tous leurs coefficients c_k ne soient nuls. Plus précisément nous construisons un B-arbre dont la racine est étiquetée par l'équation de départ et tel que chaque nœud a pour fils les équations obtenues en appliquant à l'équation qui étiquette ce nœud les opérateurs S_r. Les feuilles sont étiquetées par les équations qui ont un c_0 non nul ou un membre gauche nul.

Exemple 12 : En appliquant les opérateurs indiqués à gauche, l'équation 2-Mahler

$$(1+z^{16}+z^{18})M^2f - z^{32}M^3f + (1-z^{40}+z^{42}+z^{43})M^4f + z^{59}M^5f = 1+z^{15}$$

fournit le système

$$\begin{array}{lrcl}
S_0 & (1+z^8+z^9)Mf - z^{16}M^2f + (1-z^{20}+z^{21})M^3f & = & 1 \\
S_0S_0 & (1+z^4)f - z^8Mf + (1-z^{10})M^2f & = & 1 \\
S_1S_0 & z^4f + z^{10}M^2f & = & 0 \\
S_1 & z^{21}M^3f + z^{29}M^4f & = & z^7 \\
S_0S_1 & 0 & = & 0 \\
S_1S_1 & z^{10}M^2f + z^{14}M^3f & = & z^3 \\
S_0S_1S_1 & z^5Mf + z^7M^2f & = & 0 \\
S_0S_0S_1S_1 & 0 & = & 0 \\
S_1S_0S_1S_1 & z^2f + z^3Mf & = & 0 \\
S_1S_1S_1 & 0 & = & z,
\end{array}$$

dont la dernière équation montre d'ailleurs qu'il n'a pas de solution. Si on ne garde que les feuilles de l'arbre, le système se réduit à

$$\begin{array}{lrcl}
S_0S_0 & (1+z^4)f - z^8Mf + (1-z^{10})M^2f & = & 1 \\
S_1S_0 & z^4f + z^{10}M^2f & = & 0 \\
S_0S_1 & 0 & = & 0 \\
S_0S_0S_1S_1 & 0 & = & 0 \\
S_1S_0S_1S_1 & z^2f + z^3Mf & = & 0 \\
S_1S_1S_1 & 0 & = & z.
\end{array}$$

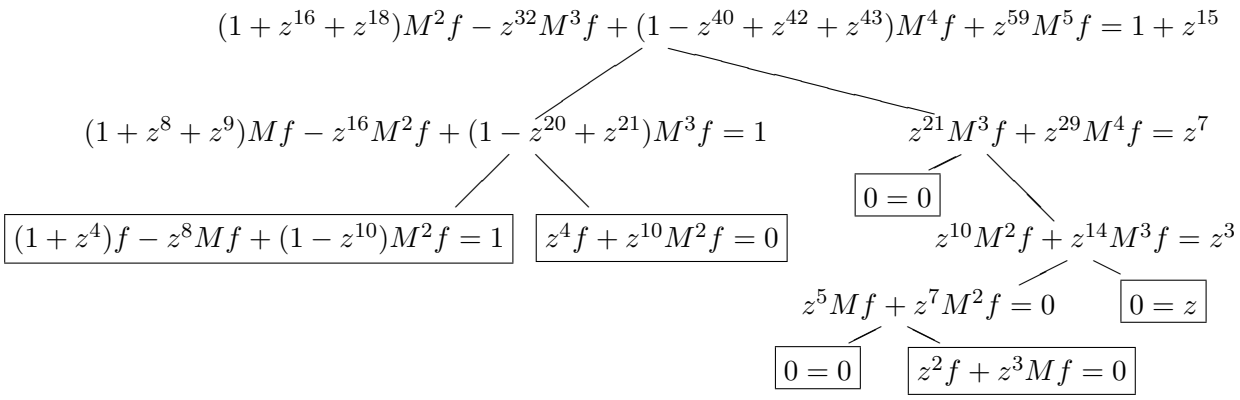

FIG. 3.1
La racine de l'arbre est étiquetée par l'équation proposée et les descendants sont étiquetés par les sections de cette équation. Ainsi les feuilles de l'arbre donnent un système dans lequel toutes les équations à premier membre non nul ont un c_0 non nul.

D'une façon générale ce système est équivalent à l'équation de départ parce que

$$P = \sum_{0\le r<B} z^r M S_r P \quad \text{pour } P \in \mathbb{K}(z)[M],\ \omega_M(P) > 0$$

et

$$b = \sum_{0\le r<B} z^r M S_r b \quad \text{pour } b \in \mathbb{K}[[z]]$$

(S_rP est le composé de deux endomorphismes, alors que S_rb est l'image de b par l'opérateur S_r). D'ailleurs les étiquettes des feuilles déterminent toutes les étiquettes de l'arbre, grâce à l'unicité de l'écriture en base B des entiers. Il y a dans le système des équations à membre gauche non nul si et seulement si c'est le cas pour l'équation initiale (d'après l'égalité $P = \sum z^r M S_r P$) et les membres droits dépendent linéairement du membre droit de l'équation initiale car ils ont été obtenus par application des opérateurs de B-section. Nous avons ainsi prouvé le lemme suivant.

Lemme 6. *Une équation de Mahler*

$$Af = b,$$

avec $A \in \mathbb{K}(z)[M]$, $A \neq 0$ et $\omega_M(A) > 0$, est équivalente à un système

$$\begin{cases} A_1 f &= b_1 \\ A_2 f &= b_2 \\ \quad\vdots & \quad\vdots \\ A_m f &= b_m. \end{cases}$$

dans lequel les A_i appartiennent à $\mathbb{K}(z)[M]$ et sont non tous nuls. De plus les A_i non nuls ont une valuation (par rapport à M) qui est nulle et un degré strictement plus petit que celui de A. Enfin les b_i dépendent linéairement de b.

Supposons maintenant que nous ayons un système $(\mathcal{S})$:

$$\left\{\begin{array}{rcl} A_1 f & = & b_1 \\ A_2 f & = & b_2 \\ \vdots & & \vdots \\ A_m f & = & b_m \end{array}\right.$$

dans lequel les A_i sont dans $\mathbb{K}(z)[M]$ et non tous nuls.

Notons D le pgcd des A_i, ou des A_i non nuls si l'on préfère. Dans le système $(\mathcal{S})$, il y a (au moins) un opérateur A_i de degré minimal en M, disons A_1. Nous divisons euclidiennement chaque A_i, $2 \leq i \leq m$, par A_1, ce qui s'écrit

$$A_i = Q_i A_1 + R_i \quad \text{avec} \;\; R = 0 \;\; \text{ou} \;\; \deg R < \deg A_1$$

et nous remplaçons le système $(\mathcal{S})$ par le système équivalent $(\mathcal{S}')$

$$\left\{\begin{array}{rcl} A_1 f & = & b_1 \\ R_2 f & = & b_2 - Q_2 b_1 \\ \vdots & & \vdots \\ R_m f & = & b_m - Q_m b_1. \end{array}\right.$$

L'itération de ce procédé fournit un système $(\mathcal{S}^\omega)$ équivalent à $(\mathcal{S})$, qui est de la forme

$$\left\{\begin{array}{rcl} Df & = & b \\ 0 & = & b'_2 \\ \vdots & & \vdots \\ 0 & = & b'_m. \end{array}\right.$$

En effet les opérateurs qui apparaissent dans les membres gauches des équations sont tous dans l'idéal (D) et cette suite de divisions euclidiennes n'est qu'une petite généralisation de l'algorithme d'Euclide, d'ailleurs classique dans la réduction des matrices sur un anneau principal. Enfin les b'_i sont obtenus à partir des b_i par application d'opérateurs pris dans $\mathbb{K}(z)[M]$.

Lemme 7. *Soit $(\mathcal{S})$ un système d'équations de Mahler*

$$\left\{\begin{array}{rcl} A_1 f & = & b_1 \\ A_2 f & = & b_2 \\ \vdots & & \vdots \\ A_m f & = & b_m \end{array}\right.$$

où les A_i, $1 \leq i \leq m$, sont dans $\mathbb{K}(z)[M]$ et non tous nuls de pgcd *D. Ce système est équivalent à un système $(\mathcal{S}^\omega)$*

$$\left\{\begin{array}{rcl} Df & = & b'_1 \\ 0 & = & b'_2 \\ \vdots & & \vdots \\ 0 & = & b'_m \end{array}\right.$$

dans lequel les second membres b'_i dépendent linéairement des b_i.

EXEMPLE 13 : Prenons le système (avec $B = 2$)

$$\begin{cases} (1+z^4)f(z) + (z+z^5-z^8)f(z^2) + (1-2z^{10})f(z^4) + (z^4-z^{14})f(z^8) &= z+z^5 & (1) \\ f(z) + zf(z^2) + z^6 f(z^4) z^{10} f(z^8) &= 1+z+z^2 & (2). \end{cases}$$

En divisant par l'opérateur $1 + zM + z^6M^2 + z^{10}M^3$, qui apparaît dans l'équation (2), nous obtenons

$$\begin{cases} f(z) + zf(z^2) + z^6 f(z^4) + z^{10} f(z^8) &= 1+z+z^2 & (2) \\ (1-z^6-2z^{10})f(z) + (z-z^7-2z^{11}+z^{14})f(z^2) + z^{16} f(z^4) &= 1+z+z^2-z^7-z^{10}-2z^{11}-z^{12} & (3) \end{cases}$$

puis en utilisant l'équation (3)

$$\begin{cases} (1-z^6-2z^{10})f(z) + (z-z^7-2z^{11}+z^{14})f(z^2) + z^{16} f(z^4) &= 1+z+z^2-z^7-z^{10}-2z^{11}-z^{12} & (3) \\ f(z) + zf(z^2) &= 2z^2+z+3 & (4) \end{cases}$$

et enfin avec (4)

$$\begin{cases} f(z) + zf(z^2) &= 3+z+2z^2 & (4) \\ 0 &= 2+z^2-3z^6-2z^8-5z^{10}-3z^{12}+3z^{14}+z^{16}+2z^{18} & (5). \end{cases}$$

La conjonction des deux lemmes précédents permet d'énoncer le théorème de réduction suivant.

Théorème 4. *Une équation de Mahler*

$$Af = b,$$

avec $A \in \mathbb{K}(z)[M]$ non nul, est équivalente à un système d'équations de Mahler

$$\begin{cases} Df &= b'_1 \\ 0 &= b'_2 \\ \vdots & \vdots \\ 0 &= b'_m \end{cases}$$

dans lequel D est dans $\mathbb{K}(z)[M]$ et de valuation nulle. De plus les b'_i dépendent $\mathbb{K}$-linéairement des b_i, $1 \leq i \leq m$.

DÉMONSTRATION. Nous obtenons ce résultat en appliquant autant de fois que nécessaire le lemme 6 suivi du lemme 7. Les degrés des opérateurs obtenus à chaque étape décroissent strictement et l'algorithme se termine bien en un nombre fini de pas. □

Pour une équation homogène il n'y a pas de contraintes sur le second membre et l'énoncé est plus simple.

Corollaire 6. *Une équation de Mahler homogène*

$$Af = 0,$$

avec $A \in \mathbb{K}(z)[M]$ non nul, est équivalente à une équation de Mahler

$$Df = 0$$

dans lequel D est dans $\mathbb{K}(z)[M]$ et de valuation nulle.

3.2.2 Réduction à un système fini d'équations

Nous pouvons désormais ne plus considérer que des équations de Mahler dont le coefficient c_0 est non nul,

$$\sum_{k=0}^{N} c_k(z) f(z^{B^k}) = b(z).$$

Notre but est ici de montrer que la résolution à une précision donnée dans l'espace des séries formelles d'une équation de Mahler se scinde en deux problèmes, obtenus en coupant la série formelle cherchée à un certain niveau, l'entier critique.

Définition 16. *Soit*

$$\sum_{k=0}^{N} c_k(z) f(z^{B^k}) = b(z)$$

une équation de Mahler dont les coefficients $c_0(z)$, ..., $c_N(z)$ et $b(z)$ sont des séries formelles avec $c_0(z)$ non nul. Nous notons δ_k la valuation de la série $c_k(z)$. L'entier critique est

$$D = \left\lfloor \max_{1\le k\le N} \frac{B^k\delta_0 - \delta_k}{B^k - 1} \right\rfloor.$$

Pour étudier une équation de Mahler, il faut d'abord mettre en valeur les valuations :

$$c_k(z) \quad = \quad z^{\delta_k} C_k(z) = \sum_{j\ge\delta_k} c_{k,j} z^j.$$

Nous distinguons partie basse et partie haute :

$$\begin{aligned}
\underline{f}(z) &= \sum_{n=0}^{D-\delta_0} f_n z^n, \\
f(z) &= \underline{f}(z) + z^{D-\delta_0+1} F(z), \\
\\
\underline{b}(z) &= \sum_{n=0}^{D} b_n\, z^n, \\
b(z) &= \underline{b}(z) + z^{D+1}\overline{b}(z), \\
\\
z^{D+1}E(z) &= b(z) - \sum_{k=0}^{N} c_k(z)\underline{f}(z^{B^k}), \\
\lambda_k &= \delta_k + (B^k - 1)(D - \delta_0 + 1) \ge 1.
\end{aligned}$$

Enfin la notation classique $[z^n]g(z)$ désigne le coefficient de z^n dans la série $g(z)$,

$$[z^n] \sum_k g_k\, z^k = g_n.$$

La démonstration s'appuie sur une idée géométrique simple, qui apparait clairement dans l'exemple de la page 39 et dans la figure 3.2. Avec toutes ces notations le coefficient de z^m dans le premier membre de l'équation

$$\sum_{k=0}^{N} c_k(z) f(z^{B^k}) = b(z)$$

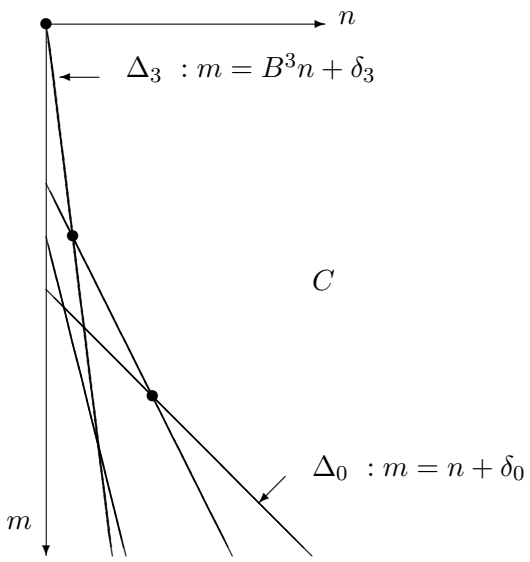

FIG. 3.2
Les équations de Mahler se prêtent à une vision géométrique de type polygone de Newton. A un terme $c_k(z)\, f(z^{B^k})$ de l'équation correspond la droite d'équation $m = B^k n + \delta_k$, où δ_k est la valuation de $c_k(z)$. Les degrés de liberté sont associés aux sommets du convexe C limité par ces droites.

est

$$\sum_{k=0}^{N} \sum_{j=\delta_k}^{m} c_{k,j}[z^{m-j}] f(z^{B^k}).$$

Pour

$$m > \max_{k=1\cdots N} \frac{B^k \delta_0 - \delta_k}{B^k - 1},$$

et $1 \leq k \leq N$, on a

$$m > \frac{B^k \delta_0 - \delta_k}{B^k - 1}$$

et *a fortiori*

$$(m - \delta_0) B^k > m - j \;\text{ si }\; j \geq \delta_k.$$

Ainsi pour $n \geq m - \delta_0$ le monôme $f_n\, z^n$ de la série $f(z)$ produit dans $f(z^{B^k})$ un terme de valuation au moins égale à nB^k et donc strictement plus grande que $m - j$ pour $j \geq \delta_k$: il a une contribution nulle dans le terme d'indice $k = 1 \ldots N$:

$$\sum_{j=\delta_k}^{d_k} c_{k,j}[z^{m-j}] f(z^{B^k}).$$

Il en est de même pour le terme d'indice $k = 0$ si $n > m - \delta_0$ car le z, qui intervient dans le terme d'indice 0 de l'équation, est de valuation 1. Quant au monôme $f_{m-\delta_0} z^{m-\delta_0}$ il fournit exactement $c_{0,\delta_0} f_{m-\delta_0}$ dans l'équation qui exprime l'égalité des coefficients de z^m dans les deux membres de l'équation de Mahler.

Ainsi le système linéaire infini associé à l'équation est-il triangulaire inférieur à partir du rang $D+1$. Sa résolution se divise donc en deux sous-problèmes : d'une part l'étude du système linéaire qui exprime l'égalité des coefficients de z^m dans les deux membres de l'équation pour $m = 0, \ldots, D$ et ce système ne porte que sur les inconnues $f_0, \ldots, f_{D-\delta_0}$, d'autre part le dévidement de la relation de récurrence qui permet de calculer les f_n d'indices supérieurs.

Exemple 14 : Considérons l'équation homogène d'ordre 2

$$z^3\,(1+z)^4\,f(z) - \left(1 + 4\,z^2 - z^3 + z^4 - 10\,z^5 - 6\,z^6 - 5\,z^7\right) f(z^2) - \left(z^2+1\right)^5 f(z^4) = 0.$$

Ici $\delta_0 = 3$ et $\delta_1 = \delta_2 = 0$, ce qui donne $D = 6$ et $D - \delta_0 = 3$. Cela signifie que le système qui détermine la partie inférieure des solutions s'obtient en considérant le coefficient de z^n dans l'équation pour n allant de 0 à 6 et porte sur les inconnues $f_0, \ldots, f_3$. Le début de la matrice infinie du système montre bien cette situation,

$$\begin{pmatrix}
-2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-9 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-7 & -4 & -1 & 0 & 0 & 0 & 0 & 0 \\
16 & 5 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 14 & 7 & 4 & 1 & 0 & 0 & 0 \\
-5 & -3 & 2 & 2 & 3 & 1 & 0 & 0 \\
0 & 5 & 11 & 5 & 6 & 4 & 1 & 0 \\
-1 & -10 & 1 & 0 & 0 & 5 & 4 & 1
\end{pmatrix}.$$

La résolution du petit système fournit $f_0 = f_1 = f_2 = 0$ et f_3 est arbitraire. Ainsi l'espace des solutions est de dimension 1. Par itération nous obtenons à z^{14} près,

$$f(z) = f_3\,\left(z^3 - 4\,z^4 + 10\,z^5 - 21\,z^6 + 34\,z^7 - 52\,z^8 + 88\,z^9 - 130\,z^{10} + 155\,z^{11} - 199\,z^{12} + 307\,z^{13} + \cdots\right).$$

En réduisant modulo 2, une variante de la suite de Rudin-Shapiro [3, p. 244] apparaît,

$$u(z) = z^3 + z^6 + z^{11} + z^{12} + z^{13} + z^{15} + z^{19} + \cdots .$$

Clairement la méthode précédente permet de traiter des équations plus générales.

Définition 17. *Une équation de Mahler linéaire générale est une équation de la forme*

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = b(z),$$

pour laquelle les coefficients $c_k(z)$, le second membre $b(z)$ et les $\phi_k(z)$ sont des séries formelles avec

$$\phi_0(z) = z,$$

$$\omega_k = \omega(\phi_k) > 1 \quad (k = 1 \ldots N)$$

et toujours

$$c_0(z) \neq 0.$$

Exemple 15 : Les opérateurs de Mahler M_B relatifs à des entiers B distincts commutent et forment même une famille stable par composition. Les équations associées aux opérateurs de l'algèbre $\mathbb{K}[z, (M_B)_{B\geq 2}]$,

$$c_0(z)\,f(z) + \sum_{k=1}^{N} c_k(z)\,f(z^{B_k}) = b(z),$$

sont des équations de Mahler générales, dans la mesure où $c_0(z)$ n'est pas nul.

Définition 18. *Pour une équation de Mahler générale*

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = b(z),$$

l'entier critique est

$$D = \left\lfloor \max_{k=1\cdots N} \frac{\omega_k \delta_0 - \delta_k}{\omega_k - 1} \right\rfloor.$$

La résolution numérique se fait encore en deux temps : résolution d'un système linéaire pour la partie basse et, s'il y a des solutions, itération pour obtenir la partie haute à une précision donnée. D'ailleurs on peut généraliser encore un peu la situation. La propriété utile de ϕ_0 est d'être réversible (*id est* inversible au sens de la composition des séries formelles). En effet si tel est le cas, en notant $\phi_0^{[-1]}$ la série réverse, l'équation se transforme en

$$a_0(t) f(t) + \sum_{k=1}^{N} a_k(t) f(\chi_k(t)) = E(t),$$

avec

$$a_k(t) = c_k(\phi_0^{[-1]}(t)), \quad k = 0 \cdots N, \quad E(t) = b(\phi_0^{[-1]}(t)),$$

$$\chi_k(t) = \phi_k(\phi_0^{[-1]}(t)), \quad k = 1 \cdots N.$$

Les propriétés d'existence, d'unicité ou de dimension de l'espace des solutions $\mathcal{S}$ sont conservées dans la composition par une série réversible et les résultats qualitatifs sont encore valables. Pour ce qui est du calcul, la connaissance de $\phi_0^{[-1]}$ (en utilisant le théorème de Lagrange, par exemple) n'est indispensable que si l'on désire connaître explicitement les solutions. En effet chaque χ_k a la même valuation que le ϕ_k correspondant et le nombre D est toujours le même. On peut donc étudier la vacuité de $\mathcal{S}$, déterminer la dimension de $\mathcal{S}$ et même calculer les solutions à une précision donnée en résolvant le système linéaire correspondant.

La recherche des coefficients $f_{D-\delta_0+1}, \ldots$ peut être exprimée en termes de séries. La substitution dans l'équation de Mahler générale de l'expression

$$f = \underline{f} + z^{D-\delta_0+1} F$$

donne pour F une équation de point fixe

$$C_0(z) F(z) + \sum_{k=1}^{N} z^{\lambda_k} C_k(z) \Phi_k(z)^{D-\delta_0+1} F(z^{\omega_k} \Phi_k(z)) = E(z),$$

avec

$$\lambda_k = \delta_k + (\omega_k - 1)(D - \delta_0 + 1) \geq 1$$

et $C_k(0) \neq 0$. Au passage remarquons que la définition de $E(z)$ est correcte parce que

$$\sum_{k=0}^{N} c_k(z) \underline{f}(\phi_k(z)) = \underline{b}(z) \quad \text{modulo } z^{D+1}.$$

Cette nouvelle équation possède une unique solution parce que le système infini correspondant est triangulaire inférieur avec des 1 sur la diagonale. L'application qui à une série g associe

$$\frac{E(z) - \sum_{k=1}^{N} z^{\lambda_k} C_k(z) \Phi_k(z)^{D-\delta_0+1} g(z^{\omega_k} \Phi_k(z))}{C_0(z)}$$

est une contraction affine de $\mathbb{K}[[z]]$ et possède donc un unique point fixe, qui est F, en utilisant le fait que $\mathbb{K}[[z]]$ muni de sa métrique usuelle est complet.

Théorème 5. *La non-vacuité et la dimension de l'espace des solutions d'une équation de Mahler linéaire générale*

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = b(z)$$

sont déterminées par la résolution d'un système linéaire $\mathcal{S}$ constitué de $D+1$ équations en les inconnues $f_0, \cdots, f_{D-\delta_0}$, lequel est obtenu en considérant les coefficients de $1, z, \cdots, z^D$ dans l'équation de Mahler.

La partie basse des solutions est obtenue par la résolution du système $\mathcal{S}$.

La partie haute est déterminée par itération d'un opérateur contractant.

Corollaire 7. *Une série $f(z)$ solution d'une équation de Mahler générale homogène*

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = 0$$

dont les coefficients f_n sont nuls pour $n \leq D - \delta_0$ est la série nulle.

La méthode de résolution fournit un critère d'Eisenstein.

Corollaire 8. *Soient $\mathbb{A}$ un anneau intègre, $\mathbb{K}$ son corps des fractions et $f \in \mathbb{K}[[z]]$ une série mahlérienne. Il existe un élément non nul $a \in \mathbb{A}$ tel que la série*

$$\sum_{n \geq 0} f_n a^n z^n$$

soit mahlérienne à coefficients dans $\mathbb{A}$.

Démonstration. La résolution de la partie basse d'une équation minimale à coefficients dans $\mathbb{A}$ satisfaite par $f(z)$ fournit des coefficients f_n avec un certain dénominateur d, qui est d'ailleurs un mineur de la matrice du système. L'obtention de la partie haute provoque à chaque cran la division par le coefficient de plus bas degré de $c_0(z)$. Il suffit de prendre pour a le produit de d et de ce coefficient. □

Remarquons que l'entier critique D est inférieur ou égal à $2\,\delta_0$ et que l'espace des solutions est de dimension au plus $D - \delta_0 + 1$, ce qui est moindre que $\delta_0 + 1$. Cependant une majoration plus naturelle de la dimension est fournie par la proposition suivante.

Proposition 14. *La dimension de l'espace des solutions d'une équation de Mahler générale homogène,*

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = 0,$$

est moindre que N.

DÉMONSTRATION. La matrice infinie qui détermine les coefficients d'une solution est plongée dans le quadrant positif de $\mathbb{R}^2$, les coefficients étant affectés aux points dont les deux coordonnées sont des entiers naturels. Il existe une partie convexe C (cf. figure 3.2) dans laquelle tous les coefficients sont nuls. Elle est limitée par les droites Δ_k d'équation $m = \omega_k n + \delta_k$ pour $0 \leq k \leq N$. Dans ces équations m est l'indice de ligne ou ordonnée et n est l'indice de colonne ou abscisse. L'axe des ordonnées est orienté de façon inhabituelle pour respecter l'écriture des matrices. La frontière de cette partie convexe C est constituée d'une part de l'axe des abscisses et d'autre part de segments des droites Δ_k avec $1 \leq k \leq N$ et d'une demi-droite de Δ_0. Plus précisément seules certaines droites Δ_k contribuent à la frontière, suivant les valeurs des pentes ω_k et des ordonnées à l'origine δ_k. De plus les pentes de celles qui apparaissent vont en décroissant strictement quand on parcourt la frontière depuis l'origine. Il en résulte que la frontière ne peut pas comporter plus de N segments ou demi-droites dans cette partie qui n'est pas l'axe des abscisses et le convexe C ne peut avoir plus de N coins ou plus vulgairement points extrémaux.

Dévider la récurrence qui définit une solution revient à considérer successivement les lignes de la matrice. Chaque ligne est limitée à droite par la partie C et a une longueur entière. Si elle n'est pas plus longue que la ligne précédente, elle fournit une contrainte sur les termes déjà définis et cela ne peut que diminuer la dimension de l'espace des solutions. Si elle est plus longue que la précédente, ce ne peut être que d'une unité car les pentes des droites Δ_k sont plus grandes que 1. Dans ce cas ou bien le coefficient extrême est non nul et l'équation correspondante détermine un nouveau terme de la suite, ce qui n'accroît pas la dimension de l'espace des solutions ou bien le coefficient extrême est nul et il est alors possible que cette dimension augmente de 1. Ce coefficient ne peut être nul que s'il y a un phénomène de collision ; deux droites Δ_k se rencontrent en un point à coordonnés entières et les contributions s'annulent, ce qui ne donnent pas de contrainte sur le dernier terme de la suite. On voit ainsi que la dimension ne peut pas excéder le nombre de points extrémaux à coordonnées entières. Ceci n'est d'ailleurs encore qu'une grossière majoration car les coefficients de la matrice associés doivent être nuls et il se peut que les autres équations imposent encore des contraintes. En tous cas ceci donne la majoration cherchée car le nombre de points extrémaux de C ne peut pas excéder N. □

La démonstration précédente fournit en prime un moyen d'estimer la dimension de l'espace des solutions d'une équation de Mahler, qui s'appuie sur un graphique comme celui de la figure 3.2. Pour chaque point extrémal, marqué d'un •, on regarde si les termes de plus bas degré des coefficients correspondants à cette intersection s'annulent. Seules les annulations de ce type peuvent apporter un degré de liberté et ce comptage permet de majorer la dimension.

Dans la pratique, il est fréquent que $\delta_0 = 0$ (le coefficient $c_0(z)$ est de valuation nulle) et la discussion sur l'existence se ramène à la considération des coefficients constants.

EXEMPLE 16 : Notons $p_B(n, m)$ le nombre de façons d'écrire un entier naturel n comme somme de m puissances de B, c'est-à-dire le nombre de partitions B-aires de n en m sommants. La série génératrice

$$P_B(u, z) = \sum_{n,m \geq 0} p_B(n, m) z^n u^m$$

vaut

$$P_B(u, z) = \prod_{k \geq 0} \frac{1}{1 - uz^{B^k}}$$

et elle vérifie l'équation

$$(1 - uz) P_B(u, z) = P_B(u, z^B)$$

avec

$$P_B(u, 0) = 1.$$

Sa résolution est immédiate et donne une formule analogue à la formule d'Euler pour les partitions d'entiers usuelles,

$$P_B(u, z) = 1 + \sum_{k \geq 0} \frac{uz^{B^k}}{(1 - uz) \cdots (1 - uz^{B^k})}.$$

Combinatoirement elle exprime la classification des partitions B-aires suivant le plus grand sommant.

EXEMPLE 17 : Un mot à bord sur un alphabet $\mathcal{A}$ est un mot de la forme bwb où $w \in \mathcal{A}^*$ et $b \in \mathcal{A}^+$. M. Régnier a montré dans [61] que la série génératrice $b(z)$ qui énumère les mots à bord sur un alphabet de taille q vérifie l'équation

$$(1-qz)(1-qz^2)b(z) + (1-qz^2)b(z^2) = qz^2.$$

Le système associé a l'allure suivante,

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 \\ -q & 1 & 0 & 0 & 0 & 0 \\ -2\,q & 1-q & 1 & 0 & 0 & 0 \\ q^2 & -q & -q & 1 & 0 & 0 \\ 0 & q^2-q & 1-q & -q & 1 & 0 \\ 0 & 0 & q^2 & -q & -q & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ q \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

et se résout immédiatement pour fournir

$$b(z) = q\,z^2 + q^2\,z^3 + q\left(q-1+q^2\right)\,z^4 + q^2\left(q-1+q^2\right)\,z^5 + q^2\left(q^2-1+q^3\right)\,z^6 + q^3\left(q^2-1+q^3\right)\,z^7 + \cdots .$$

EXEMPLE 18 : Soient u et v deux mots sur $\mathcal{A}$, un alphabet de q lettres. L. Guibas et A. Odlyzko [41] ont défini la corrélation de u sur v (l'opération n'est pas commutative). C'est un mot $\gamma(u,v)$ sur l'alphabet $\{0,1\}$ de même longueur que u et qui est obtenue de la façon suivante : on écrit le mot u et en dessous le mot v ; si u et v coïncident dans la partie où ils se chevauchent, la première lettre de $\gamma(u,v)$ est 1 et sinon 0. Ensuite on décale v d'un cran vers la droite et on compare à nouveau les deux mots dans leur partie commune ; ceci fournit la deuxième lettre de $\gamma(u,v)$. On réitère la procédure jusqu'à la dernière lettre de u. Avec par exemple, $\mathcal{A} = \{a,b\}$, $u = aababba$ et $v = babbaa$, nous obtenons $\gamma(u,v) = 0010010$, comme on le voit ci-dessous :

u	=	a	a	b	a	b	b	a				
v	=	b	a	b	b	a	a					0
			b	a	b	b	a	a				0
				b	a	b	b	a	a			1
					b	a	b	b	a	a		0
						b	a	b	b	a	a	0
							b	a	b	b	a	0
								b	a	b	b	1

Nos deux auteurs étudient plus particulièrement l'autocorrélation (cas où $u = v$) et caractérisent l'ensemble Γ des $\gamma(u,u)$ pour $u \in \mathcal{A}^*$. Ils montrent en particulier que la série génératrice, f_γ, du nombre de mots de longueur n dont l'autocorrélation s'écrit $10\cdots0\gamma$, où γ est un mot donné de longueur c pris dans Γ, vérifie l'équation de Mahler

$$z^c(1-qz)f(z) + [z^c + (1-qz)P_\gamma(z)]f(z^2) = 2k(\gamma)z^{2c}[z^c + (1-qz)P_\gamma(z)],$$

dans laquelle $k(\gamma)$ est le nombre de mots d'autocorrélation γ et

$$P_\gamma(z) = \sum_{0 \le k < c} \gamma_k z^k$$

(les mots sont indexés à partir de 0 et γ_k est la lettre d'indice k de γ). Apparemment, nous devons considérer que pour $n = c$ l'autocorrélation est γ lui-même, c'est-à-dire que la première lettre de γ, qui est un 1, se superpose avec le 1 qui est en tête de $10\cdots0\gamma$.

Pour $\gamma = \varepsilon$, le mot vide, nous avons $P_\varepsilon = 0$ et $k(\varepsilon) = 1$. L'équation vérifiée par f_ε est

$$(1-qz)f(z) + f(z^2) = 2.$$

Nous obtenons

$$f_\varepsilon(z) = 1 + q \sum_{k=0}^{+\infty} \frac{(-1)^k z^{2^k}}{(1-qz)\cdots(1-qz^{2^k})}$$

et

$$f_\varepsilon(z) = 1 + qz + q(q-1)z^2 + q^2(q-1)z^3 + q(q-1)^2(q+1)z^4 + \cdots .$$

De la même façon avec le mot $\gamma = 1$, nous avons $P_1(z) = 1$, $k(1) = q$ et l'équation

$$z(1-qz)f(z) + (1+(q-1)z)f(z^2) = 2q^2z^2(1+(q-1)z).$$

Elle se résout en

$$f_1(z) = qz\left(1 + \sum_{k=0}^{+\infty}(-1)^k \frac{z^{2^k}}{1-qz^{2^k}} \prod_{l=0}^{k-1}\left(1 + \frac{z^{2^l}}{1-qz^{2^l}}\right)\right).$$

Plus généralement, si γ est une autocorrélation de longueur $c \geq 1$, g_γ, définie par

$$f_\gamma(z) = k(\gamma)z^c(1 + zg_\gamma(z)),$$

vérifie l'équation réduite

$$(1-qz)g(z) + z(1-qz+zb_\gamma(z))g(z^2) = b_\gamma(z)$$

en posant

$$b_\gamma(z) = z^{c-1} + (1-qz)\frac{P_\gamma(z)-1}{z}.$$

Remarquons que $b_\gamma(z)$ est un polynôme malgré les apparences. Par itération, nous obtenons l'expression close

$$f_\gamma(z) = k(\gamma)z^c\left(1 + \sum_{k=0}^{+\infty}(-1)^k \frac{z^{2^k}b_\gamma(z^{2^k})}{1-qz^{2^k}} \prod_{l=0}^{k-1}\left(1 + \frac{z^{2^l}b_\gamma(z^{2^l})}{1-qz^{2^l}}\right)\right)$$

c'est-à-dire

$$f_\gamma(z) = k(\gamma)z^c\left(1 + \sum_{k=0}^{+\infty}(-1)^k\left(P_\gamma(z^{2^k}) - 1 + \frac{z^{2^k c}}{1-qz^{2^k}}\right)\prod_{l=0}^{k-1}\left(P_\gamma(z^{2^l}) + \frac{z^{2^l c}}{1-qz^{2^l}}\right)\right).$$

Pour expliciter $f_\gamma(z)$ il reste à déterminer $k(\gamma)$, ce qui se fait récursivement. Par exemple si l'on veut calculer $k(1000010010)$, on considère d'abord

$$f_\varepsilon(z) = 1 + qz + q(q-1)z^2 + q^2(q-1)z^3 + q(q-1)^2(q+1)z^4 + \cdots$$

et le coefficient de z^2 donne $k(10) = q(q-1)$. Ceci permet de calculer

$$f_{10}(z) = q\,(q-1)\,z^2 + q\,(q-1)\,z^4 + q^2\,(q-1)\,z^5 + q\,(q-1)\left(q^2-1\right)z^6 + \cdots$$

et $k(10010) = q^2\,(q-1)$. On en tire ensuite

$$f_{10010}(z) = q^2\,(q-1)\,z^5 + q^2\,(q-1)\,z^8 + q^2\,(q-1)\,z^{10} + q^2\,(q-1)^2\,z^{11} + q^4\,(q-1)\,z^{12} + \cdots$$

et $k(10000010010) = q^2(q-1)^2$ par exemple. Remarquons que les coefficients de z^6 et z^7 dans $f_{10010}(z)$ sont nuls ce qui signifie qu'il n'y pas de mots d'autocorrélation 110010 ou 1010010.

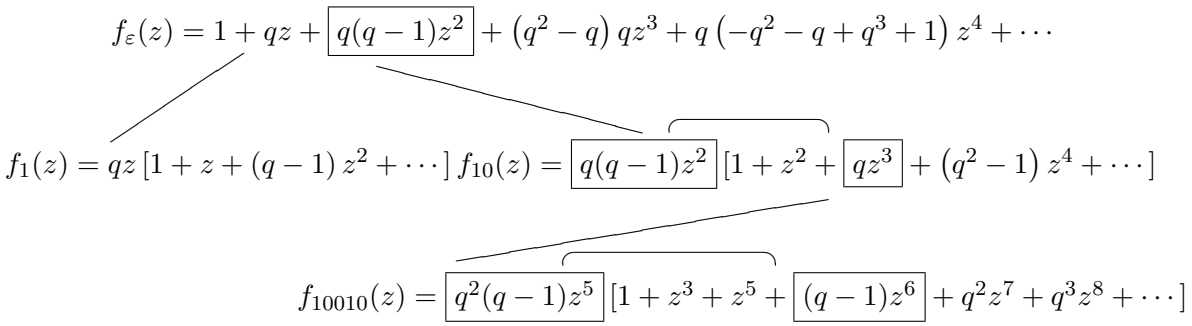

FIG. 3.3
Il y a $q^2(q-1)^2$ mots d'autocorrélation $\gamma = 10000010010$ sur un alphabet de q lettres. Le calcul se fait récursivement et demande autant d'étapes qu'il y a d'occurrences de 1 dans γ, hormis le 1 de tête.

3.3 Aspect qualitatif et analytique

La partie supérieure de la solution d'une équation de Mahler générale

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = b(z)$$

s'obtient par la résolution d'une équation de point fixe

$$C_0(z) + \sum_{k=1}^{N} z^{\lambda_k} C_k(z) \Phi_k(z)^{D-\delta_0+1} F(z^{\omega_k}\Phi_k(z)) = E(z),$$

qui se déduit simplement de la précédente ($\phi_k(z) = z^{\omega_k}\Phi_k(z)$, $\Phi_k(0) = 1$, *etc*). Le calcul de F se fait par itération d'un opérateur qui est lui même une somme de N termes et F s'exprime comme une série indexée par les mots sur l'alphabet constitué des entiers de 1 à N. Posons en effet

$$\begin{aligned} \beta(z) &= \frac{E(z)}{C_0(z)}, \\ \gamma_k(z) &= -\Phi_k(z)^{D-\delta_0+1}\frac{C_k(z)}{C_0(z)}, \end{aligned}$$

ce qui donne

$$F(z) = \beta(z) + \sum_{k=1}^{N} z^{\lambda_k}\gamma_k(z) F\left(z^{\omega_k}\Phi_k(z)\right)$$

Alors

$$F(z) = \sum_{w\in[1,N]^*} a_w(z),$$

où la famille (a_w) est définie par

$$a_\varepsilon(z) = \beta(z)$$

et

$$a_{kw}(z) = z^{\lambda_k}\gamma_k(z) a_w\left(z^{\omega_k}\Phi_k(z)\right) \quad \text{pour } k \in [1,N].$$

Proposition 15. *Si les séries formelles $\Phi_1, \ldots, \Phi_N$ définissent des fonctions analytiques au voisinage de 0, alors il en est de même des solutions formelles d'une équation de Mahler générale.*

DÉMONSTRATION. En effet choisissons un réel $\rho > 0$ tels que les fonctions $\beta, \gamma_1, \ldots, \gamma_N, \Phi_1, \ldots, \Phi_N$ soient analytiques dans le disque $\Delta(0,\rho)$ et majorée en module par une constante A dans ce disque. Il vient

$$|a_{kw}(z)| \leq A|z|\,|a_w(z)|\,,$$

$$|a_w(z)| \leq \rho^\ell A^{\ell+1}$$

et

$$\left|\sum_{|w|=\ell} a_w(z)\right| \leq A(AN\rho)^\ell$$

si $|z| \leq \rho$. Il y a donc convergence normale de la série dans ce disque si $\rho < 1/(AN)$. La fonction F est analytique dans ce disque et il en est donc de même pour f. □

On trouve un résultat similaire dans [47, p. 187] et [48, p. 164]. Les équations de Mahler au sens strict méritent un traitement plus précis.

Théorème 6. *Soit $f(z) = \sum_n f_n z^n \in \mathbb{C}[[z]]$ une série entière solution d'une équation de Mahler*

$$c_0(z)f(z) + c_1(z)f(z^B) + \ldots + c_N(z)f(z^{B^N}) = b(z)$$

dans laquelle $c_0, \ldots, c_N, b$ sont des polynômes et $c_0 \neq 0$.

Si c_0 n'a pas de racines (autres que 0) dans le disque unité, alors $f(z)$ a un rayon de convergence R au moins égal à 1.

Si le plus petit module des racines non nulles de c_0 est $r \in]0,1[$, alors la série entière $f(z)$ a un rayon de convergence $R \geq r$ et la fonction analytique $f(z)$ se prolonge en une fonction $f(z)$ méromorphe dans le disque unité. Cette fonction ne peut avoir comme pôles que les racines B-ièmes itérées, ζ, des racines $\alpha = \zeta^{B^\ell}$ de c_0. De plus l'ordre de ζ comme pôle de f est inférieur à l'ordre de α comme racine de c_0.

DÉMONSTRATION. Nous traitons seulement le cas $0 < r < 1$. Le cas $r \geq 1$ est plus simple et laissé au lecteur. La solution $f(z)$ se décompose en

$$f(z) = \underline{f}(z) + z^{D-\delta_0+1}F(z),$$

avec les notations usuelles, et la partie haute $F(z)$ vérifie

$$C_0(z)F(z) = E(z) + \sum_{k=1}^{N} z^{\lambda_k} C_k(z) F(z^{B^k}).$$

Rappelons que les λ_k sont supérieurs ou égaux à 1 et que les C_k ont une valuation nulle (pour être précis certains peuvent être nuls). En particulier

$$C_0(z) = \gamma \prod_{\alpha \in \mathcal{Z}} (1-\alpha z)^{\nu_\alpha}$$

avec des notations évidentes.

Nous définissons une famille de polynômes (u_w) de valuation nulle et une famille d'entiers (n_w) indexées par les mots sur $[1,N]$ en posant, si $E(z)$ est de valuation β et $E(z) = z^\beta \tilde{E}(z)$,

$$u_\varepsilon(z) = \tilde{E}(z),$$

$$u_{kw}(z) = C_k(z) u_w(z^{B^k}),$$

$$n_\varepsilon = \beta$$

et

$$n_{kw} = \lambda_k + B n_w.$$

Ainsi la série $F(z)$ vaut formellement

$$F(z) = \sum_{w \in [1,N]^*} \frac{z^{n_w} u_w(z)}{\prod_{j=0}^{|w|} C_0(z^{B^j})}.$$

Pour être corrects, il faut ajouter la convention suivante. Si $C_k = 0$, alors $\lambda_k = +\infty$, $u_{kw} = 0$, $n_{kw} = +\infty$ et $z^{+\infty} = 0$.

Passons à l'aspect analytique. Soit A un majorant des polynômes $\tilde{E}$, C_1, ..., C_N sur le disque unité. Pour tout mot w et tout z dans le disque unité, les inégalités suivantes sont satisfaites

$$|u_w(z)| \leq A^{|w|+1}$$

et

$$n_w \geq B^{|w|} - 1.$$

Il en résulte que pour tout entier ℓ et tout z dans le disque unité

$$\left| \sum_{|w|=\ell} z^{n_w} u_w(z) \right| \leq |z|^{B^\ell - 1} A^{\ell+1} N^\ell.$$

D'autre part, si $0 < \rho < r$, $d = \deg C_0$ et $g = |\gamma|$, les inégalités valables pour $|z| \leq \rho$ et w un mot de longueur ℓ

$$|1 - \alpha z| \geq 1 - \rho/r$$

($1/\alpha$ est une racine de C_0),

$$|C_0(z)| \geq g(1 - \rho/r)^d$$

et

$$\left| \prod_{j=0}^{|w|} C_0(z^{B^j}) \right| \geq g^{\ell+1} (1 - \rho/r)^{d(\ell+1)}$$

montrent que

$$\left| \frac{\sum_{|w|=\ell} z^{n_w} u_w(z)}{\prod_{j=0}^{|w|} C_0(z^{B^j})} \right| \leq \rho^{B^\ell - 1} N^\ell \left[\frac{A}{g(1 - \rho/r)} \right]^{\ell+1}.$$

Ainsi il y a convergence normale de cette série dans le disque $\Delta(0, \rho)$ pour $\rho < r$, ce qui permet de définir une fonction analytique dans le disque ouvert $\Delta_o(0, r)$ et la série entière a un rayon de convergence R au moins égal à r d'après les inégalités de Cauchy.

La fonction F se prolonge en une fonction méromorphe dans le disque $\Delta_o(0, r^{1/B})$. En effet son expression se scinde en

$$F(z) = E(z) + \frac{1}{C_0(z)} \sum_{w \in [1,N]^+} \frac{z^{n_w} u_w(z)}{\prod_{j=1}^{|w|} C_0(z^{B^j})}$$

et les majorations précédentes fournissent

$$\left| \frac{\sum_{|w|=\ell} z^{n_w} u_w(z)}{\prod_{j=1}^{|w|} C_0(z^{B^j})} \right| \leq \rho^{B^\ell - 1} \frac{N^\ell (A/g)^{\ell+1}}{(1 - \rho/r^{1/B})^\ell}.$$

L'hypothèse $0 < \rho < r^{1/B}$ permet encore de conclure à la convergence normale et

$$\sum_{w\in[1,N]^+} \frac{z^{n_w} u_w(z)}{\prod_{j=1}^{|w|} C_0(z^{B^j})}$$

définit donc une fonction analytique dans le disque ouvert $\Delta_o(0, r^{1/B})$.

Par récurrence, on obtient le résultat annoncé. □

3.4 Étude dans les séries de Laurent

L'étude de l'équation

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = b(z)$$

dans l'algèbre des séries de Laurent, $\mathbb{K}((z))$, se ramène au problème précédent. L'ensemble $\mathcal{S}_\nu$ des solutions qui sont dans $z^{-\nu}\mathbb{K}[[z]]$ est déterminé par l'équation $(\mathcal{E}_\nu)$

$$\sum_{k=0}^{N} c_k(z) z^{(\Omega-\omega_k)\nu} \Phi_k(z)^{-\nu} g(\phi_k(z)) = z^{\Omega\nu} b(z),$$

d'inconnue $g = z^\nu f \in \mathbb{K}[[z]]$, avec

$$\Omega = \max_{k=1,\cdots,N} \omega_k,$$

$$\phi_k(z) = z^{\omega_k}\Phi_k(z) \quad \text{et} \quad \Phi_k(0) \neq 0.$$

D'après l'étude faite dans $\mathbb{K}[[z]]$, chaque $\mathcal{S}_\nu$ est vide ou un sous-espace affine de dimension finie de $\mathbb{K}((z))$ et la suite des $\mathcal{S}_\nu$ est croissante. Il est naturel de se demander si l'espace $\mathcal{S}$ des solutions dans $\mathbb{K}((z))$ est de dimension finie. Pour voir cela de plus près, nous posons

$$c_k(z) = z^{\delta_k}(\gamma_k + \gamma'_k z + \cdots),$$

$$\phi_k(z) = z^{\omega_k}(\lambda_k + \lambda'_k z + \cdots),$$

pour $k = 1, \cdots, N$ (les γ_k et les λ_k sont non nuls, quand ils existent). De plus μ est la plus petite valeur des δ_k pour les k qui réalisent Ω, le maximum des ω_ℓ. En considérant le coefficient de z^μ dans $(\mathcal{E}_\nu)$, nous obtenons l'équation

$$\left[\sum_{k\in X_\mu} \gamma_k \lambda_k^{-\nu}\right] g_0 = 0.$$

si

$$\nu > \max(\frac{\mu}{\Omega}, \frac{\mu-\delta_0}{\Omega-1}).$$

Dans cette écriture X_i est l'ensemble des k de $[1, N]$ tels que $\omega_k = \Omega$ et $\delta_k = i$. Cette équation donne une condition suffisante pour que $\mathcal{S}$ soit de dimension finie : il suffit que

$$\sum_{k\in X_\mu} \gamma_k \lambda_k^{-\nu} \neq 0$$

pour tous les entiers ν sauf un nombre fini.

Proposition 16. *Avec ces notations, si*

$$\sum_{k\in X_\mu} \gamma_k \lambda_k^{-\nu} \neq 0$$

pour tous les entiers $\nu > \nu_0 \geq \max(\frac{\mu}{\Omega}, \frac{\mu-\delta_0}{\Omega-1})$*, l'ensemble des séries de Laurent solutions de*

$$\sum_{k=0}^{N} c_k(z) f(\phi_k(z)) = b(z)$$

est de dimension finie (s'il est non vide) et dans $z^{-\nu_0}\mathbb{K}[[z]]$*.*

Pour les équations de Mahler au sens strict, X_μ est le singleton $\{N\}$ et la condition est facilement vérifiée.

Théorème 7. *L'ensemble des solutions dans* $\mathbb{K}((z))$ *d'une équation de Mahler d'ordre* N *est dans* $z^{-\nu_0}\mathbb{K}[[z]]$ *avec* $\nu_0 = \lceil \max(\delta_N/B^N, (\delta_N - \delta_0)/(B^N - 1)) \rceil$ *et de dimension finie, s'il n'est pas vide.*

Exemple 19 : La condition utilisée dans la proposition 16 est seulement suffisante et certainement pas nécessaire. Pour l'équation

$$f(z) + f(z^2) + f(-z^2) = 0,$$

l'équation transformée par

$$f(z) = z^{-\nu} g(z)$$

est

$$z^\nu g(z) + g(z^2) + (-1)^\nu g(-z^2) = 0.$$

Ici $\mu = 0$ et en regardant les termes constants, nous voyons que g_0 ne peut être différent de 0 que si

$$1 + (-1)^\nu = 0,$$

c'est-à-dire si ν est impair. Cela se produit bien pour une infinité d'entiers, mais en regardant le coefficient de z^ν avec ν impair, nous trouvons $g_0 = 0$. Ainsi toutes les solutions sont des séries formelles et donc la série nulle.

La condition obtenue peut être raffinée en considérant le coefficient de $z^{\mu+1}$; nous trouvons, si $\nu > \max(\frac{\mu+1}{\Omega}, \frac{\mu+1-\delta_0}{\Omega-1})$, l'équation

$$\left[\sum_{k\in X_\mu} \left(\gamma_k' - \nu\gamma_k \frac{\lambda_k'}{\lambda_k} \right) \lambda_k^{-\nu} + \sum_{k\in X_{\mu+1}} \gamma_k \lambda_k^{-\nu} \right] g_0 = 0.$$

Cela fournit des contraintes qui sont respectées dans l'exemple précédent.

3.5 Solutions rationnelles

Nous avons vu comme obtenir avec une précision donnée les solutions formelles d'une équation de Mahler, mais il est bien plus tentant de déterminer des solutions sous forme close. Par exemple, nous aimerions pouvoir reconnaître que l'équation

$$zf(z) - (1+z)f(z^2) + (1-z^4)f(z^4) = 0$$

Algorithme `solution_rationnelle`

Entrée : une équation de Mahler $c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z)$ dans laquelle $c_0, \ldots, c_N$ et b sont des polynômes ;

Sortie : les solutions rationnelles de l'équation ou échec ;

1. appeler s_0 l'ordre de 0 comme racine de c_N et r_0 la partie entière de $s_0/[B^{N-1}(B-1)]$;
2. déterminer les racines ζ de c_N, qui sont à une distance au moins égale à N d'un B-cycle et poser $\alpha = \zeta^{B^N}$;
3. pour chacun des α précédents, appeler r_α le minimum des ordres de multiplicité (comme racine de c_N) des ζ qui ont fourni ce α ;
4. transformer l'équation en posant $f(z) = \dfrac{p(z)}{z^{r_0}\prod_\alpha (z-\alpha)^{r_\alpha}}$;
5. si $C_0(z)p(z) + C_1(z)p(z^B) + \ldots + C_N(z)p(z^{B^N}) = E(z)$ est l'équation transformée (dans laquelle $C_0, \ldots, C_N$ et E sont des polynômes), poser $n_k = \deg C_k$ pour $k = 0, \ldots, N$ et $n = \deg E$, puis appeler μ le maximum des n_k et de n et enfin r la partie entière de $[\mu - n_N]/[B^{N-1}(B-1)]$;
6. poser $p(z) = \sum_{\ell=0}^{r} p_\ell z^\ell$ et reporter dans l'équation transformée, ce qui fournit un système linéaire en les p_ℓ ;
7. si ce système admet pour solution $(p_0, \ldots, p_r)$, renvoyer $f(z) = \dfrac{p(z)}{z^{r_0}\prod_\alpha (z-\alpha)^{r_\alpha}}$, sinon renvoyer échec ;

fin.

FIG. 3.4
L'algorithme `solution_rationnelle` détermine les éventuelles solutions rationnelles d'une équation de Mahler.

admet pour solutions la fraction rationnelle $\dfrac{1}{1-z} = \prod_{k\geq 0}\left(1 + z^{2^k}\right)$ ainsi que la fonction de Thue-Morse $\mu(z) = \prod_{k\geq 0}\left(1 - z^{2^k}\right)$.

Une équation de Mahler,

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z),$$

ne peut avoir de solutions rationnelles que si $b(z)$ est une fraction rationnelle et en multipliant par un dénominateur commun aux c_k et b, on peut supposer que b est un polynôme.

La discussion va porter sur les pôles d'une solution rationnelle f et nous supposons donc que le corps de référence est algébriquement clos et de caractéristique nulle ou première avec B. Plus généralement on peut utiliser les facteurs irréductibles du dénominateur d'une solution.

Si 0 est pôle d'ordre r de f, il est pôle d'ordre au plus rB^{N-1} de

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_{N-1}f(z^{B^{N-1}}) - b(z).$$

Par ailleurs, si c_N admet 0 comme racine d'ordre $s \geq 0$, alors 0 est pôle d'ordre $rB^N - s$ de $c_N(z)f(z^{B^N})$. Cette remarque fournit l'inégalité

$$rB^{N-1}(B-1) \leq s.$$

Cherchons maintenant les pôles non nuls. Si f admet $\alpha \neq 0$ comme pôle, alors $f(z^B)$ admet comme pôles les racines B-ièmes de α, dont nous notons l'ensemble $\alpha^{1/B}$ par commodité. Parmi ces racines B-ièmes, il y en a au moins $B-1$ qui n'appartiennent pas à un cycle (cf. page 12) et qui sont donc à une distance au moins égale à 1 d'un cycle. De la même façon $f(z^{B^2})$ admet comme pôles les éléments de α^{1/B^2} et parmi ceux-ci il y en a au moins $B(B-1)$ qui sont à une distance au moins égale à 2 d'un cycle. En continuant ainsi nous voyons que $f(z^{B^N})$ admet comme pôles les éléments de α^{1/B^N}, qui comporte entre autres $B^{N-1}(B-1)$ éléments à une distance au moins égale à N d'un cycle. Ces $B^{N-1}(B-1)$ nombres ne sont pas pôles de

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_{N-1}f(z^{B^{N-1}}) - b(z),$$

ce qui signifie qu'ils figurent parmi les zéros de c_N. Plus précisément si α est pôle d'ordre r de f, ces éléments sont des zéros d'ordre au moins r de c_N. Autrement dit, nous considérons les zéros, ζ, de c_N qui sont à une distance au moins égale à N d'un cycle puis les ζ^{B^N} ; ce sont les éventuels pôles α non nuls de f et l'ordre de α est inférieur à tous les ordres (comme racine de c_N) des ζ qui fournissent α. De plus α ne peut être pôle que si toutes les $B^{N-1}(B-1)$ racines B^N-ièmes dont nous parlions plus haut sont racines de c_N.

Ayant trouvé les pôles possibles de f ainsi qu'un majorant de leur ordre de multiplicité et donc un dénominateur possible q, il reste à déterminer un numérateur $p = qf$. Nous substituons cette écriture dans l'équation, ce qui donne une équation pour p. Il faut chercher les solutions polynomiales d'une équation de Mahler à second membre polynôme. Pour cela le changement de z en $1/z$, possible parce que les deux substitutions par z^B et $1/z$ commutent, conduit à chercher une solution rationnelle n'ayant que 0 pour pôle. Ce qui précède permet de majorer l'ordre de ce pôle c'est-à-dire le degré de p. Finalement le problème se ramène à la résolution d'un système linéaire fini.

Récapitulons ce que nous avons obtenu en un algorithme (cf. figure 3.4). Il faut remarquer que le point 2. est assez coûteux, puisqu'il suppose de vérifier que les ζ, ζ^B, …, $\zeta^{B^{N-1}}$ ne sont pas dans un cycle et ceci se voit par des calculs de pgcd où interviennent des polynômes cyclotomiques. .

Proposition 17. *L'algorithme* `solution_rationnelle` *fournit les éventuelles solutions rationnelles d'une équation de Mahler linéaire sur un corps algébriquement clos de caractéristique nulle ou première avec B.*

EXEMPLE 20 : Soit $\mathcal{A}$ un alphabet de m lettres. Un palindrome est un mot sur $\mathcal{A}$ de longueur au moins 2 et égal à son miroir (comme ESOPERESTEETSEREPOSE ou AMANAPLANACANALPANAMA) et un palindrome sans préfixe est un palindrome qui n'admet pas de palindrome comme préfixe strict. En prenant $\mathcal{A} = \{a, b, c\}$ et à permutation près des trois lettres, les palindromes sans préfixe sont *aa*, *aba*, *abba*, *abbba*, *abcba*, ….

Notons $\pi_{m,n}$ le nombre de palindromes sans préfixe sur un alphabet de m lettres et de longueur n et

$$P_m(z) = \sum_{n \geq 2} \pi_{m,n} z^n$$

la série génératrice associée. Il est évident que $P_1(z) = z^2$ et il est bien connu que $\pi_{2,n} = 2$ pour $n \geq 2$, car les palindromes sans préfixe sont de la forme $ab \cdots ba$ si l'alphabet a deux lettres ; ainsi

$$P_2(z) = \frac{2z^2}{1-z}.$$

D'autre part [9], P_m vérifie l'équation de Mahler

$$z(1-mz^2)P_m(z)+(1+z)P_m(z^2)=mz^3(1+mz).$$

La résolution par itération fournit

$$P_m(z)=m\sum_{k\geq 0}(-1)^k z^{2^k+1}\frac{1-z^{2^k}}{1-z}\frac{1+mz^{2^k}}{(1-mz^2)(1-mz^4)\cdots(1-mz^{2^{k+1}})}$$

et en particulier pour $m=1$ et $m=2$ (en simplifiant respectivement par z^2 et $2z^2$) les jolies formules

$$1=\sum_{k\geq 0}(-1)^k z^{2^k+1}\frac{1-z^{2^k}}{1-z}\frac{1+z^{2^k}}{(1-z^2)(1-z^4)\cdots(1-z^{2^{k+1}})},$$

$$\frac{1}{1-z}=\sum_{k\geq 0}(-1)^k z^{2^k-1}\frac{1-z^{2^k}}{1-z}\frac{1+2z^{2^k}}{(1-2z^2)(1-2z^4)\cdots(1-2z^{2^{k+1}})}.$$

Il est naturel de se demander si les $P_m(z)$ avec $m\geq 3$ sont rationnelles. D'après notre étude les éventuels pôles de P_m sont les carrés des racines de $1+z$, le coefficient de $P_m(z^2)$, autrement dit 1. Nous transformons donc l'équation fonctionnelle

$$z(1-mz^2)f(z)+(1+z)f(z^2)=mz^3(1+mz)$$

en posant $f(z)=\dfrac{p(z)}{1-z}$, ce qui donne

$$z(1-mz^2)p(z)+p(z^2)=mz^3(1+mz)(1-z).$$

Ensuite nous changeons z en $1/z$ et $\tilde{p}(z)=p(1/z)$ doit satisfaire l'équation

$$z^2(z^2-m)\tilde{p}(z)+z^5\tilde{p}(z^2)=m(z+m)(z-1).$$

Nous constatons que $\tilde{p}$ admet 0 comme pôle d'ordre au plus 3, c'est-à-dire que p est un polynôme de degré au plus 3. Posant $p(z)=p_3z^3+p_2z^2+p_1z+p_0$, nous obtenons le système

$$\left\{\begin{array}{rcl} p_0 &=& 0\\ p_0 &=& 0\\ 2p_1 &=& 0\\ p_2-mp_0 &=& m\\ p_2+p_3-mp_1 &=& -m+m^2\\ -mp_2 &=& -m^2\\ -mp_3+p_3 &=& 0\end{array}\right.$$

qui se récrit

$$\left\{\begin{array}{rcl} p_0 &=& 0\\ p_1 &=& 0\\ p_2 &=& m\\ p_3 &=& m(m-2)\\ (m-1)p_3 &=& 0.\end{array}\right.$$

Ce système n'a de solutions que pour $m=0$, 1 ou 2. Pour $m=0$, nous obtenons la solution nulle ; pour $m=1$, nous trouvons $p(z)=z^2-z^3$ et $f(z)=P_1(z)$; pour $m=2$, nous avons $p(z)=2z^2$ et $f(z)=P_2(z)$. Ainsi $P_m(z)$ n'est pas rationnelle pour $m\geq 3$.

Cette technique peut être intéressante même s'il n'y a pas de solution rationnelle.

EXEMPLE 21 : R. Graham, D. Knuth et O. Patashnik [38, p. 79] proposent la relation de récurrence, liée au coût du tri par fusion dans le cas le pire :

$$\begin{aligned} f_1 &= 0, \\ f_n &= f_{\lceil n/2 \rceil} + f_{\lfloor n/2 \rfloor} + n - 1 \quad \text{pour } n > 1. \end{aligned}$$

La série génératrice associée à cette suite vérifie

$$z(1-z)^2 f(z) - (1-z^2)^2 f(z^2) = z^3$$

et un éventuel pôle de f est 1 avec l'ordre 2. Posant $f(z) = \dfrac{g(z)}{(1-z)^2}$, nous obtenons l'équation

$$zg(z) - g(z^2) = z^3,$$

qui n'admet pas de solution polynomiale, mais se résout en

$$g(z) = \lambda z + \sum_{k \geq 0} z^{2^k+1}.$$

L'examen des premières valeurs donne $\lambda = 0$ et donc

$$f(z) = \frac{z}{(1-z)^2} \sum_{k \geq 0} z^{2^k}.$$

Il en résulte que (f_n) s'obtient en sommant deux fois la suite qui vaut 1 sur les nombres $2^k + 1$ et 0 sur les autres. Ainsi [38, p. 496]

$$f_n = \sum_{k=1}^{n} \lceil \lg k \rceil = n \lceil \lg n \rceil - \mathrm{ceil}_2(n) + 1,$$

en notant $\mathrm{ceil}_2(n)$ la puissance de 2 immédiatement supérieure à n, c'est-à-dire $2^{\lceil \lg n \rceil}$.

3.6 Solutions produits

À côté des solutions rationnelles, il est naturel de chercher des solutions closes sous forme d'un produit infini

$$\prod_{k \geq 0} R(z^{B^k}),$$

où $R(z)$ est une fraction rationnelle. Une fois de plus la méthode consiste à raisonner sur les facteurs irréductibles des fractions et nous prenons comme corps de référence le corps des nombres rationnels. On peut aussi utiliser un corps algébriquement clos. Le point important est de savoir quels sont les polynômes irréductibles $\phi(z)$ qui divisent leur transformé $\phi(z^B)$.

3.6.1 Produit sous forme normale

Comme le lecteur l'a déjà compris, notre cheval de Troie consiste à compter les multiplicités des zéros et des pôles des fractions rationnelles rencontrées, ou plus généralement les multiplicités des facteurs irréductibles. Pour que ceci soit possible, il est nécessaire de standardiser l'écriture d'un produit de fractions rationnelles.

Algorithme `forme_quasi_normale`

Entrée : deux fractions rationnelles $r(z)$ et $R(z)$ ($R(0) = 1$) et un entier $B \geq 2$;

Sortie : une écriture quasi_normale $s(z)\prod_{k\geq 0} S(z^{B^k})$ de $r(z)\prod_{k\geq 0} R(z^{B^k})$;

1. décomposer en facteurs irréductibles $r(z)$ et $R(z)$;
2. extraire les polynômes cyclotomiques $\Phi_a(z)$ où a est premier avec B ;
3. simplifier respectivement $r(z)$ et $R(z)$ par les puissances convenables $s(z)$ et $S(z)$ de $\Phi_a(z)$ et $\prod_{k\geq 0} \Phi_a(z^{B^k})$;
4. tant que $r(z)$ et $R(z)$ ne sont pas égaux à 1, faire
   (a) si un facteur $\phi(z)$ de $r(z)$ est un descendant d'un facteur $\Phi(z)$ de $R(z)$, intégrer à $s(z)$ ce facteur et ses ancêtres dans la lignée entre $\phi(z)$ et $\Phi(z)$ et augmenter $S(z)$ des fils de $\Phi(z)$ autre que celui qui est ancêtre de $\phi(z)$; simplifier $r(z)$ et $R(z)$ de tous les facteurs transférés dans $s(z)$ et $S(z)$;
   (b) si un facteur $\Psi(z)$ de $R(z)$ est un descendant d'un facteur $\Phi(z)$ de $R(z)$, placer les ancêtres de $\Psi(z)$ dans $s(z)$ et les fils de ceux-ci dans $S(z)$; simplifier $r(z)$ et $R(z)$ de tous les facteurs transférés dans $s(z)$ et $S(z)$;
5. renvoyer l'écriture $s(z)\prod_{k\geq 0} S(z^{B^k})$;

fin.

FIG. 3.5
L'algorithme `forme_quasi_normale` permet de gérer les facteurs irréductibles d'un produit infini mahlérien.

EXEMPLE 22 : La fraction

$$R(z) = \frac{1-9z}{1-3z}$$

fournit le produit infini

$$\prod_{k\geq 0} R(z^{2^k}) = \frac{1-9z}{1-3z}\frac{1-9z^2}{1-3z^2}\frac{1-9z^4}{1-3z^4}\cdots,$$

qui se récrit

$$(1-9z)\prod_{k\geq 0}\left(1+3z^{2^k}\right)$$

à cause de la factorisation $1-9z^2 = (1-3z)(1+3z)$.

Cet exemple montre qu'il ne suffit pas de considérer des produits $\prod_{k\geq 0} R(z^{B^k})$ et il est de plus naturel d'introduire d'emblée des $s(z)\prod_{k\geq 0} S(z^{B^k})$ avec $s(z)$ et $S(z)$ rationnelles.

Définition 19. *Soient $s(z)$ et $S(z)$ deux fractions rationnelles, dont la seconde vérifie $S(0) = 1$. Le produit $s(z)\prod_{k\geq 0} S(z^{B^k})$ est sous forme quasi-normale si les fractions $s(z)$, $S(z)$, $S(z^B)$, ... n'ont pas de facteurs communs deux à deux.*

Le comportement vis-à-vis de l'application $z \mapsto z^B$ fait distinguer deux types de facteurs irréductibles dans $\mathbb{Q}[z]$: les polynômes cyclotomiques $\Phi_a(z)$ où a est premier avec B et les autres polynômes irréductibles.

Pour les premiers, ils ne peuvent figurer dans un $R(z^{B^k})$, avec $k \geq 1$, que dans le cas où ils sont présents dans $R(z)$. Ils génèrent alors différents facteurs dans les $R(z^{B^k})$, facile à expliciter (cf. page 14). Nous mettons à part tous ces facteurs cyclotomiques et nous ne travaillons plus qu'avec les autres. Pour ceux-ci, l'idée est de décaler les facteurs dans les produits, de façon à ce qu'un facteur irréductible apparaisse dans exactement un $R(z^{B^k})$.

Exemple 23 : Comme
$$1 + 4z^4 = (1 + 2z + 2z^2)(1 - 2z + 2z^2),$$
le produit
$$\left[(1+4z)(1+2z+2z^2)\right]\left[(1+4z^2)(1+2z^2+2z^4)\right]\left[(1+4z^4)(1+2z^4+2z^8)\right]\left[(1+4z^8)(1+2z^8+2z^{16})\right]\ldots$$
se récrit
$$\left\{(1+4z)(1+4z^2)\right\}\times$$
$$\left\{\left[(1+2z+2z^2)^2(1-2z+2z^2)\right]\left[(1+2z^2+2z^4)^2(1-2z^2+2z^4)\right]\left[(1+2z^4+2z^8)^2(1-2z^4+2z^8)\right]\ldots\right\}.$$

Il faut aussi tenir compte des facteurs de la fraction rationnelle $r(z)$ et si un même facteur apparaît dans $r(z)$ et dans un $R(z^{B^k})$, nous modifions $r(z)$ et $R(z)$ pour que ce facteur ne figure plus que dans $r(z)$.

Exemple 24 : Nous changeons
$$\{1+2z\}\left\{[1+8z]\left[1+8z^3\right]\left[1+8z^9\right]\ldots\right\}$$
en
$$\left\{(1+2z)^2(1+8z)\right\}\left\{\left[(1+2z^3)(1-2z+4z^2)\right]\left[(1+2z^9)(1-2z^3+4z^6)\right]\ldots\right\}$$
parce que
$$1 + 8z^3 = (1 + 2z)(1 - 2z + 4z^2).$$
Ainsi $1 + 2z$ n'apparaît que dans $r(z)$.

Les conditions que nous venons d'indiquer n'assurent pas l'unicité de l'écriture car il est toujours possible de rejeter plus de facteurs de $R(z)$ vers $r(z)$.

Exemple 25 : L'égalité
$$\Phi_6(z^2) = \Phi_{12}(z)\Phi_{36}(z)$$
permet de donner deux formes quasi-normales pour le produit
$$\prod_{k\geq 0}\Phi_6(z^{2^k}) = \Phi_6(z)\prod_{k\geq 0}\Phi_{12}(z^{2^k})\Phi_{36}(z^{2^k}).$$

Nous aboutissons à l'algorithme `forme_quasi_normale` (cf. figure 3.5), dans lequel, rappelons le, les fils d'un facteur irréductible $\phi(z)$ sont les facteurs irréductibles de $\phi(z^B)$ et plus généralement les descendants de $\phi(z)$ sont les fils et les descendants des fils de $\phi(z)$.

Proposition 18. *L'algorithme* `forme_quasi_normale` *fournit une expression* $s(z)\prod_{k\geq 0} S(z^{B^k})$ *dans laquelle tous les termes du produit,* $s(z)$, $S(z)$, $S(z^B)$, ..., *n'ont aucun facteur commun deux à deux, c'est-à-dire un produit sous forme quasi-normale.*

3.6.2 Solution sous forme de produit

Revenons à la recherche des produits infinis $\prod_{k\geq 0} R(z^{B^k})$ solutions d'une équation de Mahler

$$c_0(z)f(z) + \cdots + c_N(z)f(z^{B^N}) = 0.$$

Bien entendu R est une fraction rationnelle de $\mathbb{Q}(z)$ vérifiant $R(0) = 1$ et N est strictement plus grand que 1. Nous pouvons supposer que le produit a été mis sous la forme normale $s(z)\prod_{k\geq 0} S(z^{B^k})$, ce qui signifie que les fractions $s(z)$, $S(z)$, $S(z^B)$, *etc* n'ont pas de facteurs communs deux à deux. Cependant nous allons faire l'hypothèse supplémentaire que $s = 1$ parce que le cas où $s(z^B)$ et $S(z)$ ont des facteurs communs pose problème.

L'équation obtenue en remplaçant $f(z)$ par $\prod_{k\geq 0} S(z^{B^k})$,

$$c_0(z)S(z)S(z^B)\dots S(z^{B^{N-1}}) + c_1(z)S(z^B)\dots S(z^{B^{N-1}}) + \dots + c_{N-1}(z)S(z^{B^{N-1}}) + c_N(z) = 0,$$

montre que les zéros de $S(z^{B^{N-1}})$ sont des zéros de $c_N(z)$, autrement dit les facteurs irréductibles de $S(z^{B^{N-1}})$ affectés d'un exposant (strictement) positif apparaissent dans $c_N(z)$ avec un exposant positif ou nul. Nous cherchons donc les facteurs irréductibles de $c_N(z)$; nous conservons ceux qui ont un exposant positif puis nous remontons jusqu'à l'ancêtre de rang $N-1$ de ceux-ci. Si dans cette recherche nous butons à un rang strictement plus petit que $N-1$ sur un polynôme cyclotomique Φ_a, où a est premier avec B, nous abandonnons ce facteur. Nous retenons tous les ancêtres obtenus et nous leur affectons la plus petite des multiplicités des descendants qui les ont fait trouver. Les facteurs irréductibles de $S(z)$ affectés d'une multiplicité positive sont à prendre parmi ceux-ci avec une multiplicité inférieure à celle que nous venons de leur affecter.

Nous avons ainsi les numérateurs possibles de $S(z)$. Choisissons l'un d'entre eux $n(z)$ et posons $S = n/d$, en supposant n et d premier entre eux. Il reste à déterminer d. Pour cela nous reportons cette écriture dans l'équation précédente, ce qui donne

$$c_0(z)n(z)n(z^B)\cdots n(z^{B^{N-1}}) + c_1(z)d(z)n(z^B)\cdots n(z^{B^{N-1}}) + \cdots + c_N(z)d(z)d(z^B)\cdots d(z^{B^{N-1}}) = 0.$$

D'après cette égalité, $d(z)$ divise $c_0(z)$ parce que d est premier avec n, mais aussi parce que nous sommes partis d'une forme quasi-normale, ce qui fait que d est premier avec $n(z^B)$, …, $n(z^{B^{N-1}})$. Nous extrayons donc les facteurs irréductibles de $c_0(z)$ premiers avec $n(z)$ et nous testons toutes les possibilités. Nous obtenons ainsi tous les produits, sans partie rationnelle $s(z)$, solutions de l'équation (cf. figure 3.6).

Proposition 19. *L'algorithme* `solution_produit` *fournit toutes les solutions produits d'une équation de Mahler homogène*

$$c_0(z)f(z) + \cdots + c_N(z)f(z^{B^N}) = 0,$$

qui admettent une forme quasi-normale $\prod_{k\geq 0} S(z^{B^k})$.

Exemple 26 : Prenons l'équation d'ordre $N = 2$

$$zf(z) - (1+z)f(z^2) + (1-z^4)f(z^4) = 0.$$

Algorithme `solution_produit`

Entrée : une équation de Mahler homogène $c_0(z)f(z) + \cdots + c_N(z)f(z^{B^N}) = 0$;

Sortie : les solutions produits qui admettent une forme quasi-normale $\prod_{k\geq 0} S(z^{B^k})$;

1. appliquer $N-1$ fois graeffe$_B$ à partir de $c_N(z)$, en éliminant les polynômes cyclotomiques $\Phi_a(z)$ rencontrés si a est premier avec B ;
2. affecter les facteurs irréductibles $\phi(z)$ du polynôme obtenu du plus plus exposant positif k tel que $\phi^k(z^{B^{N-1}})$ divise $c_N(z)$;
3. pour chaque diviseur $n(z)$ du produit des $\phi^k(z)$ trouvés en 2.,

   pour chaque diviseur $d(z)$ de $c_0(z)/\mathrm{pgcd}(c_0(z), n(z))$, tester si le produit infini $\prod_{k\geq 0} n(z^{B^k})/d(z^{B^k})$ est solution de l'équation proposée ;
4. renvoyer les éventuelles solutions ;

fin.

FIG. 3.6
L'algorithme `solution_produit` permet de trouver des produits infinis solutions d'une équation de Mahler.

Pour ce qui est du dénomimateur d, il vaut nécessairement 1 car $c_0(z) = z$ ne nous fournit pas de facteur irréductible (nous ne considérons jamais que les facteurs ϕ tels que $\phi(0) = 1$). Pour le numérateur nous regardons les facteurs de $c_2(z) = 1 - z^4$, c'est-à-dire Φ_1, Φ_2 et Φ_4. Nous éliminons Φ_1 qui n'a pas de père. Il nous reste à considérer Φ_1, père de Φ_2, et Φ_2, père de Φ_4, chacun avec la multiplicité 1. Nous avons donc à tester Φ_1, Φ_2 et $\Phi_1\Phi_2$. Seuls Φ_1 et Φ_2 conviennent et ils nous fournissent respectivement la fonction de Thue-Morse

$$\mu(z) = \prod_{k\geq 0} \left(1 - z^{2^k}\right)$$

et

$$\frac{1}{1-z} = \prod_{k\geq 0} \left(1 + z^{2^k}\right).$$

EXEMPLE 27 : Le produit infini $\prod_{k\geq 0}(1 - 3z^{2^k})(1 - 9z^{2^k})$ est solution de l'équation

$$(1+5z)f(z) - (1+3z)(1-10z+45z^2)f(z^2) + 48z^2(1+3z)(1-3z)(1-3z^2)f(z^4) = 0$$

mais sa forme normale est $(1-9z)\prod_{k\geq 0}(1-3z^{2^k})^2(1+3z^{2^k})$ et l'algorithme ne s'applique pas. Essayons cependant. L'équation est d'ordre 2 et les pères des facteurs de $c_2(z) = 48z^2(1+3z)(1-3z)(1-3z^2)$ sont $1-9z$ et $1-3z$. D'autre part $c_0(z) = 1+5z$ nous fournit un facteur possible pour le dénominateur. Nous devons tester comme $S(z)$ les huit fractions

$$\frac{(1-3z)^\alpha(1-9z)^\beta}{(1+5z)^\gamma},$$

où $0 \leq \alpha, \beta, \gamma \leq 1$. Nous obtenons ainsi exactement une solution : celle que nous connaissions. L'algorithme fonctionne donc, bien que ses conditions d'application ne soient pas réunies.

3.6.3 La méthode de réduction de Kuczma

M. Kuczma [47, pp. 259–261] présente une méthode de réduction de l'ordre pour une équation de Mahler

$$c_0(z)f(z) + \ldots + c_N(z)f(z^{B^N}) = b(z)$$

qui revient à factoriser à droite l'opérateur

$$P(z, M) = c_0(z) + c_1(z)M \ldots + c_N(z)M^N$$

par un opérateur du premier ordre $M - \lambda(z)$, c'est-à-dire à trouver $\lambda(z)$ rationnel tel que

$$P(z, M) = Q(z, M)(M - \lambda(z)).$$

L'existence de cette factorisation est équivalente au fait que le produit infini

$$\prod_{k\geq 0} \frac{1}{\lambda(z^{B^k})}$$

annule l'opérateur $P(z, M)$. Puisque nous savons déterminer des solutions produits d'une équation de Mahler qui admettent une forme quasi-normale

$$\prod_{k\geq 0} S(z^{B^k}),$$

nous pouvons appliquer cette méthode et obtenir certaines factorisations.

Proposition 20. *Il existe un algorithme pour déterminer les facteurs (à droite) du premier degré $M - \lambda(z)$ d'un opérateur $P(z, M) \in \mathbf{Q}(z)[M]$, qui ont la propriété que les $\lambda(z^{B^k})$ n'ont pas de facteurs communs deux à deux.*

Exemple 28 : Reprenons, avec $B = 2$, l'opérateur

$$P(z, M) = (1 + 5z) - (1 + 3z)(1 - 10z + 45z^2)M + 48z^2(1 + 3z)(1 - 3z)(1 - 3z^2)M^2.$$

Nous avons vu au paragraphe précédent qu'il s'annulait sur $\prod_{k\geq 0}(1 - 3z^{2^k})(1 - 9z^{2^k})$. Cela signifie que $P(z, M)$ est divisible par $M - \dfrac{1}{(1 - 3z)(1 - 9z)}$.

Précisément nous avons l'égalité

$$P(z, M) = \left[48z^2M - (1 + 5z)\right] \left[(1 - 3z)(1 - 9z)M - 1\right]$$

et, par exemple, la résolution de l'équation

$$(1 + 5z)f(z) - (1 + 3z)(1 - 10z + 45z^2)f(z^2) + 48z^2(1 + 3z)(1 - 3z)(1 - 3z^2)f(z^4) = z^2$$

se scinde en la résolution des deux équations

$$\begin{array}{rcl} -(1 + 5z)g(z) + 48z^2g(z^2) & = & z^2, \\ -f(z) + (1 - 3z)(1 - 9z)f(z^2) & = & g(z). \end{array}$$

3.6.4 Produits évanescents

L'identité d'Euler

$$\frac{1}{1-z} = \prod_{k\geq 0}(1+z^{2^k})$$

montre que le travail de réduction qui nous a amené à la notion de forme quasi-normale n'est pas terminé et nous allons maintenant chercher les fractions rationnelles qui s'écrivent sous la forme d'un produit infini.

Définition 20. *Le produit* $\prod_{k\geq 0} R(z^{B^k})$*, dans lequel* $R(z)$ *est une fraction rationnelle telle que* $R(0) = 1$*, est dit évanescent s'il se réduit à une fraction rationnelle.*

Remarquons tout de suite qu'il existe une infinité de telles formules : il suffit de prendre les polynômes cyclotomiques $\Phi_a(z)$, où a est premier avec B. En effet la factorisation

$$\Phi_a(z^B) = \prod_{d|B} \Phi_{da}(z),$$

fournit

$$\Phi_a(z^B) = \phi(z)\Phi_a(z)$$

si l'on pose

$$\phi(z) = \prod_{d|B, d\neq 1} \Phi_{da}(z)$$

et donc le produit évanescent

$$\Phi_a(z) = \prod_{k\geq 0} \frac{1}{\phi(z^{B^k})}.$$

Exemple 29 : L'égalité

$$\Phi_3(z^2) = \Phi_3(z)\Phi_6(z)$$

donne le produit évanescent

$$\Phi_3(z) = \prod_{k\geq 0} \frac{1}{\Phi_6(z^{2^k})}$$

c'est-à-dire

$$1+z+z^2 = \prod_{k\geq 0} \frac{1}{1-z^{2^k}+z^{2.2^k}}.$$

Avec $a = 5$ et $B = 6$, nous obtenons l'identité

$$1+z+z^2+z^3+z^4 = \prod_{k\geq 0} \frac{1}{\phi(z^{6^k})},$$

si

$$\phi(z) = (1-z+z^2-z^3+z^4)(1-z+z^3-z^4+z^5-z^7+z^8)(1+z-z^3-z^4-z^5+z^7+z^8).$$

Théorème 8. *Il n'y a essentiellement pas d'autres produits évanescents que les*

$$\Phi_a(z) = \prod_{k\geq 0} \frac{1}{\psi_a(z^{B^k})},$$

où a *est premier avec* B *et* $\psi_a = \prod_{d|B, d\neq 1} \Phi_{da}$.

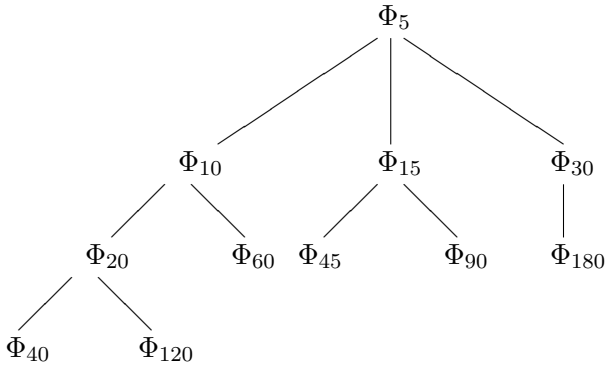

FIG. 3.7
Les relations de parenté, dans le cas où $B = 6$, entre les facteurs de $R = \Phi_{10}\Phi_{15}^2\Phi_{20}^2\Phi_{30}^2\Phi_{45}\Phi_{60}^2$.

DÉMONSTRATION. Si une fraction rationnelle $R(z)$ définit un produit infini $\prod_{k\geq 0} R\left(z^{B^k}\right)$ qui est lui-même une fraction rationnelle $\rho(z)$ alors $R(z) = \rho(z)/\rho(z^B)$ et le problème est donc de caractériser les produits infinis pour lesquels la fraction rationnelle est un quotient $\rho(z)/\rho(z^B)$. Considérons un facteur irréductible $\phi(z)$ de $\rho(z)$ affecté de l'exposant ν.

Si ϕ est un polynôme cyclotomique Φ_a, où a est premier avec B, il apparaît dans $\rho(z)/\rho(z^B)$ un $\left[\Phi_a \prod_{d|B} \Phi_{da}^{-1}\right]^\nu$ c'est-à-dire le produit de tous les fils de Φ_a affectés du même exposant.

Si ϕ n'est pas de ce type, il figure dans $\rho(z)/\rho(z^B)$ un $\phi^\nu \phi_1^{-\nu} \dots \phi_\ell^{-\nu}$, en notant $\phi_1, \dots, \phi_\ell$ les fils de ϕ. Cependant ces ϕ_i sont illusoires et hormis le premier ils se simplifient tous dans le produit infini. D'ailleurs l'application de l'algorithme `forme_quasi_normale` ferait disparaître ce ϕ de $R(z)$ et le ferait apparaître dans la fraction rationnelle qui est en tête de l'écriture quasi-normale. □

L'algorithme `forme_quasi_normale`, appliqué à un produit donne une factorisation dans laquelle il suffit d'identifier les facteurs non cyclotomiques d'une part et de voir si d'autre part les facteurs cyclotomiques se regroupent correctement pour conclure à son évanescence.

EXEMPLE 30 : Il est immédiat que

$$\prod_{k\geq 0} \frac{(1-3\,z^{2^k})(1+3\,z^{4.2^k})}{1-9\,z^{2^k}} = \frac{1}{(1-9z)(1+3z)}.$$

EXEMPLE 31 : Avec $B = 6$ et

$$R = \Phi_{10}\Phi_{15}^2\Phi_{20}^2\Phi_{30}^2\Phi_{45}\Phi_{60}^2\Phi_{90}\Phi_{180},$$

une forme quasi_normale est

$$\Phi_{10}\Phi_{15}^2\Phi_{30}^2 \prod_{k\geq 0} \left[\Phi_{20}\Phi_{60}\Phi_{45}\Phi_{90}\Phi_{180}\right]^3 (z^{6^k}).$$

Comme tous les fils de Φ_{10}, Φ_{15} et Φ_{30} apparaissent élevés au cube, nous remplaçons cette expression par

$$\frac{\Phi_{10}\Phi_{15}^2\Phi_{30}^2}{\Phi_{10}^3\Phi_{15}^3\Phi_{30}^3} \prod_{k\geq 0} \left[\Phi_{10}\Phi_{15}\Phi_{30}\right]^3 \left(z^{6^k}\right).$$

Le terme entre crochets est bien un T convenable, puisqu'il vaut $\Phi_5(z^6)/\Phi_5(z)$ et le produit se réduit à

$$\frac{1}{\Phi_{10}^2\Phi_{15}\Phi_{30}}\,\frac{1}{\Phi_5^3} = \frac{1}{\Phi_5^3\Phi_{10}^2\Phi_{15}\Phi_{30}}.$$

Deuxième partie

Aspect automatique

Les séries B-régulières sont un havre de paix dans la jungle des séries mahlériennes. La donnée de deux matrices carrées A_0 et A_1, d'une matrice ligne λ et d'une matrice colonne γ suffit à déterminer une suite 2-régulière. Si n est un entier naturel de développement binaire $\epsilon_\ell \cdots \epsilon_1 \epsilon_0$, le produit $\lambda A_{\epsilon_\ell} \cdots A_{\epsilon_1} A_{\epsilon_0} \gamma$ est la valeur de la suite pour l'entier n. Cette définition fait tout de suite penser aux séries reconnaissables usuelles en théorie des langages formels. La ressemblance n'est pas fortuite et les séries B-régulières leurs correspondent exactement. La traduction utilise la numération en base B, qui fait passer d'un entier à un mot sur l'alphabet constitué des chiffres 0, 1, ..., $B-1$. Nous disposons ainsi de toutes les techniques liées aux séries rationnelles non commutatives : représentation linéaire, rang, matrice de Hankel, récurrence, *etc.* Qui plus est cette interprétation des séries rationnelles a le mérite d'être fidèle contrairement à l'image commutative qui fait perdre beaucoup d'information. Les séries B-régulières sont omniprésentes non seulement pour tout ce qui touche à la représentation des entiers en base B, mais aussi dans les algorithmes du type *diviser pour régner*. Ce dernier point de vue fournit quantité d'exemples et en montre l'intérêt pratique.

Le premier chapitre de cette partie, le chapitre 4, est voué à la traduction des propriétés des séries rationnelles et fait retrouver les résultats d'Allouche et Shallit [6]. Ces deux auteurs avaient déjà signalé le lien entre séries rationnelles et séries B-régulières, mais notre insistance à le valoriser nous semble présenter sous un jour nouveau les séries B-régulières. Les séries B-régulières forment un ensemble clos par les lois usuelles, satisfont des récurrences simples, que l'on obtient aisément par leur matrice de Hankel, sont facilement calculables par leurs représentations linéaires, bref présentent un agréable formalisme algébrique.

Les deux chapitres suivants, 5 et 6, sont consacrés à la généralisation du théorème de Christol, Kamae, Mendès France et Rauzy. Ces quatre auteurs ont montré [18] que les suites q-automatiques à valeurs dans le corps fini $\mathbb{F}_q$ ont pour séries génératrices les séries formelles algébriques sur le corps des fractions rationnelles, $\mathbb{F}_q(z)$. Les suites B-automatiques ne sont rien d'autre que les suites B-régulières qui ne prennent qu'un nombre fini de valeurs et l'extension est donc naturelle. Cependant l'utilisation des séries algébriques joue sur le fait qu'une série formelle $f(z)$ à coefficients dans $\mathbb{F}_q$ vérifie $f(z^q) = f(z)^q$ et les équations que nous devons considérer dans le cas B-régulier ne sont plus algébriques mais mahlériennes.

Les séries B-régulières à coefficients dans un corps vérifient une équation de Mahler. Ce résultat n'est pas surprenant car la méthode employée pour les séries automatiques s'adapte directement aux séries régulières. Cependant elle est ici effective et fournit souvent l'équation mahlérienne minimale vérifiée par la série. L'introduction d'une classe d'opérateurs rationnels qui sert d'intermédiaire entre les séries rationnelles et les séries régulières permet de donner une seconde démonstration, dans l'esprit des séries rationnelles. L'arithmétique du chapitre 2 montre que ces opérateurs ont une écriture fractionnaire et le dénominateur d'une telle fraction fournit immédiatement une équation de Mahler pour la série régulière associée.

Le dernier chapitre de cette partie, le chapitre 6, donne des conditions suffisantes pour qu'une série mahlérienne soit B-régulière. On rencontre d'abord un cas facile dans lequel la condition essentielle est immédiatement vérifiée. Son importance pratique, en particulier dans l'étude des récurrences *diviser pour régner*, fait que nous l'étendons en une version vectorielle de façon à pouvoir traiter les définitions par cas. L'étude de produits infinis mahlériens fait passer de ce cas simple à un critère général, qui s'adapte à différentes situations. D'abord le théorème de Christol, Kamae, Mendès France et Rauzy se transforme en un énoncé où la caractéristique du corps divise la base de numération mais ne lui est plus nécessairement égale. Ensuite un critère pour les anneaux d'entiers réduits suivant un certain module permet d'atteindre le résultat dont la constatation empirique fut à l'origine de toute cette partie : la suite du nombre de partitions binaires réduite modulo une

puissance de 2 est 2-automatique. Enfin un critère valable dans un corps algébriquement clos permet d'étudier des récurrences *diviser pour régner* ou des suites liées aux problèmes de numération, qui ne ressortissent pas au cas facile, que nous avons d'abord signalé.

Chapitre 4

Séries B-régulières

Les séries B-régulières sont la traduction des séries rationnelles via la numération en base B et ceci est le point de départ de ce chapitre. Les notions classiques sur les séries rationnelles sont ensuite adaptées à cette nouvelle situation. Les représentations linéaires sont ici liées aux opérateurs de section, qui sont les opérateurs fondamentaux. La notion de rang, à travers l'utilisation des matrices de Hankel, permet d'obtenir des représentations minimales et de vérifier de façon automatique l'égalité de deux séries régulières. Les propriétés de clôture, les récurrences ou les propriétés des coefficients, avec la notion de condensée analogue à la densité des langages formels, font cerner la nature des séries B-régulières. Les nombreux exemples et les méthodes de calcul, souvent effectives, éclairent leur champ d'application. Il est clair que l'on peut continuer la traduction mais cela ne présente pas de difficulté et le lecteur n'aura aucun mal à poursuivre de lui-même.

4.1 Définition

La mise en place de la notion de série B-régulière nécessite le rappel de quelques notations classiques en théorie des langages. Les scalaires appartiennent ici à un anneau commutatif $\mathbb{A}$ au lieu d'un demi-anneau, comme on le suppose usuellement. Si $\mathcal{X}$ est un alphabet, c'est-à-dire un ensemble fini, $A\langle\langle\mathcal{X}\rangle\rangle$ (resp. $A\langle\mathcal{X}\rangle$) désigne suivant l'usage l'algèbre des séries formelles (resp. des polynômes) en les indéterminées non commutatives $x \in \mathcal{X}$ à coefficients dans l'anneau commutatif $\mathbb{A}$. Le support d'une série S,

$$S = \sum_{w \in \mathcal{X}^*} (S, w)\, w,$$

est l'ensemble des mots w pour lesquels le coefficient (S, w) est non nul.

L'alphabet utilisé, $\mathcal{X}$, est l'ensemble des chiffres en base B , un entier supérieur ou égal à 2, c'est-à-dire $\{x_0, \cdots, x_{B-1}\}$. En outre $\mathcal{X}_+$ est l'ensemble $\{x_1, \cdots, x_{B-1}\}$ des chiffres non nuls et ε est le mot vide. Il faut préciser que x_r correspond au chiffre r dans l'écriture en base B des entiers. Nous ne différencions ces deux objets que dans un souci de clarté. Si cela ne crée pas d'ambiguïté, on utilisera aussi le chiffre r au lieu de x_r. Comme cette écriture a une grande importance pour la suite, il faut encore introduire quelques définitions.

Définition 21. *Si n est un entier naturel, son écriture en base B est notée $\tilde{n}$, les chiffres de poids faible étant à droite. Au nombre 0 correspond le mot vide ε.*

Si $w \in \mathcal{X}^*$ s'écrit $r_N \cdots r_0$, sa valeur est

$$\bar{w} = r_N B^N + \cdots + r_1 B + r_0.$$

Sa longueur est notée $|w|$.

Définition 22. *Le logarithme de base* B *de l'entier* $n > 0$ *est* $\log_B n$ *et*

$$\lambda_B(n) = \begin{cases} 1 + \lfloor \log_B n \rfloor & \text{si } n > 0 \\ 0 & \text{si } n = 0 \end{cases}$$

représente la longueur de la représentation de n *en base* B. *Si* $B = 2$ *nous utilisons* $\lg = \log_2$.

La longueur du mot $\tilde{n}$ est donc $\lambda_B(n)$, que nous noterons plutôt $\lambda(n)$ si cela ne prête pas à confusion.

Rappelons brièvement la définition des séries rationnelles. Les opérations rationnelles de $A\langle\langle\mathcal{X}\rangle\rangle$ sont les trois lois (addition, produit de Cauchy, produit externe) qui donnent à $A\langle\langle\mathcal{X}\rangle\rangle$ sa stucture de $\mathbb{A}$-algèbre associative unifère, augmentées de l'étoile ou quasi-inverse. Une partie de $A\langle\langle\mathcal{X}\rangle\rangle$ est rationnellement close si elle est close pour les opérations rationnelles, où le rôle de la division est joué par le quasi-inverse. Une intersection de parties rationnellement closes étant rationnellement close, un argument classique de fermeture permet de définir la notion de clôture rationnelle. Pour toutes les propriétés des séries rationnelles nous renvoyons à [13] et [63].

Définition 23. *Les séries rationnelles sont les éléments de la clôture rationnelle de* $A\langle\mathcal{X}\rangle$, *notée* $A^{\mathrm{rat}}\langle\langle\mathcal{X}\rangle\rangle$.

Le passage des entiers à leur écriture en base B s'étend linéairement et fait correspondre les séries B-régulières [6] aux séries rationnelles.

Exemple 32 : La série de Fredholm $\sum_{k\geq 0} z^{2^k}$ correspond ainsi à la série rationnelle $x_1 x_0^* = \sum_{k\geq 0} x_1 x_0^k$, en utilisant la numération binaire.

Définition 24. *Une série formelle* $f(z) = \sum_{n=0}^{+\infty} f_n z^n$ *à coefficients dans* $\mathbb{A}$ *est* B*-régulière si la série à support dans* $\varepsilon + \mathcal{X}_+\mathcal{X}^*$

$$S = \sum_{n=0}^{+\infty} f_n \tilde{n}$$

est rationnelle. Nous dirons aussi que la suite (f_n) *est* B*-régulière. La série rationnelle* S *est alors la série associée à la série* $f(z)$.

Plus rigoureusement il faudrait écrire série $(\mathbb{A}, B)$-régulière car la notion dépend de l'anneau utilisé. Nous ne le ferons que s'il y a un risque de confusion.

Il est clair que le passage de S à $f(z)$ est bijectif.

Proposition 21. *Les séries* B*-régulières forment un* $\mathbb{A}$*-module isomorphe au* $\mathbb{A}$*-module des séries rationnelles à support dans* $\varepsilon + \mathcal{X}_+\mathcal{X}^*$.

4.2 Représentations linéaires

D'après le théorème de Kleene-Schützenberger, une série $S \in A\langle\langle\mathcal{X}\rangle\rangle$ est rationnelle si et seulement si elle est reconnaissable, c'est-à-dire si et seulement s'il existe un entier $N \geq 1$, un morphisme de monoïdes

$$\mu : \mathcal{X}^* \longrightarrow M_N(\mathbb{A})$$

et deux matrices

$$\lambda \in M_{1,N}(\mathbb{A}) \quad \text{et} \quad \gamma \in M_{N,1}(\mathbb{A})$$

telles que pour tout mot $w \in \mathcal{X}^*$

$$(S, w) = \lambda\ \mu(w)\ \gamma.$$

Un tel triplet (λ, μ, γ) est alors une représentation linéaire de S.

La traduction de cette propriété pour les séries B-régulières donne l'énoncé suivant [6].

Théorème 9. *Une série formelle $f(z) \in \mathbb{A}[[z]]$ est B-régulière si et seulement s'il existe un entier $N \geq 1$, B matrices carrées*

$$A_0\,,\ A_1\,,\ \ldots\,,\ A_{B-1} \in M_N(\mathbb{A})$$

et deux matrices

$$\lambda \in M_{1,N}(\mathbb{A}) \quad \textit{et} \quad \gamma \in M_{N,1}(\mathbb{A})$$

telles que pour tout entier n

$$f_n = \lambda A_{\epsilon_\ell} \cdots A_{\epsilon_1} A_{\epsilon_0} \gamma$$

si l'écriture en base B de n vaut

$$\tilde{n} = \epsilon_\ell \cdots \epsilon_1 \epsilon_0.$$

Définition 25. *La donnée de N, A_0, A_1, $\ldots$ A_{B-1}, λ et γ est une représentation linéaire de la série régulière $f(z)$. L'entier N est la dimension de cette représentation.*

Exemple 33 : H.-K. Hwang et J.-M. Steyeart [43] ont rencontré dans l'étude des tas (« heaps ») la suite qui à l'entier n, d'écriture binaire $\tilde{n} = 1\epsilon_\ell \cdots \epsilon_1 \epsilon_0$, associe le nombre $s_n = \overline{1\epsilon_\ell \cdots \epsilon_1 \epsilon_0} + \overline{1\epsilon_\ell \cdots \epsilon_1} + \cdots + \overline{1\epsilon_\ell}$. Par exemple $s_{100} = \overline{1100100} + \overline{110010} + \overline{11001} + \overline{1100} + \overline{110} + \overline{11} = 100 + 50 + 25 + 12 + 6 + 3 = 196$.

Si nous posons

$$A_0 = \begin{pmatrix} 0 & -2 & -2 & -4 \\ 1 & 3 & 2 & 4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 1 & 3 \\ 0 & 0 & -1 & -3 \\ 1 & 0 & -1/2 & -7/2 \\ 0 & 1 & 3/2 & 9/2 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 0 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

nous obtenons

$$A_1\,A_1\,A_0\,A_0\,A_1\,A_0\,A_0 = \begin{pmatrix} 70 & 142 & 143 & 289 \\ -70 & -142 & -143 & -289 \\ -97 & -197 & -395/2 & -797/2 \\ 98 & 198 & 397/2 & 799/2 \end{pmatrix}$$

et

$$\lambda\,A_1\,A_1\,A_0\,A_0\,A_1\,A_0\,A_0\,\gamma = 196$$

ce qui est bien s_{100}. Plus généralement cette suite est 2-régulière et A_0, A_1, λ, γ en est une représentation linéaire de dimension 4.

Rappelons comment apparaissent les représentations linéaires des séries rationnelles [13]. Si u et w sont deux mots sur $\mathcal{X}$, on définit

$$wu^{-1} = \begin{cases} 0 & \text{si } u \text{ n'est pas suffixe de } w \\ v & \text{si } w = vu. \end{cases}$$

Cette définition s'étend aux séries formelles et donne la division à droite par u,

$$Su^{-1} = \sum_{w \in \mathcal{X}^*} (S, wu)\, w,$$

qui est une opération à gauche, linéaire du monoïde $\mathcal{X}^*$ sur le $\mathbb{A}$-module $A\langle\langle \mathcal{X} \rangle\rangle$. On montre alors qu'une série S est rationnelle si et seulement s'il existe un $\mathbb{A}$-module de type fini contenant S et stable par division à droite.

La traduction de cette propriété aux séries régulières est immédiate. En effet à la division par x_r correspond l'application qui aux entiers $Bn + r$ associe n et efface les autres. L'extension aux séries formelles fait apparaître les opérateurs de B-section S_r, tels que

$$S_r f(z) = \sum_{n \geq 0} f_{Bn+r} z^n.$$

Ceux-ci fournissent une action linéaire du monoïde libre $\mathcal{X}^*$ sur $\mathbb{A}[[z]]$. Nous obtenons ainsi une caractérisation des séries B-régulières.

Théorème 10 (Théorème de stabilité)**.** *Une série $f \in \mathbb{A}[[z]]$ est B-régulière si et seulement s'il existe un $\mathbb{A}$-module de type fini contenant $f(z)$ et stable par B-section.*

À dire vrai le passage des opérateurs de division à droite aux opérateurs de section n'est pas tout à fait celui que nous venons d'énoncer. En effet l'opérateur de division à droite par x_0 devrait fournir un opérateur de section S'_0 défini par

$$S'_0 f(z) = \sum_{n \geq 1} f_{Bn} z^n$$

et non

$$S_0 f(z) = \sum_{n \geq 0} f_{Bn} z^n$$

car le mot vide ne se termine pas par x_0. Les deux opérateurs sont donc liés par la relation

$$S_0 = \delta_0 + S'_0$$

en notant δ_0 l'évaluation en 0. Cet à peu près ne change rien qualitativement car entre les deux familles d'opérateurs S_0, S_1, …, S_{B-1} et S'_0, S_1, …, S_{B-1} nous avons les relations

$$S_r \delta_0 = 0 \ \ (r \neq 0), \quad S'_0 \delta_0 = \delta_0 S'_0 = 0,$$

ce qui donne

$$S_0^\ell = \delta_0 + {S'_0}^\ell$$

et donc, pour $r \neq 0$,

$$S_r S_0^\ell = S_r {S'_0}^\ell.$$

Ainsi le fait d'employer S_0 au lieu de S'_0 amène-t-il tout au plus à grossir un peu le module stable utilisé en y incluant les constantes. Bien que le théorème paraisse évident nous allons en donner une démonstration pour bien mettre en valeur le passage des séries rationnelles aux séries régulières. Celle-ci est calquée sur la démonstration que l'on donne pour les séries rationnelles [13, p. 18].

Définition 26. *La notation S_r est étendue en posant $S_w = S_{r_N} \cdots S_{r_0}$ si $w = r_N \cdots r_0 \in \mathcal{X}^*$. Nous dirons encore que les S_w sont des opérateurs de B-section.*

Cette définition est correcte parce que $S_{uv} = S_u S_v$. Passons à la démonstration du théorème.

Démonstration. Nous commençons par le sens facile de l'équivalence.

Soit $f \in \mathbb{A}[[z]]$ une série B-régulière, dont la série rationnelle associée est S. D'après la propriété de stabilité des séries rationnelles, il existe un sous-module $\mathcal{M}$ de type fini dans $A\langle\langle\mathcal{X}\rangle\rangle$ contenant S et stable par les opérations x_r^{-1}. Or, dans le passage des séries à support dans $\varepsilon + \mathcal{X}_+\mathcal{X}^*$ aux séries formelles en z, l'opération de division à droite x_r^{-1} devient la multiplication à gauche par l'opérateur de B-section S_r, à l'exception de x_0^{-1} qui donne $S_0' = S_0 - \delta_0$, et l'ensemble des $S_{r_k} \cdots S_{r_1} f(z)$ est dans le module de type fini $\mathcal{M}' + \mathbb{A}$, où $\mathcal{M}'$ est l'image isomorphe de $\mathcal{M}$. Ainsi l'orbite de f est dans un sous-module de type fini de $\mathbb{A}[[z]]$.

Passons à la réciproque. Soit $\mathcal{F}$ un sous-module de type fini de $\mathbb{A}[[z]]$, stable par l'action de $\mathcal{X}^*$ et contenant une série $f(z)$. Notons $(e_t)_{t\in\mathcal{T}}$ une famille génératrice finie de $\mathcal{F}$,

$$A_r = (\alpha_{r,t,u})_{(t,u)\in\mathcal{T}^2}$$

une matrice de l'opérateur de B-section S_r par rapport à cette famille génératrice, pour $0 \le r < B$.

La série s'exprime comme une combinaison linéaire

$$f(z) = \sum_{t\in\mathcal{T}} e_t(z)\,\gamma_t$$

et nous considérons $(\gamma_t)_{t\in\mathcal{T}}$ comme une matrice colonne. Introduisons les matrices Ξ et Ξ_+ à coefficients dans $A\langle\mathcal{X}\rangle$,

$$\Xi = \sum_{0\le r<B} A_r x_r,$$

$$\Xi_+ = \sum_{0<r<B} A_r x_r$$

et la série

$$S = \sum_{n\ge 0} f_n\,\tilde{n}$$

associée à $f(z)$. La notation étendue S_w pour les composés d'opérateurs de section permet d'écrire, pour $t \in \mathcal{T}$ et $n > 0$,

$$[z^n]e_t = [z^0]S_{\tilde{n}}e_t = S_{\tilde{n}}e_t(0).$$

Si

$$\tilde{n} = r_N \cdots r_0,$$

nous avons

$$S_{\tilde{n}}e_t = \sum_u \sum_{u_0} \cdots \sum_{u_{N-1}} \alpha_{r_N,u,u_{N-1}} \cdots \alpha_{r_1,u_1,u_0}\alpha_{r_0,u_0,t}\,e_u$$

et

$$S_{\tilde{n}}e_t(0)\,\tilde{n} = \sum_u \sum_{u_0} \cdots \sum_{u_{N-1}} \alpha_{r_N,u,u_{N-1}}\,r_N\,\cdots\alpha_{r_1,u_1,u_0}\,r_1\,\alpha_{r_0,u_0,t}\,r_0\,e_u(0)$$

donc

$$[z^n]e_t\,\tilde{n} = \sum_u e_u(0)\left(\Xi_+\Xi^N\right)_{u,t},$$

le Ξ_+ apparaissant parce que le chiffre de poids le plus fort r_N est non nul. Nous avons, en sommant sur n (sans oublier 0),

$$\sum_n [z^n]e_t(z)\,\tilde{n} = \sum_u e_u(0)\,(I + \Xi_+\Xi^*)_{u,t},$$

si I désigne la matrice identique. En appelant λ le vecteur ligne $(e_u(0))_{u\in\mathcal{T}}$, nous concluons que

$$S = \lambda\,(I + \Xi_+\Xi^*)\,\gamma.$$

D'après les propriétés de l'étoile d'une matrice [13, p. 23], la matrice $\Xi_+\Xi^*$ a ses coefficients dans $A^{\mathrm{rat}}\langle\langle\mathcal{X}\rangle\rangle$ et la série S est donc rationnelle. Il en résulte que la série $f(z)$ est B-régulière. □

La démonstration fournit une représentation linéaire de la série S rationnelle associée à la série B-régulière $f(z)$.

Corollaire 9. *Soit $f(z)$ une série régulière et $(e_t)_{t\in\mathcal{T}}$ une famille génératrice finie d'un module stable par section, contenant $f(z)$. Si A_r est une matrice de l'opérateur de section S_r par rapport à cette famille ; si les matrices Ξ et Ξ_+ sont définies par*

$$\Xi = \sum_{0\le r<B} A_r x_r,$$

$$\Xi_+ = \sum_{0<r<B} A_r x_r \ ;$$

si de plus γ est un vecteur colonne de coordonnées de f par rapport à $(e_t)_{t\in\mathcal{T}}$ et λ le vecteur ligne $(e_t(0))_{t\in\mathcal{T}}$, alors $f(z)$ est associée à la série rationnelle

$$S = \lambda\,(I + \Xi_+\Xi^*)\,\gamma.$$

Ce résultat permet de calculer une expression rationnelle de la série rationnelle associée à une série régulière.

Exemple 34 : La série à coefficients dans $\mathbb{Z}$

$$m_B(z) = \sum_{n\ge0} r_B(n) z^n,$$

où $r_B(n)$ est la valeur du miroir de l'écriture B-aire de n, est B-régulière [6]. Les égalités

$$\begin{aligned} r_B(Bn) &= r_B(n) \\ r_B(Bn+r) &= r_B(n) + B^{\lambda_B(n)} r \quad 0<r<B, \end{aligned}$$

amènent à introduire

$$\beta(z) = \sum_{n\ge0} B^{\lambda_B(n)} z^n = 1 + \sum_{k\ge0} z^{B^{k+1}}\,\frac{z^{B^k} - z^{B^{k+1}}}{1-z}.$$

Cette série est B-régulière puisqu'elle correspond à la série rationnelle

$$\varepsilon + B\mathcal{X}_+(B\mathcal{X})^*.$$

D'ailleurs $S_0\beta = 1 - B + B\beta$ et $S_r\beta = B\beta$ pour tout $r \in [0, B[$. En utilisant la base $(m_B, \beta, 1)$ du $\mathbb{Z}$-module engendrée par l'orbite de m_B sous l'action de $\mathcal{X}^*$, et en posant

$$\mathcal{X}' = \sum_{0<r<B} r x_r,$$

les matrices définies dans le corollaire valent

$$\Xi = \begin{pmatrix} \mathcal{X} & 0 & 0 \\ \mathcal{X}' & B\mathcal{X} & 0 \\ 0 & (1-B)\,x_0 & x_0 \end{pmatrix}, \quad \Xi_+ = \begin{pmatrix} \mathcal{X}_+ & 0 & 0 \\ \mathcal{X}' & B\mathcal{X}_+ & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix} \text{ et } \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Tout ceci donne l'expression rationnelle

$$R_B = \mathcal{X}'\mathcal{X}^* + B\mathcal{X}_+(B\mathcal{X})^*\mathcal{X}'\mathcal{X}^*$$

pour la série associée à $m_B(z)$.

EXEMPLE 35 : Imaginons un paquet de cartes numérotées de 1 à n et rangées dans l'ordre. Nous enlevons la première carte, nous mettons la seconde sous le paquet, nous enlevons la troisième, nous mettons la quatrième carte sous le paquet, et ainsi de suite jusqu'à ce qu'il ne reste plus qu'une carte. Le problème de Josephus est la détermination du numéro, j_n, de cette dernière carte. A un petit changement de notation près et avec un point de vue plus historique et macabre, il est présenté par Graham, Knuth et Patashnik dans [38, p. 8].

Il n'est pas difficile de voir que la suite (j_n) satisfait à la récurrence

$$\begin{array}{ll} j_{2n} = 2\,j_n & (n \geq 1), \\ j_{2n-1} = j_{2n} - 2 & (n \geq 2). \end{array}$$

Cette récurrence permet d'obtenir une expression explicite de j_n :

$$j_n = 2n - 2^\nu \quad \text{si} \quad 2^{\nu-1} < n \leq 2^\nu$$

et la série génératrice

$$j(z) = z + 2z^2 + 2z^3 + 4z^4 + 2z^5 + 4z^6 + 6z^7 + 8z^8 + 2z^9 + 4z^{10} + 6z^{11} + 8z^{12} + \cdots .$$

Si nous introduisons les séries

$$\vartheta(z) = \frac{1}{1-z}, \qquad \epsilon(z) = \sum_{\nu \geq 0} 2^{\nu+1} z^{2^\nu},$$

nous obtenons les relations

$$\begin{array}{cccc} S_0 j = 2j, & S_0\vartheta = \vartheta, & S_0\epsilon = 2\epsilon, & S_0 1 = 1, \\ S_1 j = 2j + 2\vartheta - \epsilon - 1, & S_1\vartheta = \vartheta, & S_1\epsilon = 2, & S_1 1 = 0, \end{array}$$

qui montrent que $j(z)$ est $(\mathbb{Z}, 2)$-régulière. Les matrices associées aux opérateurs de section s'écrivent

$$A_0 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 2 & 0 \end{pmatrix}.$$

Nous obtenons successivement

$$\Xi = x_0 A_0 + x_1 A_1 = \begin{pmatrix} 2x_0 + 2x_1 & 0 & 0 & 0 \\ 2x_1 & x_0 + x_1 & 0 & 0 \\ -x_1 & 0 & 2x_0 & 0 \\ -x_1 & 0 & 2x_1 & x_0 \end{pmatrix},$$

$$\Xi_+ = x_1 A_1 = \begin{pmatrix} 2x_1 & 0 & 0 & 0 \\ 2x_1 & x_1 & 0 & 0 \\ -x_1 & 0 & 0 & 0 \\ -x_1 & 0 & 2x_1 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

et une expression rationnelle de la série associée à $j(z)$,

$$J = \lambda(I + \Xi_+\Xi^*)\gamma = (\varepsilon + 2x_1\left[\{x_0 + x_1\}^* - (2x_0)^*\right])\, x_1\, (2\{x_0 + x_1\})^*\,.$$

La série rationnelle associée à $f(z)$ admet l'expression $\lambda(I + \Xi_+\Xi^*)\gamma$ si $\Xi = \sum_r A_r x_r$ et les A_r sont les matrices de la représentation linéaire que nous utilisons. Cette représentation linéaire correspond à la série $\lambda\,\Xi^*\gamma$ et non à la série naturellement associée à $f(z)$, parce que nous utilisons l'opérateur S_0 au lieu de l'opérateur S_0'. En particulier cette série $\lambda\,\Xi^*\gamma$ n'est généralement pas à support dans $\varepsilon + \mathcal{X}_+\mathcal{X}^*$. Ainsi dans la représentation indiquée ci-dessus pour la suite de Josephus, le produit $\lambda A_0 A_1 \gamma$ vaut 1 et non pas 0, comme on pourrait s'y attendre.

Pour définir une série B-régulière, il suffit de se donner arbitrairement des matrices A_0, A_1, …, A_{B-1}, λ et γ, mais les représentations linéaires définies dans le corollaire précédent vérifient une condition de cohérence supplémentaire qui porte sur les matrices A_0 et λ. Ce phénomène provient de la confusion entre l'entier 0, d'écriture le mot vide ε, et le chiffre 0.

Proposition 22. *Soit A_0, A_1, …, A_{B-1}, λ, γ une représentation linéaire d'une série B-régulière obtenue en application du corollaire précédent, alors*

$$\lambda\, A_0 = \lambda\ ;$$

en particulier 1 est valeur propre de A_0 si la série est non nulle.

Inversement la donnée d'une représentation linéaire A_0, A_1, …, A_{B-1}, λ, γ satisfaisant la condition $\lambda\, A_0 = \lambda$ définit une série B-régulière, pour laquelle les A_r s'interprètent comme des matrices des opérateurs de section par rapport à une famille $(e_t(z))_{t\in\mathcal{T}}$ et $\lambda_t = e_t(0)$. Dans cette famille, la série $e_t(z)$ est obtenue en utilisant la représentation A_0, A_1, …, A_{B-1}, λ, $\gamma(t)$ où $\gamma(t)$ est le vecteur d'indice t de la base canonique de $\mathbb{A}^{\mathcal{T}}$.

Démonstration. Introduisons les séries formelles B-régulières de représentation linéaire A_0, A_1, …, A_{B-1}, λ, $\gamma(j)$ pour $j = 1 \ldots N$, où $\gamma(j)$ désigne le j-ième vecteur de la base canonique de $\mathbb{A}^N$. Avec cette notation les λ_j sont définis par $\lambda_j = g_j(0)$ et vérifient

$$\lambda_j = S_0 g_j(0) = \sum_{i=1}^{N} A_0(i,j) g_i(0) = \sum_{i=1}^{N} A_0(i,j)\lambda_i,$$

ce qui s'écrit encore

$$\lambda\, A_0 = \lambda.$$

□

Définition 27. *Une représentation linéaire A_0, A_1, …, A_{B-1}, λ, γ d'une série B-régulière vérifiant $\lambda\, A_0 = \lambda$ est dite standard. Dans la suite, seules des représentations linéaires standard seront utilisées.*

La définition des séries B-régulières introduit une série rationnelle naturellement associée à une série B-régulière $f(z)$, qui est disons $S = \lambda(I + \Xi_+\Xi^*)\gamma$. Celle-ci a la propriété remarquable d'être à support dans $\varepsilon + \mathcal{X}_+\mathcal{X}^*$. L'addition d'une série rationnelle quelconque à support dans $x_0\mathcal{X}^*$ procure une série rationnelle R qui coïncide avec S sur les écritures d'entiers et toute représentation linéaire de R fournit une représentation linéaire de $f(z)$. Utiliser une représentation linéaire standard revient à imposer $R = \lambda\,\Xi^*\gamma$. En particulier le fait de mettre des 0 en tête des écritures en base B ne change pas la valeur associée car $(R, x_0 w) = (R, w)$.

Exemple 36 : Allouche et Shallit [6, p. 192] considèrent la suite 0, 1, 3, 4, 9, 10, 12, 13, 27, 28, 30, 31, 36, ... définie par ses deux premiers termes, le fait qu'elle est strictement croissante et la propriété que trois termes quelconques ne sont pas en progression arithmétique. Elle est 2-régulière et admet la représentation linéaire

$$A_0 = \begin{pmatrix} 9 & 24 \\ -2 & -5 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & -3 \\ 1 & 4 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 1 & 4 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 4/3 \\ -1/3 \end{pmatrix}.$$

Elle admet d'ailleurs aussi la représentation de dimension 3

$$A'_0 = \begin{pmatrix} 4 & 2 & 5 \\ -4 & 1 & 4 \\ 1 & 0 & 0 \end{pmatrix}, \quad A'_1 = \begin{pmatrix} 0 & 0 & -4 \\ 3 & 0 & 13 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\lambda' = \begin{pmatrix} 0 & 1/3 & 4/3 \end{pmatrix}, \quad \gamma' = \begin{pmatrix} 2 \\ -4 \\ 1 \end{pmatrix}.$$

Ces deux représentations sont standard.

Les séries régulières apparaissent souvent dans des problèmes où une structure est brisée en plusieurs morceaux de même taille, souvent en liaison avec l'écriture dans une base de numération. Ceci se traduit généralement par des relations de récurrence qui font intervenir la partie entière et l'on pourrait finir par croire que toute relation de ce type amène une série régulière. Il n'en est rien et nous allons illustrer ceci en considérant le problème de Josephus avec un entier $q \geq 3$, ce qui signifie que l'on sort les cartes de q en q (cf. page 73).

Exemple 37 : Pour étudier la suite de $(J_q(n))$ dans le cas $q \geq 3$, nous utiliserons le petit lemme suivant.

Lemme. *Si (u_n) et (v_n) sont deux suites d'entiers naturels telles que*

$$u_n \underset{n\to+\infty}{\sim} C\rho^n, \quad v_n \underset{n\to+\infty}{\sim} C\rho^n/b,$$

avec C un réel non entier, ρ un rationnel non entier strictement plus grand que 1 et b un entier naturel supérieur ou égal à 2, alors il y a une infinité de termes de (v_n) qui ne sont pas des termes de (u_n).

S'il n'en était pas ainsi, nous aurions pour un certain entier relatif k et pour n assez grand l'égalité $u_n = v_{n+k}$, car les deux suites sont strictement croissantes à partir d'un certain rang. En passant aux équivalents cela donne

$$\rho^k = b$$

ce qui est absurde.

On sait [38, p. 8] que la suite de Josephus d'indice q peut être définie par l'algorithme suivant.

1. Définir la suite (D_k) par

$$D_0 = 1, \quad D_k = \left\lceil \frac{q}{q-1} D_{k-1} \right\rceil.$$

2. Déterminer le premier entier k tel que

$$D_k > (q-1)n.$$

3. Alors

$$J_q(n) = qn + 1 - D_k.$$

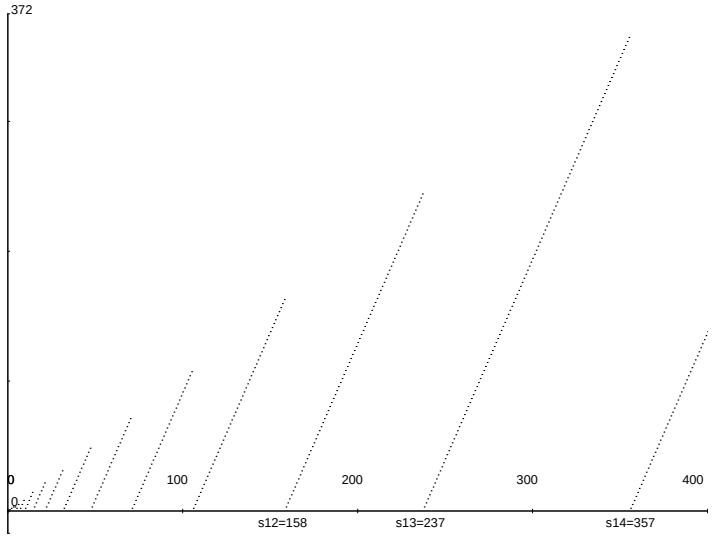

FIG. 4.1
La suite de Josephus d'indice 3 n'est pas B-régulière pour tout entier B. En effet ses points de saut, $s_k \sim 1,622\,(3/2)^k$, ne forment pas un ensemble invariant dans l'homothétie de rapport $1/B$.

Evidemment pour étudier la B-régularité de J_q, il suffit d'étudier celle de la suite constante par intervalles $D(n)$, qui est définie par

$$D(n) = D_k \quad \text{si} \;\; D_{k-1} \leq (q-1)n < D_k.$$

Les intervalles s'écrivent $[s_{k-1}+1, s_k]$ où s_k est la partie entière de $D_k/(q-1)$. Nous dirons que les s_k sont les points de saut. Odlyzko et Wilf [59] ont montré que

$$D_k \underset{k\to+\infty}{\sim} K(q) \left(\frac{q}{q-1}\right)^k$$

où $K(q)$ est un certain réel strictement positif. En particulier $K(3)$ vaut environ $1,622$. Pour voir que la série génératrice $D(z)$ de $(D(n))$ n'est pas B-régulière, il suffit de montrer que ses sections $S^\ell_{B,0}D(z)$ sont linéairement indépendantes. Pour $\ell = 0,\, 1\,\ldots$, la section $S^\ell_{B,0}D(z)$ a des points de saut qui se comportent comme

$$\frac{1}{B^\ell}\frac{K(q)}{q-1}\left(\frac{q}{q-1}\right)^k.$$

Grâce au petit lemme, deux sections ne peuvent avoir qu'un nombre fini de points de saut en commun, ce qui interdit une relation de dépendance linéaire pour cette famille.

4.3 Matrices de Hankel

Une série S est rationnelle si elle appartient à un module de type fini stable sous l'action des opérateurs de division. Ceci équivaut à dire que sa matrice de Hankel H définie par

$$H_{u,v} = (S, uv) \quad (u, v \in \mathcal{X}^*)$$

est de rang fini, c'est-à-dire que la famille des vecteurs colonnes de H est contenue dans un sous-module de type fini de $\mathbb{A}^{\mathcal{X}^*}$ [63, p. 25]. Comme les séries rationnelles qui nous intéressent sont

essentiellement à support dans $\varepsilon + \mathcal{X}_+\mathcal{X}^*$ les lignes dont les indices u ne sont pas dans ce langage sont nulles et ceci conduit à les négliger.

Définition 28. *La B-matrice de Hankel d'une série formelle $f(z)$ est la matrice infinie H de type $\mathbb{N} \times \mathcal{X}^*$ définie par*

$$H_{n,w} = f_{B^k n+r} \quad (n \geq 0,\ w \in \mathcal{X}^*)$$

si w est un mot de longueur k et $B^k n + r$ la valeur du mot $\tilde{n}w$.

Les indices de lignes de cette matrice sont les entiers naturels et les indices de colonnes sont les mots sur $\mathcal{X}$. Pour pouvoir écrire cette matrice, nous ordonnons $\mathcal{X}^*$ suivant la longueur et l'ordre lexicographique pour les mots de même longueur.

Définition 29. *L'ordre strict sur $\mathcal{X}^*$ est défini par $u \prec v$ si et seulement si $|u| < |v|$ ou $|u| = |v|$ et $u \prec_{\text{lex}} v$.*

Voici par exemple, avec $B = 2$, la sous-matrice obtenue en ne retenant que les lignes d'indice entre 0 et 7 et les colonnes d'indice entre ε et x_1x_1, ou ε et 11 si l'on préfère.

$$\begin{pmatrix} f_0 & f_0 & f_1 & f_0 & f_1 & f_2 & f_3 \\ f_1 & f_2 & f_3 & f_4 & f_5 & f_6 & f_7 \\ f_2 & f_4 & f_5 & f_8 & f_9 & f_{10} & f_{11} \\ f_3 & f_6 & f_7 & f_{12} & f_{13} & f_{14} & f_{15} \\ f_4 & f_8 & f_9 & f_{16} & f_{17} & f_{18} & f_{19} \\ f_5 & f_{10} & f_{11} & f_{20} & f_{21} & f_{22} & f_{23} \\ f_6 & f_{12} & f_{13} & f_{24} & f_{25} & f_{26} & f_{27} \\ f_7 & f_{14} & f_{15} & f_{28} & f_{29} & f_{30} & f_{31} \end{pmatrix}$$

Les colonnes de H sont, dans l'ordre, (f_n), (f_{2n}), (f_{2n+1}), (f_{4n}), (f_{4n+1}), (f_{4n+2}), *etc.* On voit évidemment l'opération des entiers qui traduit la concaténation des écritures binaires. L'aspect un peu curieux et bègue de la première ligne vient du choix que nous avons fait pour l'opérateur de section d'indice 0.

Théorème 11. *Une série formelle $f(z)$ est B-régulière si et seulement si sa matrice de Hankel est de rang fini.*

La matrice de Hankel d'une série formelle $f(z)$ n'est pas a priori symétrique comme la matrice de Hankel d'une série $S \in A\langle\langle\mathcal{X}\rangle\rangle$. La finitude du rang étant invariante par transposition, nous retrouvons le fait (bien connu pour les suites automatiques) qu'il est équivalent d'utiliser la lecture directe ou inverse pour étudier les séries régulières. Autrement dit nous pouvons caractériser les séries régulières par la propriété suivante.

Proposition 23. *Une série $f(z)$ est B-régulière si et seulement si elle appartient à un module de type fini stable par les opérateurs*

$$T_{B,k} : g(z) = \sum_{n\geq 1} g_n z^n \longmapsto \sum_{n\geq 1} g_{n+B^{\lambda(n)}k} z^n \quad (k \geq 0).$$

Corollaire 10. *Si la série $f(z)$ est B-régulière, il en est de même des séries $T_{B,k}f(z)$ $(k \geq 0)$.*

Définition 30. *Nous supposons que l'anneau de référence est un corps $\mathbb{K}$ ou un anneau intègre dont le corps des fractions est $\mathbb{K}$. Le rang $\operatorname{rg} f$ d'une série B-régulière $f(z)$ est la dimension du sous-espace vectoriel de $\mathbb{K}(z)$ engendré par les sections de $f(z)$.*

Désormais l'anneau de référence est un corps $\mathbb{K}$. On sait que le rang de la matrice de Hankel d'une série rationnelle est alors la dimension minimale d'une représentation linéaire de la série, appelée aussi rang de la série [13, p. 35].

Proposition 24. *Soit* A_r *(*$0 \le r < B$*),* λ*,* γ *une représentation linéaire standard de* $f(z)$*,* $S = \lambda(I + \Xi_+\Xi^*)\gamma$ *la série rationnelle associée à* $f(z)$ *et* $R = \lambda\,\Xi^*\gamma$*. Alors le rang de* $f(z)$ *est le rang de* S *ou encore le rang de* R*.*

Démonstration. Les trois séries $f(z)$, S et R ont bien même rang, parce qu'on obtient la matrice de Hankel de S en adjoignant à celle de $f(z)$ les lignes nulles indexées par les mots x_0w. Quant à celle de R, on fabrique la ligne d'indice x_0w en recopiant celle d'indice w. □

Proposition 25. *Le rang d'une série formelle régulière* $f(z)$ *est la dimension minimale d'une représentation linéaire standard de la série ou encore le rang de sa matrice de Hankel. Une représentation linéaire standard de dimension le rang de la série est dite réduite.*

Insistons sur le fait qu'il faut se limiter aux représentations standard, faute de quoi on ne contrôle pas les valeurs de la série rationnelle sur les mots qui ne sont pas des écritures d'entiers. En particulier, on peut donner des représentations non standard qui définissent des séries B-régulières dont le rang est supérieur à la dimension de la représentation.

Exemple 38 : Appelons $\epsilon_k(n)$ le chiffre d'indice k de l'écriture en base B de l'entier n. La série génératrice de cette suite est la fraction rationnelle

$$\epsilon_k(z) = \frac{1 - z^{B^k}}{1 - z} \left[\sum_{1 \le r < B} r\, z^{rB^k} \right] \frac{1}{1 - z^{B^{k+1}}}.$$

On voit tout de suite que

$$S_r\epsilon_k(z) = \epsilon_{k-1}(z)$$

si $k \ge 1$ et $0 \le r < B$. D'autre part

$$S_r\epsilon_0(z) = \frac{r}{1 - z}$$

pour $0 \le r < B$. Le $\mathbb{Z}$-module stable par section engendré par $\epsilon_k(z)$ admet donc pour base $\epsilon_k(z)$, $\epsilon_{k-1}(z)$, $\ldots$, $\epsilon_0(z)$ et $1/(1 - z)$. Ainsi $\epsilon_k(z)$ est de rang $k + 2$.

Exemple 39 : Les séries 2-régulières $f(z)$ de rang 1 sont définies par la donnée de trois nombres $f_0 \neq 0$, a_0 et a_1 et ont pour expression

$$f(z) = f_0 \sum_{n=0}^{+\infty} a_0^{|\tilde{n}|_0} a_1^{|\tilde{n}|_1} z^n = f_0 \left[1 + a_1 z + a_0 a_1 z^2 + a_1^2 z^3 + a_0^2 a_1 z^4 + a_0 a_1^2 z^5 + \cdots\right].$$

Un exemple typique de série de rang 1 est la série de Thue-Morse ($f_0 = 1$, $a_0 = 1$, $a_1 = -1$).

Exemple 40 : Toute suite périodique (a_k) de période T définit une série 2-régulière de rang au plus T par le produit infini

$$f(z) = \prod_{k \ge 0} \left(1 + a_k z^{2^k}\right).$$

En effet tous les $S_{\epsilon_\ell} S_{\epsilon_{\ell-1}} \cdots S_{\epsilon_1} f(z)$ sont proportionnels à $(1+a_r z) \cdots (1+a_{T-1} z^{2^{T-r-1}}) f(z^{2^{T-r}})$ si $0 \le r < T$ et $\ell \equiv r \bmod T$.

EXEMPLE 41 : La matrice de Hankel d'une série de la forme

$$f(z) = \prod_{k\geq 0} \left(1 + a_k z^{2^k}\right)$$

a l'allure suivante

$$\begin{pmatrix}
1 & 1 & a_0 & 1 & a_0 & a_1 & a_0a_1 & 1 & a_0 \\
a_0 & a_1 & a_0a_1 & a_2 & a_0a_2 & a_1a_2 & a_0a_1a_2 & a_3 & a_0a_3 \\
a_1 & a_2 & a_0a_2 & a_3 & a_0a_3 & a_1a_3 & a_0a_1a_3 & a_4 & a_0a_4 \\
a_0a_1 & a_1a_2 & a_0a_1a_2 & a_2a_3 & a_0a_2a_3 & a_1a_2a_3 & a_0a_1a_2a_3 & a_3a_4 & a_0a_3a_4 \\
a_2 & a_3 & a_0a_3 & a_4 & a_0a_4 & a_1a_4 & a_0a_1a_4 & a_5 & a_0a_5 \\
a_0a_2 & a_1a_3 & a_0a_1a_3 & a_2a_4 & a_0a_2a_4 & a_1a_2a_4 & a_0a_1a_2a_4 & a_3a_5 & a_0a_3a_5 \\
a_1a_2 & a_2a_3 & a_0a_2a_3 & a_3a_4 & a_0a_3a_4 & a_1a_3a_4 & a_0a_1a_3a_4 & a_4a_5 & a_0a_4a_5 \\
a_0a_1a_2 & a_1a_2a_3 & a_0a_1a_2a_3 & a_2a_3a_4 & a_0a_2a_3a_4 & a_1a_2a_3a_4 & a_0a_1a_2a_3a_4 & a_3a_4a_5 & a_0a_3a_4a_5 \\
a_3 & a_4 & a_0a_4 & a_5 & a_0a_5 & a_1a_5 & a_0a_1a_5 & a_6 & a_0a_6 \\
a_0a_3 & a_1a_4 & a_0a_1a_4 & a_2a_5 & a_0a_2a_5 & a_1a_2a_5 & a_0a_1a_2a_5 & a_3a_6 & a_0a_3a_6 \\
a_1a_3 & a_2a_4 & a_0a_2a_4 & a_3a_5 & a_0a_3a_5 & a_1a_3a_5 & a_0a_1a_3a_5 & a_4a_6 & a_0a_4a_6 \\
a_0a_1a_3 & a_1a_2a_4 & a_0a_1a_2a_4 & a_2a_3a_5 & a_0a_2a_3a_5 & a_1a_2a_3a_5 & a_0a_1a_2a_3a_5 & a_3a_4a_6 & a_0a_3a_4a_6 \\
a_2a_3 & a_3a_4 & a_0a_3a_4 & a_4a_5 & a_0a_4a_5 & a_1a_4a_5 & a_0a_1a_4a_5 & a_5a_6 & a_0a_5a_6 \\
a_0a_2a_3 & a_1a_3a_4 & a_0a_1a_3a_4 & a_2a_4a_5 & a_0a_2a_4a_5 & a_1a_2a_4a_5 & a_0a_1a_2a_4a_5 & a_3a_5a_6 & a_0a_3a_5a_6 \\
a_1a_2a_3 & a_2a_3a_4 & a_0a_2a_3a_4 & a_3a_4a_5 & a_0a_3a_4a_5 & a_1a_3a_4a_5 & a_0a_1a_3a_4a_5 & a_4a_5a_6 & a_0a_4a_5a_6
\end{pmatrix}$$

et la sous-matrice obtenue en ne conservant que les lignes et les colonnes dont les indices sont de la forme 2^i et $0^j = x_0^j$ respectivement n'est rien d'autre que la matrice de Hankel au sens classique,

$$\begin{pmatrix}
a_0 & a_1 & a_2 & a_3 & \cdots \\
a_1 & a_2 & a_3 & a_4 & \\
a_2 & a_3 & a_4 & a_5 & \\
a_3 & a_4 & a_5 & a_6 & \\
\vdots & & & &
\end{pmatrix},$$

de la série

$$F(t) = \sum_{k\geq 0} a_k t^k.$$

La 2-régularité de $f(z)$ implique donc la rationalité de $F(t)$. Cependant $F(t)$ ne peut pas être une série rationnelle quelconque. Supposons en effet la suite (a_k) géométrique : $a_k = a\rho^k$ (avec $a \neq 0$). La série $f(z)$ est alors donnée par

$$f(z) = \sum_{n\geq 0} a^{\nu(n)} \rho^{\sigma(n)} z^n,$$

$$f(z) = 1 + az + arz^2 + a^2rz^3 + ar^2z^4 + a^2r^2z^5 + a^2r^3z^6 + a^3r^3z^7 + ar^3z^8 + a^2r^3z^9 + a^2r^4z^{10} + \cdots,$$

en notant $\nu(n)$ le nombre d'occurrence de 1 dans l'écriture binaire de n et $\sigma(n)$ la somme $\sum_i i\epsilon_i$ si $n = \sum_i 2^i\epsilon_i$. La matrice de Hankel est alors de la forme suivante,

$$\begin{pmatrix}
1 & 1 & a & 1 & a & a\rho & a^2\rho & 1 & a & a\rho & a^2\rho & a\rho^2 & a^2\rho^2 & a^2\rho^3 \\
a & a\rho & a^2\rho & a\rho^2 & a^2\rho^2 & a^2\rho^3 & a^3\rho^3 & a\rho^3 & a^2\rho^3 & a^2\rho^4 & a^3\rho^4 & a^2\rho^5 & a^3\rho^5 & a^3\rho^6 \\
a\rho & a\rho^2 & a^2\rho^2 & a\rho^3 & a^2\rho^3 & a^2\rho^4 & a^3\rho^4 & a\rho^4 & a^2\rho^4 & a^2\rho^5 & a^3\rho^5 & a^2\rho^6 & a^3\rho^6 & a^3\rho^7 \\
a^2\rho & a^2\rho^3 & a^3\rho^3 & a^2\rho^5 & a^3\rho^5 & a^3\rho^6 & a^4\rho^6 & a^2\rho^7 & a^3\rho^7 & a^3\rho^8 & a^4\rho^8 & a^3\rho^9 & a^4\rho^9 & a^4\rho^{10} \\
a\rho^2 & a\rho^3 & a^2\rho^3 & a\rho^4 & a^2\rho^4 & a^2\rho^5 & a^3\rho^5 & a\rho^5 & a^2\rho^5 & a^2\rho^6 & a^3\rho^6 & a^2\rho^7 & a^3\rho^7 & a^3\rho^8 \\
a^2\rho^2 & a^2\rho^4 & a^3\rho^4 & a^2\rho^6 & a^3\rho^6 & a^3\rho^7 & a^4\rho^7 & a^2\rho^8 & a^3\rho^8 & a^3\rho^9 & a^4\rho^9 & a^3\rho^{10} & a^4\rho^{10} & a^4\rho^{11} \\
a^2\rho^3 & a^2\rho^5 & a^3\rho^5 & a^2\rho^7 & a^3\rho^7 & a^3\rho^8 & a^4\rho^8 & a^2\rho^9 & a^3\rho^9 & a^3\rho^{10} & a^4\rho^{10} & a^3\rho^{11} & a^4\rho^{11} & a^4\rho^{12} \\
a^3\rho^3 & a^3\rho^6 & a^4\rho^6 & a^3\rho^9 & a^4\rho^9 & a^4\rho^{10} & a^5\rho^{10} & a^3\rho^{12} & a^4\rho^{12} & a^4\rho^{13} & a^5\rho^{13} & a^4\rho^{14} & a^5\rho^{14} & a^5\rho^{15}
\end{pmatrix}.$$

Si la série est 2-régulière, le mineur d'indices 0, 1, 3, ..., $2^n - 1$ pour les lignes et ε, 0, 00, ..., 0^n pour les colonnes est nul pour n assez grand. Ceci s'écrit

$$\det\left(a^i\rho^{i(i-1)/2+ij}\right)_{0\le i,j\le n} = a^{\binom{n}{2}}\rho^{\binom{n+1}{3}}\prod_{0\le k<l\le n}(\rho^l-\rho^k) = 0$$

et montre que ρ est nécessairement une racine de l'unité ou 0, dans l'hypothèse où l'anneau de référence est un corps. Cette condition est d'ailleurs suffisante d'après l'exemple précédent. D'autre part nous verrons que la série

$$f(z) = \prod_{k\ge 0}\left(1+(k+1)z^{2^k}\right)$$

n'est pas régulière, alors que

$$F(t) = \sum_{k\ge 0}(k+1)t^k$$

est rationnelle. Il semble donc que $F(t)$ ne peut avoir que des pôles simples racines de l'unité, ce qui signifie que la suite (a_k) est périodique à partir d'un certain rang.

Pour prouver ceci nous remarquons que la rationalité de $F(t)$ fournit pour a_k une expression de la forme

$$a_k = \sum_\rho P_\rho(k)\rho^k$$

en notant P_ρ un polynôme de degré $n_\rho - 1$, si n_ρ est l'ordre de multiplicité de la racine ρ. D'autre part nous avons obtenu la rationalité de $F(t)$ en considérant la sous-suite dont les indices sont des 2^i, puisque nous avons utilisé la sous-matrice dont les indices de ligne et de colonnes sont respectivement de la forme 2^i et 0^j. Utilisons maintenant la sous-matrice dont les indices de ligne et de colonnes sont respectivement de la forme $2^{i+1}+2^i$ et 0^j, autrement dit la sous-suite dont les indices sont des nombres à deux bits. Ici encore apparaît une série rationnelle dont la matrice de Hankel est cette fois-ci

$$\begin{pmatrix} a_0a_1 & a_1a_2 & a_2a_3 & a_3a_4 & \cdots \\ a_1a_2 & a_2a_3 & a_3a_4 & a_4a_5 & \\ a_2a_3 & a_3a_4 & a_4a_5 & a_5a_6 & \\ a_3a_4 & a_4a_5 & a_5a_6 & a_6a_7 & \\ \vdots & & & & \end{pmatrix}.$$

Puisque celle-ci utilise les mêmes colonnes d'indice 0^j que la matrice de $F(t)$, la série rationnelle

$$F_1(t) = \sum_{k\ge 0} a_ka_{k+1}t^k$$

est définie par la même relation de récurrence que $F(t)$. L'égalité

$$a_ka_{k+1} = \sum_{\rho_1,\rho_2} P_{\rho_1}(k)P_{\rho_2}(k)(\rho_1\rho_2)^k$$

doit donner une expression des coefficients de $F_1(t)$ de la même forme que l'expression de a_k, ce qui fait que l'ensemble des racines ρ est stable par multiplication. C'est donc un groupe de racines de l'unité, disons le groupe des racines T-ièmes de l'unité $\mathbb{U}_T$. La limitation aux a_k d'indice k multiple de T permet d'éliminer les racines de l'unité et $a_{\ell T}$ s'écrit

$$a_{\ell T} = \sum_\rho P_\rho(\ell T) = Q(\ell),$$

où $Q(\ell)$ est un polynôme dont le degré est $\nu - 1$ si ν est le maximum des multiplicités des ρ. Il se peut que $Q(\ell)$ admette quelques racines entières mais $Q(\ell)$ n'est pas nul pour les ℓ plus grands qu'un certain L. Le remplacement de $f(z)$ par

$$S_0^{LT}f(z) = \prod_{k\ge 0}\left(1+a_{k+LT}z^{2^k}\right),$$

qui est aussi régulière, permet de supposer que le polynôme $Q(\ell)$ associé ne s'annule pas sur les entiers naturels. Cela revient aussi à utiliser une certaine sous-matrice de la matrice de Hankel de $f(z)$ et correspond à un simple décalage sur $F(t)$. La sous-matrice de la matrice de Hankel de $f(z)$ obtenue en ne conservant que les lignes et les colonnes dont les indices sont respectivement de la forme $1+2^T+\cdots+2^{\ell T}$ et $1(0^T1)^j$, liées aux entiers dont l'écriture binaire est dans le langage $1(0^T1)^*$, vaut

$$\begin{pmatrix} a_0 & a_0a_T & a_0a_Ta_{2T} & a_0a_Ta_{2T}a_{3T} & \cdots \\ a_0a_T & a_0a_Ta_{2T} & a_0a_Ta_{2T}a_{3T} & a_0a_Ta_{2T}a_{3T}a_{4T} & \\ a_0a_Ta_{2T} & a_0a_Ta_{2T}a_{3T} & a_0a_Ta_{2T}a_{3T}a_{4T} & a_0a_Ta_{2T}a_{3T}a_{4T}a_{5T} & \\ a_0a_Ta_{2T}a_{3T} & a_0a_Ta_{2T}a_{3T}a_{4T} & a_0a_Ta_{2T}a_{3T}a_{4T}a_{5T} & a_0a_Ta_{2T}a_{3T}a_{4T}a_{5T}a_{6T} & \\ \vdots & & & & \end{pmatrix}.$$

Comme cette matrice est de rang fini, la série

$$G(t)=\sum_{j\geq \ell_0}\left(\prod_{\ell=\ell_0}^{j}Q(\ell)\right)t^j$$

est rationnelle ce qui est impossible si ν, qui est le degré de $Q(\ell)$, est supérieur ou égal à 1. Ainsi la fraction rationnelle n'a que des pôles simples et qui sont tous des racines de l'unité.

L'exemple précédent se généralise aisément à un entier $B\geq 2$ et fournit l'énoncé suivant.

Proposition 26. *La série*

$$\prod_{k\geq 0}\left(1+a_kz^{B^k}\right),$$

à coefficients dans un corps, est B-régulière si et seulement si la suite (a_k) est périodique à partir d'un certain rang.

4.4 Récurrences

Les suites B-régulières vérifient divers types de récurrence et nous voulons montrer ici celles qui traduisent précisément le fait que les séries B-régulières sont étroitement associées aux séries rationnelles. Nous commençons par un exemple.

Exemple 42 : La complexité du tri fusion dans le cas le pire vérifie la récurrence, du type *diviser pour régner*,

$$T_n=T_{\lfloor n/2\rfloor}+T_{\lceil n/2\rceil}+n-1.$$

En utilisant cette relation, il n'est pas difficile de vérifier que $T(z)=\sum_{n\geq 0}T_nz^n$ est $(\mathbb{Z},2)$-régulière. Un module de type fini adéquat est celui engendré par $T(z)$, $T(z)/z$, $2z/(1-z)^2$, $z(1+z)/(1-z)^2$ et $(1+z)/(1-z)^2$. Avec cette base les opérateurs de section S_0 et S_1 ont respectivement pour matrice

$$A_0=\begin{pmatrix} 2&1&0&0&0\\ 0&1&0&0&0\\ 0&1&2&1&1\\ 1&0&0&1&0\\ 0&0&0&0&1\end{pmatrix},\quad A_1=\begin{pmatrix} 1&0&0&0&0\\ 1&2&0&0&0\\ 1&0&0&1&-1\\ 0&0&0&0&0\\ 0&1&2&1&3\end{pmatrix}$$

et la représentation linéaire est complétée par

$$\lambda = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

La sous-matrice de sa matrice de Hankel obtenue en ne conservant que les lignes d'indice entre 0 et 14 et les colonnes d'indice entre ε et 111 est

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 1 & 3 & 0 & 0 & 1 & 3 & 5 & 8 & 11 & 14 \\
0 & 1 & 3 & 5 & 8 & 11 & 14 & 17 & 21 & 25 & 29 & 33 & 37 & 41 & 45 \\
1 & 5 & 8 & 17 & 21 & 25 & 29 & 49 & 54 & 59 & 64 & 69 & 74 & 79 & 84 \\
3 & 11 & 14 & 33 & 37 & 41 & 45 & 89 & 94 & 99 & 104 & 109 & 114 & 119 & 124 \\
5 & 17 & 21 & 49 & 54 & 59 & 64 & 129 & 135 & 141 & 147 & 153 & 159 & 165 & 171 \\
8 & 25 & 29 & 69 & 74 & 79 & 84 & 177 & 183 & 189 & 195 & 201 & 207 & 213 & 219 \\
11 & 33 & 37 & 89 & 94 & 99 & 104 & 225 & 231 & 237 & 243 & 249 & 255 & 261 & 267 \\
14 & 41 & 45 & 109 & 114 & 119 & 124 & 273 & 279 & 285 & 291 & 297 & 303 & 309 & 315 \\
17 & 49 & 54 & 129 & 135 & 141 & 147 & 321 & 328 & 335 & 342 & 349 & 356 & 363 & 370 \\
21 & 59 & 64 & 153 & 159 & 165 & 171 & 377 & 384 & 391 & 398 & 405 & 412 & 419 & 426 \\
25 & 69 & 74 & 177 & 183 & 189 & 195 & 433 & 440 & 447 & 454 & 461 & 468 & 475 & 482 \\
29 & 79 & 84 & 201 & 207 & 213 & 219 & 489 & 496 & 503 & 510 & 517 & 524 & 531 & 538 \\
33 & 89 & 94 & 225 & 231 & 237 & 243 & 545 & 552 & 559 & 566 & 573 & 580 & 587 & 594 \\
37 & 99 & 104 & 249 & 255 & 261 & 267 & 601 & 608 & 615 & 622 & 629 & 636 & 643 & 650 \\
41 & 109 & 114 & 273 & 279 & 285 & 291 & 657 & 664 & 671 & 678 & 685 & 692 & 699 & 706
\end{pmatrix}.$$

Elle est de rang 5 et les colonnes numéros 1, 2, 3, 4 et 6 d'indices ε, 0, 1, 00 et 10 sont indépendantes, ce qui implique que les suites (T_n), (T_{2n}), (T_{2n+1}), (T_{4n}) et (T_{4n+2}) sont indépendantes. Comme nous connaissons une représentation de dimension 5, nous pouvons affirmer que $T(z)$ est de rang 5.

En exprimant les colonnes de la sous-matrice en fonction des colonnes d'indice ε, 0, 1, 00 et 10, nous soupçonnons que la suite vérifie les relations de récurrence suivantes :

$$\begin{aligned}
T_{4n+1} &= 4T_n - 5T_{2n} + T_{2n+1} + 2T_{4n}, \\
T_{4n+3} &= -12T_n + 15T_{2n} - 3T_{2n+1} - 5T_{4n} + 3T_{4n+2}, \\
T_{8n} &= 4T_n - 8T_{2n} + 5T_{4n}, \\
T_{8n+1} &= 12T_n - 17T_{2n} + T_{2n+1} + 7T_{4n}, \\
T_{8n+2} &= 12T_n - 16T_{2n} + 6T_{4n} + T_{4n+2}, \\
T_{8n+3} &= 4T_n - 5T_{2n} - 3T_{2n+1} + 2T_{4n} + 3T_{4n+2}, \\
T_{8n+4} &= -4T_n + 6T_{2n} - 6T_{2n+1} - 2T_{4n} + 5T_{4n+2}, \\
T_{8n+5} &= -20T_n + 27T_{2n} - 11T_{2n+1} - 9T_{4n} + 8T_{4n+2}, \\
T_{8n+6} &= -36T_n + 48T_{2n} - 16T_{2n+1} - 16T_{4n} + 11T_{4n+2}, \\
T_{8n+7} &= -52T_n + 69T_{2n} - 21T_{2n+1} - 23T_{4n} + 14T_{4n+2}.
\end{aligned}$$

Il est possible de vérifier ces relations en utilisant la récurrence initiale, mais nous verrons plus loin une méthode plus efficace.

Toutes ces relations n'ont pas le même intérêt. En effet pour construire une représentation linéaire qui utilise la base (T_n), (T_{2n}), (T_{2n+1}), (T_{4n}) et (T_{4n+2}), seules les relations

$$\begin{aligned}
T_{4n+1} &= 4T_n - 5T_{2n} + T_{2n+1} + 2T_{4n}, \\
T_{4n+3} &= -12T_n + 15T_{2n} - 3T_{2n+1} - 5T_{4n} + 3T_{4n+2}, \\
T_{8n} &= 4T_n - 8T_{2n} + 5T_{4n}, \\
T_{8n+2} &= 12T_n - 16T_{2n} + 6T_{4n} + T_{4n+2}, \\
T_{8n+4} &= -4T_n + 6T_{2n} - 6T_{2n+1} - 2T_{4n} + 5T_{4n+2}, \\
T_{8n+6} &= -36T_n + 48T_{2n} - 16T_{2n+1} - 16T_{4n} + 11T_{4n+2}
\end{aligned}$$

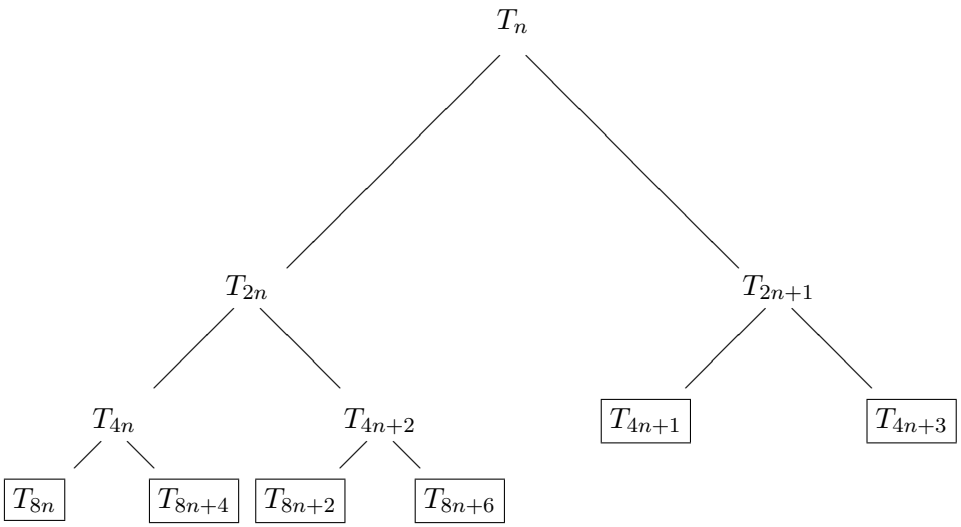

FIG. 4.2
Les feuilles de l'arbre donnent la forme des relations de récurrence.

sont utiles, comme on s'en convainc facilement en considérant l'arbre binaire de la figure 4.2. D'ailleurs ces relations définissent complètement la suite quand on connaît les valeurs de T_0, T_1, T_2. Elles se traduisent par une nouvelle représentation linéaire de dimension 5 avec les matrices

$$A_0 = \begin{pmatrix} 0 & 0 & 4 & 4 & 12 \\ 1 & 0 & -5 & -8 & -16 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 5 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & -12 & -4 & -36 \\ 0 & 0 & 15 & 6 & 48 \\ 1 & 0 & -3 & -6 & -16 \\ 0 & 0 & -5 & -2 & -16 \\ 0 & 1 & 3 & 5 & 11 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Toutes les séries régulières vérifient des récurrences du même type que celle que nous venons de rencontrer. Pour exposer ceci nous avons besoin de quelques notions supplémentaires.

Définition 31. *L'algèbre engendrée par les opérateurs de B-section $S_{B,r}$ est notée $\mathbb{A}\langle S_* \rangle$.*

Proposition 27. *L'algèbre $\mathbb{A}\langle S_* \rangle$ est isomorphe à l'algèbre des polynômes $A\langle \mathcal{X} \rangle$.*

DÉMONSTRATION. Il suffit de vérifier que la famille $(S_w)_{w \in \mathcal{X}^*}$ est libre. Si $\sum_w \lambda_w S_w = 0$, l'application de cet opérateur à z^n, où $n = \overline{1u}$ et u est le mot le plus long qui donne un coefficient λ non nul, donne le polynôme nul et le coefficient de z est λ_u, qui est donc nul. □

Définition 32. *Le B-annulateur $\mathcal{I}_f$ d'une série $f(z)$ est l'idéal à gauche des $\sum_w \lambda_w S_w \in \mathbb{A}\langle S_* \rangle$ qui s'annulent sur $f(z)$.*

L'algèbre $\mathbb{A}\langle S_*\rangle$ et l'idéal $\mathcal{I}_f$ ne sont que des versions édulcorées des notions d'algèbre et d'idéal *syntactiques* dues à Ch. Reutenauer [62, p. 45].

EXEMPLE 43 : Reprenons la série $T(z)$ associé au tri-fusion dans le cas le pire. Les relations de récurrence ci-dessus expriment des relations de dépendance linéaires entre les sections de la série et nous pourrions tout aussi bien les écrire de la façon suivante (rappelons que S_w est le composé $S_{r_N}\cdots S_{r_0}$ si $w = r_N\cdots r_0 \in \mathcal{X}^*$, en particulier S_ε est l'identité) :

$$\begin{aligned}
S_{01}T(z) &= 4S_\varepsilon T(z) - 5S_0T(z) + S_1T(z) + 2S_{00}T(z),\\
S_{11}T(z) &= -12S_\varepsilon T(z) + 15S_0T(z) - 3S_1T(z) - 5S_{00}T(z) + 3S_{10}T(z),\\
S_{000}T(z) &= 4S_\varepsilon T(z) - 8S_0T(z) + 5S_{00}T(z),\\
S_{010}T(z) &= 12S_\varepsilon T(z) - 16S_0T(z) + 6S_{00}T(z) + S_{10}T(z),\\
S_{100}T(z) &= -4S_\varepsilon T(z) + 6S_0T(z) - 6S_1T(z) - 2S_{00}T(z) + 5S_{10}T(z),\\
S_{110}T(z) &= -36S_\varepsilon T(z) + 48S_0T(z) - 16S_1T(z) - 16S_{00}T(z) + 11S_{10}T(z).
\end{aligned}$$

Ainsi l'opérateur $S_{01} - 4S_\varepsilon + 5S_0 - S_1 - 2S_{00}$ est dans le noyau $\mathcal{I}_T$. La composition à gauche par S_0 montre qu'il en est de même de l'opérateur $S_{001} - 4S_0 + 5S_{00} - S_{01} - 2S_{000}$. Celui-ci fournit la relation de récurrence

$$T_{8n+1} = 4T_{2n} - 5T_{4n} + T_{4n+1} - 2T_{8n}.$$

Pour tout dire, cette multiplication par S_0 équivaut à une substitution de $2n$ à n dans les relations de récurrences. À partir de ces relations, on peut retrouver toutes les relations de récurrences de ce type vérifiées par la suite. Par exemple le fait que $S_{000} - 4S_\varepsilon + 8S_0 - 5S_{00}$ et $S_{01} - 4S_\varepsilon + 5S_0 - S_1 - 2S_{00}$ soient dans $\mathcal{I}_T$ implique que $S_{001} - 12S_\varepsilon + 17S_0 - S_1 - 7S_{00}$ est dans $\mathcal{I}_T$, c'est-à-dire que la suite (T_n) vérifie la récurrence vue plus haut

$$T_{8n+1} = 12T_n - 17T_{2n} + T_{2n+1} + 7T_{4n}.$$

Définition 33. *Un code suffixe est une partie $\mathcal{C}$ de $\mathcal{X}^*$ qui vérifie la propriété suivante : si elle contient un mot, alors elle ne contient pas ses suffixes stricts (ses facteurs droits propres). Un code suffixe est complet si tout mot assez long possède un suffixe dans $\mathcal{C}$.*

Une partie suffixielle $\mathcal{S}$ est une partie de $\mathcal{X}^*$, qui dès qu'elle contient un mot, contient tous ses suffixes.

EXEMPLE 44 : A l'arbre de la figure 4.2 est naturellement associé celui de la figure 4.3. Les feuilles fournissent le code suffixe complet $\mathcal{C} = \{000, 100, 010, 110, 01, 11\}$ et les nœuds internes donnent la partie suffixielle $\mathcal{S} = \{\varepsilon, 0, 1, 00, 10\}$.

On montre [13, p. 41] qu'il y a bijection entre les codes suffixes complets finis et les parties suffixielles non vides, le passage se faisant par les formules $\mathcal{S} = \mathcal{X}^* \setminus \mathcal{C}\mathcal{X}^*$ et $\mathcal{C} = \mathcal{X}\mathcal{S} \setminus \mathcal{S}$.

Théorème 12 (Théorème des récurrences typiques)**.** *Si $f(z)$ une série B-régulière, il existe une partie suffixielle finie $\mathcal{S}$ de $\mathcal{X}^*$, de code suffixe associé $\mathcal{C}$, telle que la série $f(z)$ vérifie les relations*

$$S_c f(z) = \sum_{s\in\mathcal{S}} \alpha_{c,s} S_s f(z) \quad (c \in \mathcal{C}).$$

Si l'anneau de référence est un corps, on peut de plus affirmer que le nombre d'éléments de $\mathcal{S}$ est le rang de $f(z)$, que les $S_s f(z)$ $(s \in \mathcal{S})$ forment une base de l'espace stable par section engendré par $f(z)$ et que l'idéal annulateur $\mathcal{I}_f$ est engendré par les $S_c - \sum_{s\in\mathcal{S}} \alpha_{c,s} S_s$ $(c \in \mathcal{C})$.

DÉMONSTRATION. Commençons par supposer que l'anneau de référence est un corps $\mathbb{K}$. Si $\operatorname{rg} f = 0$, il n'y a rien à faire ; nous prenons pour $\mathcal{S}$ la partie vide et $\mathcal{C}$ est réduit au mot vide. Sinon nous construisons pas à pas la partie $\mathcal{S}$ de façon à avoir sans cesse une partie suffixielle. Nous posons d'abord $\mathcal{S} = \{\varepsilon\}$ et $\mathcal{C} = \emptyset$ puis nous regardons successivement les sections $S_r f(z)$ dans l'ordre $r = 0, 1, \ldots$ c'est-à-dire les colonnes de la

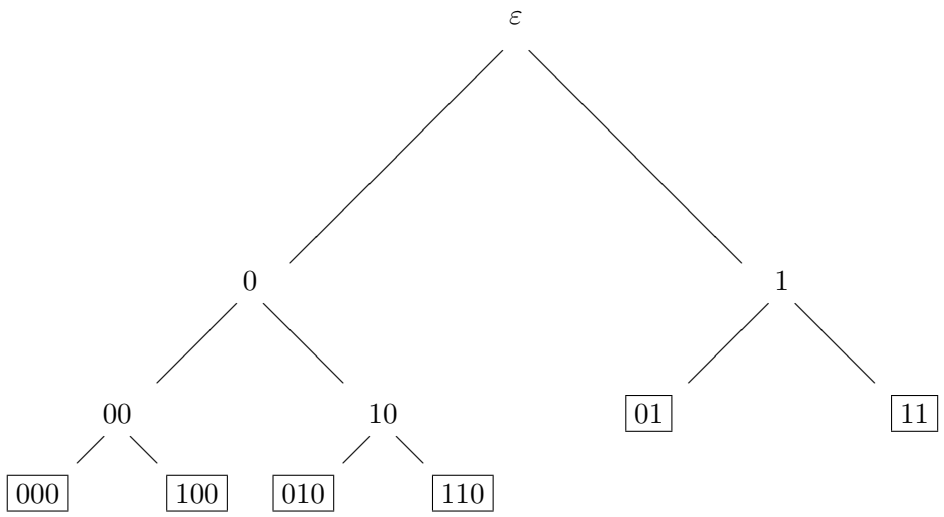

FIG. 4.3
Les étiquettes des feuilles forment un code suffixe complet.

matrice de Hankel dans leur ordre naturel. Chaque section $S_r f(z)$ ou bien est indépendante des précédentes et nous mettons le mot x_r dans $\mathcal{S}$, ou bien est dépendante des précédentes et nous mettons x_r dans $\mathcal{C}$, nous l'exprimons en fonction des $S_s f(z)$, où s est déjà dans $\mathcal{S}$. Nous considérons ensuite dans l'ordre les mots u qui sont dans $\mathcal{S}$ et pour chacun nous regardons les $S_r S_u f(z)$ avec r successivement égal à 0, 1, ... Nous appliquons ce procédé autant que faire se peut. Comme l'espace vectoriel engendré par les sections est de dimension $N = \operatorname{rg} f$, ce calcul termine en considérant au plus $1 + B + \cdots + B^{N-1}$ sections et la partie obtenue $\mathcal{S}$ est suffixielle. La partie $\mathcal{C}$ obtenue est clairement le code suffixe associé. Les relations obtenues sont de la forme indiquée et vérifient même une contrainte supplémentaire qui s'exprime par $\alpha_{c,s} = 0$ si $c \prec s$.

Pour le cas général, nous reprenons la démonstration de [62, p. 30]. Si A_r $(0 \leq r < B)$, λ, γ est une représentation linéaire de $f(z)$ de dimension N, nous notons $A_{w_1 \cdots w_l}$ le produit $A_{w_1} \cdots A_{w_l}$ et nous considérons le sous-anneau $\mathbb{B}$ de $\mathbb{A}$ engendré par les coefficients des matrices λ, γ et A_0, A_1, ... Cet anneau est de type fini et donc nœthérien. Il en résulte que $\mathbb{B}^N$ est un $\mathbb{B}$-module nœthérien. Si $\mathcal{S}$ est une partie de $\mathcal{X}^*$, nous notons $\mathcal{M}(\mathcal{S})$ le sous-module de $\mathbb{B}^N$ engendré par les λA_w pour w dans $\mathcal{S}$. La famille des sous-modules $\mathcal{M}(\mathcal{S})$ obtenue en faisant varier $\mathcal{S}$ dans l'ensemble des parties suffixielles finies de $\mathcal{X}^*$ admet un élément maximal. Appelons $\mathcal{S}$ une partie suffixielle finie qui fournit ce sous-module et $\mathcal{C}$ le code suffixe complet associé. Pour chaque c pris dans $\mathcal{C}$, nous avons $\mathcal{M}(\mathcal{S}) = \mathcal{M}(\mathcal{S} \cup \{c\})$ d'où une relation

$$\lambda A_c = \sum_{s \in \mathcal{S}} \alpha_{c,s} \lambda A_s.$$

□

Si l'anneau de référence est un corps, la démonstration précédente fournit un moyen pratique d'obtenir une représentation linéaire et des relations de récurrence pour une série régulière.

Définition 34. *Une représentation linéaire obtenue par l'algorithme exposé dans la démonstration précédente sera dite typique.*

La majoration du nombre de sections considérées dans la démonstration ou encore la forme des relations de récurrence fournissent tout de suite un théorème d'égalité à la Eilenberg-Schützenberger [31, p. 143].

Théorème 13 (Théorème d'égalité)**.** *Si $f(z)$ est une série régulière à coefficients dans un anneau intègre, de rang inférieur ou égal à N et telle que $f_n = 0$ pour tous les entiers n strictement inférieurs à B^N alors $f(z) = 0$.*

En particulier, pour vérifier que deux représentations linéaires de dimension N_1 et N_2 définissent la même série régulière, il suffit de calculer les valeurs pour les entiers de 0 à $B^{N_1+N_2} - 1$.

EXEMPLE 45 : Les deux représentations linéaires que nous avons rencontrées dans l'étude de la suite (T_n) liée au tri-fusion sont équivalentes. En effet ces représentations utilisaient respectivement comme base $T(z)$, $T(z)/z$, $2z/(1-z)^2$, $z(1+z)/(1-z)^2$ et $(1+z)/(1-z)^2$ d'une part et $T(z)$, $S_0T(z)$, $S_1T(z)$, $S_{00}T(z)$ et $S_{10}T(z)$ d'autre part. La fusion ces deux bases en une famille à 9 éléments $T(z)$, $T(z)/z$, ..., $(1+z)/(1-z)^2$, $S_0T(z)$, et $S_{10}T(z)$ permet de construire une représentation linéaire de dimension 9 pour la différence des deux séries qu'elles définissent respectivement et il suffit de vérifier que cette différence est nulle jusqu'au rang $2^9 - 1 = 511$ pour conclure qu'elles définissent toutes les deux la série $T(z)$. En particulier ceci justifie la validité des relations de récurrence que nous avons données.

Revenons sur le théorème des récurrences typiques par un énoncé qui sera utile au chapitre 7.

Proposition 28. *Une représentation linéaire A_0, A_1, ..., λ, γ de dimension N d'une série B-régulière est réduite si et seulement si les produits λA_w et $A_w\gamma$, avec $w \in \mathcal{X}^*$, engendrent respectivement $\mathbb{K}^{1\times N}$ et $\mathbb{K}^{N\times 1}$.*

Si A_0, A_1, ..., λ, γ est une représentation linéaire réduite, standard et typique d'une série B-régulière de rang N, il existe N mots u_1, u_2, ..., u_N, pris dans $\varepsilon + \mathcal{X}_+\mathcal{X}^*$, tels que les λA_{u_1}, ..., λA_{u_N} engendrent $\mathbb{K}^{1\times N}$ et N mots v_1, v_2, ..., v_N tels que les $A_{v_1}\gamma$, ..., $A_{v_N}\gamma$ constituent la base canonique de $\mathbb{K}^{N\times 1}$.

DÉMONSTRATION. Nous ne démontrons que le second point de la proposition, car le premier est issu de [13, p. 37]. Pour ce qui est des $A_w\gamma$, il existe, d'après le théorème des récurrences typiques, une partie suffixielle $\mathcal{S}$ telle que les sections $S_sf(z)$ forment une base de l'espace stable par section engendré par la série $f(z)$. Avec une telle base, les $A_s\gamma$ sont alors les vecteurs de la base canonique de $\mathbb{C}^N$. Nous numérotons les éléments de $\mathcal{S}$ de façon que $A_{v_j}\gamma$ soit le j-ième vecteur de base de $\mathbb{C}^N$. Quant aux λA_w, l'élimination des 0 à gauche provient du fait que la représentation obtenue est standard. □

4.5 Propriétés de clôture

Allouche et Shallit [6, p. 174] ont caractérisé les séries rationnelles qui sont B-régulières quand l'anneau de référence est un corps.

Proposition 29. *Une fraction rationnelle sur un corps $\mathbb{K}$ est B-régulière si et seulement si ses pôles sont des racines de l'unité, dans la clôture algébrique de $\mathbb{K}$. En particulier une fraction rationnelle sur un corps fini est B-régulière.*

DÉMONSTRATION. Les sections d'une série rationnelle ont pour pôles les puissances B-ièmes des pôles de la fraction. Si la série rationnelle est B-régulière les pôles des séries, qui sont dans l'espace de dimension finie stable par section, forment un ensemble fini stable par l'élévation à la puissance B, donc sont des racines de l'unité. La réciproque est évidente car il suffit, par décomposition en éléments simples dans une extension convenable, de considérer les fractions de la forme $1/(1-\omega z)^N$, où ω est une racine de l'unité. □

EXEMPLE 46 : En particulier, si l'anneau de référence est un corps, la série génératrice d'une suite géométrique $\sum_n \rho^n z^n = 1/(1-\rho z)$ est régulière si et seulement ρ est 0 ou une racine de l'unité [6, p. 173].

Si les pôles de la fraction rationnelle sont des racines N-ièmes de l'unité et si l'ordre maximum de ces pôles est k, toutes les sections vérifient cette même propriété, ce qui fait que le rang de la fraction comme série B-régulière est au plus $N\,(k+1)$.

EXEMPLE 47 : La série génératrice du chiffre d'indice k de l'écriture en base B est la série rationnelle (cf. page 78)

$$\epsilon_k(z) = \frac{1-z^{B^k}}{1-z}\left(\sum_{1\le r<B} r\, z^{rB^k}\right)\frac{1}{1-z^{B^{k+1}}}$$

et son rang est $k+2$. Ceci est conforme à la majoration que nous venons de donner. En pratique cette majoration est trop large parce que la fraction rationnelle possède une symétrie par rapport à ses pôles. Ici tous les pôles sont simples et n'interviennent que par la fraction $1/(1-z^{B^{k+1}})$, ce qui fait que les résidus ne sont pas indépendants les uns des autres.

Les séries ($\mathbb{A}$,B)-régulières forment évidemment un module sur $\mathbb{A}$.

Proposition 30. *Si $f(z)$ et $g(z)$ sont régulières il en est de même de $f(z)+g(z)$ et on a l'inégalité* $\operatorname{rg}(f+g) \le \operatorname{rg} f + \operatorname{rg} g$.

Examinons les différents produits que l'on peut appliquer aux séries régulières. La concaténation dans $\mathcal{X}^*$ se traduit par une opération non commutative dans les séries formelles, que nous notons ici $\diamond$, et qui est définie par

$$z^n \diamond z^m = z^{B^{\lambda_B(m)}n+m}.$$

Evidemment elle est associative et admet 1 comme neutre. Plus lourdement, si

$$f = \sum_{n\ge 0} f_n z^n \;\text{ et }\; g = \sum_{n\ge 0} g_n z^n$$

alors la série $h = f \diamond g$ a pour coefficients les

$$h_n = \sum_{B^{\lambda(l)}k+l=n} f_k g_l$$

et le nombre de termes de cette somme est le nombre de chiffres non nuls dans l'écriture en base B de n augmenté de 1.

EXEMPLE 48 : Clairement la relation dans $\mathbb{N}$: $n \preceq m$ si et seulement si « $\tilde{n}$ est un suffixe de $\tilde{m}$ » est une relation d'ordre. Dans l'esprit de Rota [29], la fonction ζ est

$$\zeta(z) = \frac{1}{1-z}$$

et son carré

$$\zeta^{\diamond 2}(z) = \frac{1}{1-z}\left(1+\sum_{k\ge 0} z^{B^k}\frac{1-z^{B^k(B-1)}}{1-z^{B^{k+1}}}\right)$$

donne le nombre de « diviseurs » de chaque entier, c'est-à-dire le nombre de chiffres non nuls augmenté de 1.

La notion de clôture rationnelle se traduit par le résultat suivant.

Proposition 31. *L'ensemble des séries B-régulières à coefficients dans $\mathbb{A}$ est la plus petite partie $\mathcal{R}$ de $\mathbb{A}[[z]]$ vérifiant*

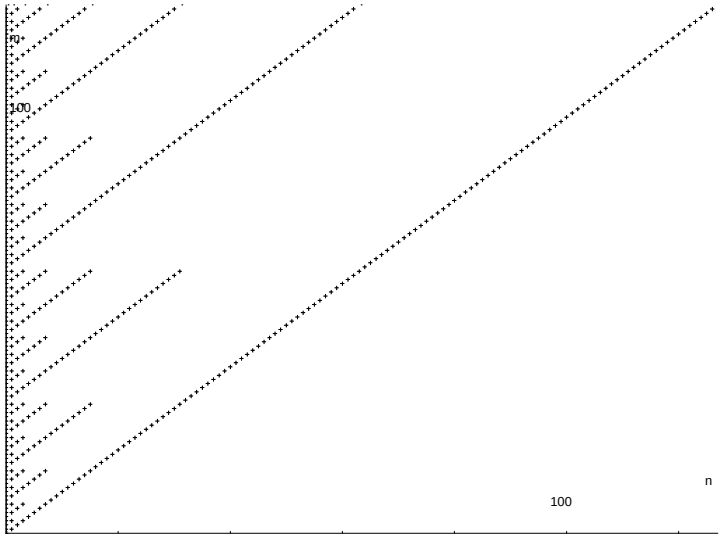

FIG. 4.4
Le graphe de la relation « l'écriture binaire de n est un suffixe de celle de m ».

- $\mathbb{A}[z] \subset \mathcal{R}$,
- $\mathcal{R} + \mathcal{R} \subset \mathcal{R}$,
- $\mathbb{A}\mathcal{R} \subset \mathcal{R}$,
- $\mathcal{R} \diamond \mathcal{R} \subset \mathcal{R}$,
- $f \in \mathcal{R},\ f(0) = 0 \ \Rightarrow\ \sum_{k\geq 0} f^{\diamond k} \in \mathcal{R}$.

Le produit $\diamond$, s'il est naturel ici, ne paraît pas avoir beaucoup d'utilisations. Le produit usuel et le produit de Hadamard sont plus dignes d'attention.

Théorème 14. *L'ensemble des séries B-régulières est stable par produit usuel et produit de Hadamard. Si f et g sont B-régulières, le rang de fg est au plus* $2 \operatorname{rg} f \operatorname{rg} g$ *et celui de $f \odot g$ est au plus* $\operatorname{rg} f \operatorname{rg} g$.

Pour le produit de Hadamard, ceci provient directement du résultat similaire pour les séries rationnelles. Pour le produit usuel il est dû à Allouche et Shallit [6, p. 173] et nous allons en redonner une démonstration.

DÉMONSTRATION. Soient f et g deux séries B-régulières. Quitte à utiliser le sous-anneau engendré par les coefficients des matrices de représentations linéaires de f et g, on peut supposer que l'anneau est nœthérien. Soient $\mathcal{F}$ et $\mathcal{G}$ deux sous-modules de type fini de $\mathbb{A}[[z]]$ contenant respectivement f et g et stable par les opérateurs de B-section. Pour conclure il suffit de montrer que le sous-module $\mathcal{M} = \mathcal{F}\mathcal{G} + z\mathcal{F}\mathcal{G}$, qui contient le produit fg, est stable lui aussi. D'après la formule (cf. page 20)

$$S_r(uv) = \sum_{s+t\equiv r \bmod B} z^{(s+t)\div B} S_s(u) S_t(v),$$

où, rappelons le, $a \div b$ désigne le quotient dans la division euclidienne de a par b, il est clair que

$$S_r(\mathcal{F}\mathcal{G}) \subset \mathcal{M}.$$

En outre, si $\phi \in \mathcal{F}$ et $\psi \in \mathcal{G}$,

$$S_r(z\phi\psi) = z^{(1+t)\div B} S_t(\phi\psi),$$

où le t est déterminé par

$$t \equiv r - 1 \bmod B.$$

En particulier l'exposant de z ne peut valoir 1 (c'est-à-dire être non nul) que si $t = B - 1$. Le calcul de $S_t(\phi\psi)$ ramène au cas précédent, ce qui permet de conclure, en remarquant que dans le « mauvais » cas où $t = B - 1$, il n'y a justement pas de z en facteur dans les termes de $S_t(\phi\psi)$.

La majoration du rang découle directement de la démonstration. Il en est de même pour le produit de Hadamard en utilisant la démonstration classique pour les séries rationnelles [13, p. 21]. □

Exemple 49 : Greene et Knuth [40, p. 25 à 28] considèrent la suite $f(n)$ définie par

$$f(n) = 1 + \min_i \left\{ \frac{i-1}{n} f(i-1) + \frac{n-i}{n} f(n-i) \right\},$$

en liaison avec le coût minimal de la recherche d'un entier fixé entre 1 et n. Les différences secondes de la suite définie par $g(n) = nf(n)$, $g(0) = 0$ et $g(1) = 0$, sont données par

$$\Delta^2 g(n) = \begin{cases} 2 & \text{si } n \text{ est une puissance de 2} \\ 1 & \text{si } n \text{ est pair sans être une puissance de 2} \\ -1 & \text{si } n \text{ est impair,} \end{cases}$$

ce qui fait que la série génératrice $g(z)$ vaut

$$g(z) = \frac{1}{(1-z)^2} \left(\frac{1}{1+z} + \sum_{k \geq 0} z^{2^k} \right).$$

Il en résulte que $g(z)$ est ($\mathbb{Z}$,2)-régulière comme produit de séries ($\mathbb{Z}$,2)-régulières.

Proposition 32. *La dérivée d'une série formelle B-régulière est B-régulière et son rang est moindre que* $4 \operatorname{rg} f$.

Démonstration. La dérivée de la série formelle $f(z)$ n'est rien d'autre que le produit de Hadamard de la série décalée $(f(z) - f(0))/z$ et de $1/(1-z)^2$. La première est B-régulière et de rang inférieur à $2 \operatorname{rg} f$. La majoration du rang de $f'(z)$ découle du résultat sur le produit de Hadamard et du fait que $1/(1-z)^2$ est de rang 2. □

Exemple 50 : La dérivée de la série de Thue-Morse est 2-régulière de rang 3 et admet la représentation linéaire définie par

$$A_0 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & -4 & -6 \\ 0 & 1 & 1 \end{pmatrix}$$

et

$$\lambda = \begin{pmatrix} -1 & -1 & -1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

en prenant comme base $\mu'(z)$, $S_0\mu'(z)$ et $S_{00}\mu'(z)$. Puisque la série de Thue-Morse est de rang 1, la majoration du rang est cohérente.

4.6 Coefficients des séries B-régulières

Les coefficients des séries rationnelles vérifient des propriétés arithmétiques qui admettent une traduction immédiate pour les séries régulières. Par exemple les séries B-régulières vérifient un critère d'Eisenstein [13, p. 30], qui est à comparer avec celui de la page 41.

Proposition 33. *Soient $\mathbb{A}$ un anneau intègre, $\mathbb{K}$ son corps des fractions et $f \in \mathbb{K}[[z]]$ une série $(\mathbb{K}, B)$-régulière. Il existe un élément non nul $a \in \mathbb{A}$ tel que la série*

$$\sum_{n\geq 0} f_n a^{1+\lambda_B(n)} z^n$$

soit $(\mathbb{A}, B)$-régulière.

Démonstration. Il suffit d'utiliser une représentation linéaire de $f(z)$ et de prendre pour a un multiple commun des dénominateurs des matrices utilisées. □

Le cas le plus utile est celui des séries à coefficients rationnels.

Proposition 34. *Soit $f \in \mathbb{Q}[[z]]$ un série B-régulière. Il existe un entier $a \geq 1$ tel que*

$$a^{1+\lambda_B(n)} f_n \in \mathbb{Z}$$

pour tout entier n. En particulier

$$f_n = 0 \text{ ou } |f_n| > \frac{1}{2a^2 n^{\log_B a}}.$$

Exemple 51 : La série du logarithme

$$\log(1+z) = \sum_{n\geq 1} (-1)^{n+1} \frac{z^n}{n} \in \mathbb{Q}[[z]]$$

n'est pas B-régulière (pour tout B), car il n'y a pas d'entier $a > 0$ tel que

$$n \mid a^{1+\lambda_B(n)}$$

pour tout n.

Cet exemple montre qu'une primitive de série B-régulière n'est généralement pas B-régulière.

Les coefficients d'une série B-régulière ont une croissance polynomiale [6], ce qui correspond à la croissance exponentielle des coefficients d'une série rationnelle [13, p. 30].

Théorème 15. *Soit $f \in \mathbb{C}[[z]]$ une série B-régulière. Il existe un réel α tel que*

$$|f_n| = O(n^\alpha).$$

Démonstration. Il suffit d'utiliser une borne sur les coefficients des matrices d'une représentation linéaire de $f(z)$ pour obtenir une majoration de ce type. □

Exemple 52 : La série régulière

$$f(z) = \prod_{k\geq 0} (1 + a\, z^{B^k})$$

a pour ordre de croissance $\alpha = \ln|a| / \ln B$, ce qui signifie que son coefficient d'indice n est un $O(n^{\alpha+\epsilon})$ pour tout $\epsilon > 0$. Ceci montre que tout réel est l'ordre de croissance d'une série régulière.

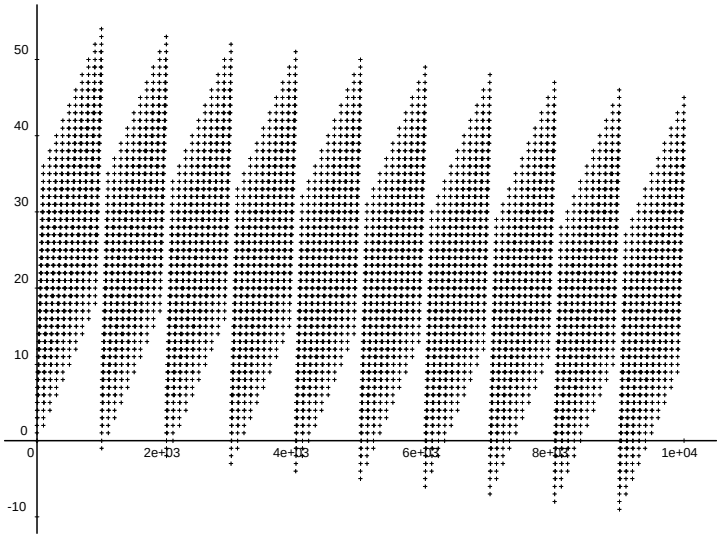

FIG. 4.5
A chaque *preuve par neuf* est associée une suite qui s'exprime par une combinaison $\sum c_k\,\epsilon_k$ des chiffres ϵ_k de l'écriture en base B et toutes ces suites ont un comportement en $\ln n$. Ici est illustrée la preuve par 7 en base 10 exprimée par $s_7(n) = \sum(-1)^i(\epsilon_{3i} + 3\,\epsilon_{3i+1} + 2\,\epsilon_{3i+2})$. Le caractère 1000-régulier de cette suite saute aux yeux.

En ce qui concerne la croissance des coefficients, qui sera reprise au chapitre 7, nous citons pour mémoire le résultat suivant [13, p. 120], qui n'est cependant guère utile en pratique car la majoration est évidente dans les exemples.

Proposition 35. *Si $f(z)$ est une série $(\mathbb{Z}, B)$-régulière admettant une représentation linéaire réduite A_0, …, A_{B-1}, λ, γ, alors*

$$f_n \underset{n\to+\infty}{=} O(\ln^\beta n)$$

pour un certain réel $\beta \geq 0$ si et seulement si l'ensemble des traces de tous les produits de matrices A_r, $0 \leq r < B$, est fini.

EXEMPLE 53 : Il n'est pas difficile de vérifier qu'un entier n est divisible par 7 si et seulement la somme

$$s_7(n) = \sum_{i\geq 0}(-1)^i\epsilon_{3i} + 3\sum_{i\geq 0}(-1)^i\epsilon_{3i+1} + 2\sum_{i\geq 0}(-1)^i\epsilon_{3i+2}$$

est divisible par 7, en notant $\epsilon_\ell \cdots \epsilon_0$ son écriture en base 10.

Evidemment $s_7(1000n + r) = -s_7(n) + s_7(r)$ et $(s_7(n))$ est donc une suite 1000-régulière de rang 2. Une représentation linéaire réduite est donnée par les matrices

$$A_r = \begin{pmatrix} -1 & 0 \\ s_7(r) & 1 \end{pmatrix}, \quad r = 0, \ldots, 999,$$

en prenant comme base $(s_7(n))$ et la suite constante de valeur 1. Il est clair que les traces de tous les produits de A_r ne peuvent prendre comme valeurs que 0 et 2, car ces produits ont pour valeurs propres 1 et ± 1. D'autre part une grossière majoration montre que $s_7(n)$ est plus petit que trois fois la somme des chiffres de n et donc que $3\log_{10} n$. D'ailleurs $s_7(n)$ est semblable à $\log n$ comme on le voit en considérant

les entiers dont l'écriture vérifie $\epsilon_k = 1$ si k est congru à 1, 2 ou 3 modulo 6 et vaut 0 sinon. Il est clair que cette argumentation s'applique à toutes les *preuves par neuf* que l'on peut inventer.

Une série régulière $f(z)$ est directement liée à une série rationnelle S et il est naturel de s'intéresser à l'image commutative $F(t)$ de S. Comme tous les mots de longueur ℓ donnent le même monôme, on l'obtient en sommant la série suivant les intervalles $\left[B^{\ell-1}, B^{\ell}\right[$.

Définition 35. *La série condensée d'une série formelle $f(z) \in \mathbb{A}[[z]]$ est*

$$Kf(t) = f_0 + \sum_{\ell \geq 1} \left(\sum_{B^{\ell-1} \leq n < B^{\ell}} f_n \right) t^{\ell}.$$

L'application K est l'opérateur de condensation.

L'image commutative d'une série rationnelle est rationnelle et cette définition admet un corollaire immédiat.

Proposition 36. *La série condensée d'une série régulière est rationnelle.*

Les propriétés de clôture des séries B-régulières montrent que non seulement $Kf(t)$ est rationnelle si $f(z)$ est régulière, mais aussi

$$\sum_{\ell \geq 1} \left(\sum_{B^{\ell-1}-r \leq n < B^{\ell}-r} f_n \right) t^{\ell}, \quad \sum_{\ell \geq 0} f_{B^{\ell}+r} t^{\ell}, \quad \sum_{\ell \geq 0} \left(\sum_{B^{\ell} \leq n < B^{\ell+1}} \binom{n+m}{m} f_n \right) t^{\ell},$$

par exemple, en utilisant respectivement le produit de Cauchy avec z^r et le produit de Hadamard avec $\displaystyle\sum_{\ell \geq 0} z^{B^{\ell}+r}$ et $\dfrac{1}{(1-z)^{m+1}}$, qui sont des séries régulières.

Exemple 54 : Nous avons déjà vu que la série, dont le coefficient d'indice n est $r_2(n)$, la valeur du miroir de l'écriture binaire de l'entier n,

$$r(z) = \sum_{n \geq 0} r_2(n) z^n$$

est ($\mathbb{Z}$,2)-régulière et qu'une expression rationnelle de la série associée est

$$R = x_1(x_0 + x_1)^* + 2x_1(2(x_0 + x_1))^* x_1(x_0 + x_1)^*.$$

La condensée vaut

$$Kr(t) = t\frac{1}{1-2t} + \frac{2t}{1-4t}\, t\, \frac{1}{1-2t} = \frac{t}{1-4t},$$

ce que l'on peut vérifier facilement en raisonnant directement sur les écritures binaires. D'ailleurs ceci saute aux yeux sur la figure 4.6.

Exemple 55 : La série

$$f(z) = \prod_{k \geq 0} \left(1 + z^{2^k} + z^{2.2^k}\right)$$

$$= 1 + z + 2z^2 + z^3 + 3z^4 + 2z^5 + 3z^6 + z^7 + 4z^8 + 3z^9 + 5z^{10} + 2z^{11} + 5z^{12} + 3z^{13} + 4z^{14} + z^{15} + 5z^{16} + 4z^{17} + \cdots$$

est 2-régulière et une représentation linéaire est donnée par

$$A_0 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

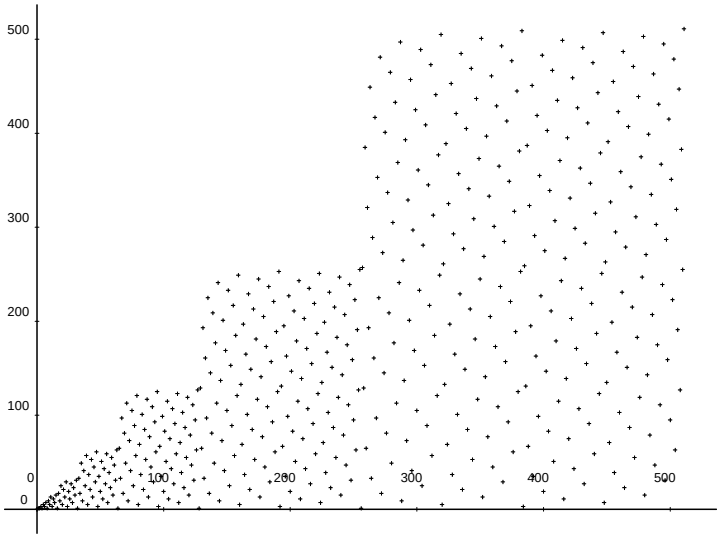

FIG. 4.6
La suite miroir présente un découpage naturel par les puissances de 2. D'une tranche à la suivante l'échelle est multipliée par 2 et la somme des valeurs est multipliée par 4.

$$\gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \lambda = \begin{pmatrix} 1 & 0 \end{pmatrix}.$$

Nous en tirons la série rationnelle associée

$$S = \varepsilon + x_1 \left[\varepsilon + (x_0 + x_1)^* x_0\right] \left[x_0 + x_1 + x_1 (x_0 + x_1)^* x_0\right]^*$$

et la série condensée

$$Kf(t) = 1 + t\left(1 + \frac{t}{1-2t}\right) \frac{1}{1 - (2t + t^2/(1-2t))} = \frac{1-2t}{1-3t} = 1 + \sum_{\ell \geq 1} 3^{\ell-1} t^\ell.$$

Le fait que $Kf(t)$ soit rationnelle quand $f(z)$ est régulière impose une forte contrainte sur le comportement asymptotique des coefficients de la série et on peut utiliser ceci comme on emploie la notion de densité pour les langages ou les séries rationnelles [63, p. 92].

EXEMPLE 56 : Prouvons une fois de plus que la série du logarithme n'est pas B-régulière. La série condensée de

$$\frac{1}{z} \ln \frac{1}{1-z} = \sum_{n \geq 0} \frac{z^n}{n+1}$$

est

$$F(t) = 1 + \sum_{\ell \geq 1} (H_{B^\ell} - H_{B^{\ell-1}}) t^\ell,$$

en notant H_n le n-ième nombre harmonique. L'égalité

$$H_{B^\ell} - H_{B^{\ell-1}} \underset{\ell \to +\infty}{=} \ln B + o(1)$$

et le fait que $\ln B$ est transcendant montre que $F(t)$ n'est pas rationnelle, car l'éventuelle limite de la suite des coefficients d'une fraction rationnelle est algébrique sur le corps de base. *A fortiori* la série de départ n'est pas B-régulière pour tout B.

EXEMPLE 57 : Nous avons rencontré la notion d'autocorrélation d'un mot en liaison avec les équations de Mahler au chapitre 3 (page 43) et nous avons alors montré comment on pouvait calculer à une précision donnée les séries génératrices $f_\gamma(z)$ du nombre de mots d'autocorrélation $10^\ell\gamma$ sur un alphabet de q lettres.

Toute autocorrélation est une écriture binaire d'entiers et on peut donc compacter toutes ces séries génératrices en une seule $k(z) = \sum_{n\geq 0} k_n z^n$, en notant k_n le nombre de mots d'autocorrélation l'écriture binaire de n. Il est peu probable que cette série,

$$k(z) = 1 + qz + q(q-1)z^2 + qz^3 + q^2(q-1)z^4 + q(q-1)z^5 + qz^7$$
$$+ q(q+1)(q-1)^2z^8 + q(q^2+1)z^9 + q(q-1)z^{10} + qz^{15} + q^2(q+1)(q-1)^2z^{16} + \cdots,$$

soit 2-régulière, mais peut-être en est il ainsi de la série caractéristique de son support,

$$c(z) = 1 + z + z^2 + z^3 + z^4 + z^5 + z^7 + z^8 + z^9 + z^{10} + z^{15} + z^{16} + z^{17} + z^{18} + z^{19} + z^{21} + z^{31} + \cdots.$$

Cependant A. Odlyzko et L. Guibas [41, p. 28] ont montré que le nombre d'autocorrélations de longueur ℓ, qui est le coefficient de t^ℓ dans la condensée $Kc(t)$ de la série précédente, a un logarithme semblable à $\ln^2 \ell$ quand ℓ tend vers l'infini, ce qui est incompatible avec le comportement des coefficients d'une série rationnelle. Ainsi $c(z)$ n'est pas 2-régulière.

Proposition 37. *Toute série rationnelle en une indéterminée est la condensée d'une série B-régulière.*

DÉMONSTRATION. Considérons une fraction rationnelle $r(t)$ dont la suite des coefficients est définie par la récurrence minimale [13, chap. 4]

$$r_n + a_1\, r_{n-1} + \cdots + a_N\, r_{n-N} = 0$$

et les conditions initiales $r_0, \ldots, r_{N-1}$. Le n-ième terme de la série vaut $r_n = \lambda C^n \gamma$, en appelant C la matrice compagne

$$C = \begin{pmatrix} & & & -a_N \\ 1 & & & -a_{N-1} \\ & \ddots & & \vdots \\ & & 1 & -a_1 \end{pmatrix},$$

λ la matrice ligne des conditions initiales et γ le premier vecteur de base,

$$\lambda = \begin{pmatrix} r_0 & r_1 & \cdots & r_{N-1} \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Définissons maintenant une série B-régulière par la représentation linéaire dont les matrices carrées sont

$$A_0 = I_N, \quad A_1 = \cdots = A_{B-1} = C,$$

et λ, γ sont donnés ci-dessus. Cette représentation linéaire est évidemment standard et elle est réduite parce que la représentation (λ, C, γ) de $r(t)$ est réduite. Le terme général de la suite B-régulière qu'elle définit est donné par

$$f_n = \lambda\, C^{\lambda(n)-z(n)}\gamma,$$

en notant comme d'habitude $\lambda(n)$ le nombre de chiffres de l'écriture de n en base B et aussi $z(n)$ le nombre de 0 dans cette écriture. La série condensée, $s(t)$, de $f(z)$ a pour terme constant

$$s_0 = f_0 = r_0.$$

Pour $\ell \geq 1$, le coefficient de t^ℓ dans $s(t)$ vaut

$$\sum_{B^{\ell-1} \leq n < B^\ell} r_{\ell - z(n)} = (B-1) \sum_{z=0}^{\ell-1} \binom{\ell-1}{z} r_{\ell-z},$$

parce qu'un nombre dont l'écriture comporte z zéros est constitué d'un chiffre de tête non nul, suivi d'un mot de $\ell - 1$ chiffres parmi lesquels z sont des zéros. La condensée s'exprime donc par

$$\begin{aligned}
s(t) &= r_0 + (B-1) \sum_{\ell \geq 1} t^\ell \sum_{z=0}^{\ell-1} \binom{\ell-1}{z} r_{\ell-z} \\
&= r_0 + (B-1) \sum_{k \geq 1} r_k \sum_{\ell \geq k} \binom{\ell-1}{\ell-k} t^\ell \\
&= r_0 + (B-1) \sum_{k \geq 1} r_k \, t^k \sum_{j \geq 0} \binom{k+j-1}{j} t^j \\
&= r_0 + (B-1) \sum_{k \geq 1} r_k \, \frac{t^k}{(1-t)^k} \\
&= r_0 + (B-1) \left[r\left(\frac{t}{1-t}\right) - r_0 \right] \\
&= r\left(\frac{t}{1-t}\right) - (B-2)\, r_0.
\end{aligned}$$

Inversement la série rationnelle $r(u)$ est fonction de la condensée $s(t)$,

$$r(u) = s\left(\frac{u}{1+u}\right) + (B-2)\, s_0,$$

et ceci montre comment obtenir $s(t)$ comme série condensée. Il suffit de définir $r(u)$ par cette formule et d'utiliser une représentation linéaire réduite de $r(u)$ pour construire une série B-régulière $f(z)$ donnée par une représentation linéaire standard et réduite. □

Une autre idée pour se ramener à des séries rationnelles en une indéterminée consiste à employer comme Ch. Reutenauer les séries [62, p. 72]

$$\sum_{n \geq 0} (S, uw^n v)\, t^n.$$

Dans le contexte des séries régulières, ceci amène à considérer par exemple les séries (correspondant au cas où w est une chaîne de zéros)

$$\sum_{n \geq 0} f_{B^n m + r} t^n.$$

Cependant la rationalité de ces séries extraites ne suffit pas à caractériser la rationalité d'une série et on n'obtient ainsi que des conditions nécessaires de régularité.

Exemple 58 : La série

$$f(z) = \prod_{k \geq 0} \left(1 + (k+1) z^{2^k}\right)$$

n'est pas 2-régulière, car la série traduction de $\sum_{n \geq 0} (S, x_1^n)\, t^n$ vaut

$$\sum_{n \geq 0} f_{2^n - 1} t^n = \sum_{n \geq 0} n!\, t^n$$

et n'est pas rationnelle puisque ses coefficients ont une croissance trop rapide. Le même raisonnement est applicable à toutes les séries

$$f(z) = \prod_{k\geq 0} \left(1 + P(k) z^{B^k}\right),$$

où P est un polynôme non constant. Nous retrouvons par cette méthode une partie de la proposition 26.

Ces résultats ne sont qu'une toute petite approche du comportement asymptotique des coefficients d'une série régulière et nous reprendrons ce sujet dans la troisième partie.

4.7 B-machines et séries B-automatiques

Définition 36. *Les séries B-automatiques sont les séries B-régulières qui ne prennent qu'un nombre fini de valeurs.*

Allouche et Shallit [6, p. 168] ont montré que ce point de vue était équivalent à la définition par substitution due à Cobham [20]. Nous préférons cette définition qui met bien l'accent sur le fait que les séries B-automatiques ne sont que des cas particuliers de séries B-régulières. D'ailleurs elles forment un sous-module du module des séries régulières, qui est de plus stable par produit de Hadamard.

On peut aussi utiliser le point de vue mécaniste ; un B-automate consiste en un ensemble fini $\mathcal{S}$, appelé ensemble des états, dans lequel est distingué un état dit initial, la donnée de B applications de transition δ_r de $\mathcal{S}$ dans lui-même, indexées par les chiffres de l'écriture en base B, et enfin une application de sortie ϕ de $\mathcal{S}$ dans un ensemble $\mathbb{A}$. Ici $\mathbb{A}$ est un anneau commutatif.

La suite (u_n) associée au B-automate est définie comme suit : partant de l'état initial, on applique successivement les transitions δ_{ϵ_0}, δ_{ϵ_1}, …, δ_{ϵ_ℓ}, si l'entier n a pour écriture en base B le mot $\epsilon_\ell \cdots \epsilon_0$ (les poids forts sont à gauche) ; ceci fournit un état s de l'automate et u_n est la valeur sur s de la fonction de sortie ϕ.

La traduction en termes de représentation linéaire est immédiate. La dimension de la représentation est le nombre d'états de l'automate et l'ensemble des indices est l'ensemble des états $\mathcal{S}$. La matrice A_r est la matrice de l'application de transition δ_r, autrement dit $a_{r,s,t} = 1$ si $\delta_r(s) = t$ et 0 sinon. Le vecteur colonne γ donne l'état initial : $\gamma_s = 1$ si s est l'état initial et 0 sinon. Enfin le vecteur ligne λ fournit la fonction de sortie : λ_t est la valeur de ϕ en t. Remarquons cependant que la représentation obtenue n'est pas nécessairement standard.

Exemple 59 : La suite du pliage de papier est définie comme suit [26]. On plie une bande de papier une infinité de fois et toujours dans le même sens. Ensuite on déplie la bande et l'on observe les plis. Ils peuvent être entrants ou sortants et en codant convenablement ces plis par 0 ou 1, on obtient une suite qui commence par 1101100. On peut considérer que 0 et 1 sont les deux éléments de $\mathbb{F}_2$. Cette suite est 2-régulière car elle satisfait la récurrence

$$\begin{cases} u_{4k} &= 1, \\ u_{4k+2} &= 0, \\ u_{2k+1} &= u_k. \end{cases}$$

Cette récurrence donne tout de suite le 2-automate du pliage de papier, représenté sur la figure 4.7. En ordonnant les quatre états par $i < a < b < c$, la représentation linéaire est donnée par

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix},$$

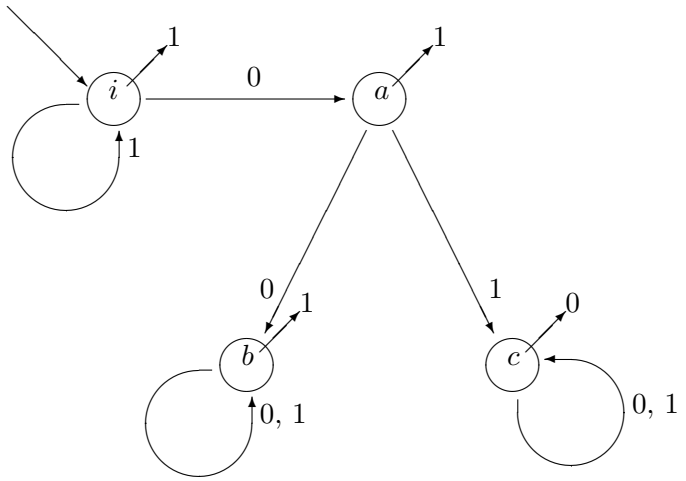

FIG. 4.7
La suite du pliage de papier est 2-automatique. On peut la calculer en utilisant le 2-automate ci-dessus. L'état initial i est indiqué par une flèche entrante. Si l'on cherche la valeur de la suite pour l'entier treize, d'écriture binaire 1101, on passe successivement par les états i, i, a, c et c en suivant les flèches étiquetées 1, 0, 1 et enfin 1. La fonction de sortie donne alors la valeur 0.

$$\lambda = \begin{pmatrix} 1 & 1 & 1 & 0 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Jacob [45] a montré que l'on peut décider si un monoïde de matrices finiment engendré est fini. En particulier on peut décider si une série rationnelle à coefficients dans un corps est d'image finie, c'est-à-dire si ses coefficients sont pris dans un sous-ensemble fini. Il en résulte que l'on peut décider si une série régulière à coefficients dans un corps est automatique. Comme Jacob le fait remarquer le coût est prohibitif si la réponse est négative, mais presque acceptable si la série est automatique.

La preuve de ce théorème est trop longue et technique pour que nous l'exposions ici, mais nous allons expliquer l'idée sous-jacente sur un exemple, dans le cadre des séries régulières et en nous limitant au corps $\mathbb{Q}$, comme Berstel et Reutenauer [13, pp. 113–120]. Le point crucial est le lemme suivant.

Lemme. *Soit $\mathcal{M}$ un monoïde de matrices carrées d'ordre N à coefficients rationnels. On suppose qu'il n'existe pas de sous-espace propre de $\mathbb{Q}^N$ stable par toutes les matrices de ce monoïde et que les valeurs propres des matrices de $\mathcal{M}$ sont nulles ou des racines de l'unité. Alors $\mathcal{M}$ est fini et de cardinal au plus $(2N+1)^{N^2}$.*

EXEMPLE 60 : La série génératrice $u(z)$ de la suite (u_n) définie par la relation de récurrence

$$u_n = -u_{n-3} + u_{\lfloor n/2 \rfloor}$$

et les conditions initiales

$$u_0 = 0, \quad u_1 = 1, \quad u_2 = 2,$$

satisfait l'équation de Mahler

$$(1+z^3)u(z) = (1+z)u(z^2) + z(1+z).$$

Cette équation fournit l'expression

$$u(z) = \sum_{k\geq 0} \frac{1+z}{1+z^3} \cdots \frac{1+z^{2^k}}{1+z^{3.2^k}}\, z^{2^k},$$

ou encore

$$u(z) = (1+z+z^2) \sum_{k,\ell\geq 0} \left(z^{(6\ell+1)2^k} - z^{(6\ell+3)2^k} \right).$$

La série $u(z)$ est donc 2-automatique comme produit d'un polynôme et d'une série 2-automatique. En utilisant sa matrice de Hankel, nous obtenons une représentation réduite de dimension 5

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & -1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Cette représentation est construite en considérant successivement chaque colonne de la matrice comme dans la démonstration du théorème des récurrences typiques (cf. page 84). Partant de l'ensemble vide, nous définissons une base de l'espace engendré par $u(z)$ sous l'action des opérateurs de section, en adjoignant les colonnes qui ne dépendent pas des précédentes et en notant les relations de dépendance rencontrées, ce qui fournit les matrices A_0 et A_1. Pour obtenir une représentation linéaire qui traduit un 2-automate, il suffit de remplacer la dépendance linéaire par l'égalité. Nous trouvons ainsi un 2-automate à treize états,

$$A'_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \end{pmatrix},$$

$$A'_1 = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\
0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 \\
0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0
\end{pmatrix},$$

$$\lambda' = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 0 & 0 & 0 & -1 & -1 \end{pmatrix}, \quad \gamma' = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Pour prouver que la série est 2-automatique en utilisant la première représentation linéaire, nous tenons le raisonnement suivant. Par construction, il n'existe pas de sous-espace propre de $\mathbb{Q}^5$ stable par A_0 et A_1 et donc par toutes les matrices du monoïde engendré. Si la série est 2-automatique, les valeurs propres des matrices de ce monoïde sont nulles ou des racines de l'unité car toute application dans un ensemble fini vérifie des équations de la forme $f^r = f^s$ avec $r < s$ (ici les valeurs propres de A_0 et A_1 sont 0, 1 et -1) ; nous pouvons donc affirmer dans ce cas que le monoïde engendré par A_0 et A_1 ne comporte pas plus de $(2\times 5+1)^{5^2} = 1083470594338837220418302 51$ matrices. Si le monoïde engendré n'était pas fini, l'algorithme proposé par Jacob amènerait à calculer environ ce nombre de matrices pour conclure. Dans le cas positif qui nous occupe, il demanderait cependant moins de calcul car il suffit de trouver le premier entier ℓ tel que tous les produits de A_0 et A_1 de longueur $\ell + 1$ soient des produits de longueur strictement plus petite. Ici ce premier entier, que Jacob appelle la largeur du monoïde par rapport au système générateur, est 6 et le calcul de 124 produits montre que le monoïde contient 38 matrices distinctes.

4.8 Lemme de Fatou

Le lemme de Fatou, classique en théorie des séries rationnelles, se transpose aux séries B-régulières.

Théorème 16. *Si $\mathbb{A}$ est un anneau principal, dont le corps des fractions est $\mathbb{K}$, et $f(z)$ une série $(\mathbb{K}, B)$-régulière de rang N à coefficients dans $\mathbb{A}$, alors $f(z)$ est $(\mathbb{A}, B)$-régulière de rang N.*

Démonstration. Nous transposons la démonstration de [63, p. 30]. Si N est le rang de $f(z)$, on peut trouver N colonnes linéairement indépendantes de la matrice de Hankel de $f(z)$, qui correspondent disons à $S_{u_1} f(z)$, $S_{u_2} f(z)$, …, $S_{u_N} f(z)$. Comme ces colonnes sont indépendantes, on peut choisir certaines lignes,

d'indices i_1, i_2, …, i_N, qui vont donner une matrice K inversible de taille N. Pour un mot w, il existe une relation de dépendance

$$S_w f(z) = \sum_{j=1}^{N} \alpha_j(w)\, S_{u_j} f(z)$$

dans laquelle les $\alpha_j(w)$ sont des éléments de $\mathbb{K}$. En ne retenant que les lignes d'indices i_1, i_2, …, i_N, nous obtenons un système qui détermine les $\alpha_j(w)$,

$$\begin{pmatrix} S_w f_1 \\ S_w f_2 \\ \vdots \\ S_w f_N \end{pmatrix} = K \begin{pmatrix} \alpha_1(w) \\ \alpha_2(w) \\ \vdots \\ \alpha_N(w) \end{pmatrix},$$

puisque K est inversible. Comme les $S_w f_j$ sont des éléments de $\mathbb{A}$, les $\alpha_j(w)$ sont des rationnels qui admettent tous un dénominateur commun, disons d, valable pour tous les w et tous les j, ce d ne dépendant que de la matrice K.

Ainsi le $\mathbb{A}$-module stable engendré par $f(z)$ est inclus dans le $\mathbb{A}$-module libre de base les $1/d\, S_{u_j} f(z)$. Comme l'anneau est principal, un sous-module d'un module libre est libre et le $\mathbb{A}$-module engendré par les sections de $f(z)$ est donc libre et admet une base $g_1(z)$, $g_2(z)$, … ayant a *priori* moins de N éléments. Cependant cette $\mathbb{A}$-base est aussi une $\mathbb{K}$-base et elle comporte donc aussi N éléments. Il ne reste qu'à exprimer les matrices des opérateurs de section dans cette base pour obtenir une représentation linéaire de $f(z)$, dont l'existence montre que $f(z)$ est $(\mathbb{A}, B)$-régulière de rang N. □

La démonstration précédente a l'inconvénient de ne pas être constructive et ce pour deux raisons *a priori*. La première est qu'il n'existe pas de borne pour la recherche d'une sous-matrice K. D'après les relations de récurrence typiques des séries régulières, il y a N colonnes indépendantes parmi les $(B^{N+1}-1)/(B-1)$ premières colonnes de la matrice de Hankel. En effet la partie suffixielle associée à la série contient au pire un mot de longueur N et on peut donc borner le nombre de colonnes à considérer. Par contre il n'y a rien à espérer pour ce qui est des lignes, comme on s'en convainc aisément en multipliant $f(z)$ par une grande puissance de z. La seconde raison tient à la recherche d'une base d'un sous-module d'un module libre sur un anneau principal. Si $\mathcal{M}$ est un module de base e_1, e_2, …, e_k et $\mathcal{N}$ est un sous-module de $\mathcal{M}$, la technique consiste en dernier ressort à considérer les coordonnées sur e_1 des éléments de $\mathcal{N}$; on obtient ainsi des éléments de l'anneau qui forment un idéal et il faut déterminer un générateur de cet idéal. Ceci est généralement impossible parce qu'on ne peut pas considérer tous les éléments de $\mathcal{N}$. En pratique il y a cependant moyen de déterminer un base convenable.

Exemple 61 : Nous avons déjà considéré (cf. page 69) la suite [43] qui à l'entier n, d'écriture binaire $\tilde{n} = 1\epsilon_\ell \cdots \epsilon_1\epsilon_0$, associe le nombre $s_n = \overline{1\epsilon_\ell \cdots \epsilon_1\epsilon_0} + \overline{1\epsilon_\ell \cdots \epsilon_1} + \cdots + \overline{1\epsilon_\ell}$ et nous en avons donné la représentation linéaire

$$A_0 = \begin{pmatrix} 0 & -2 & -2 & -4 \\ 1 & 3 & 2 & 4 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 1 & 3 \\ 0 & 0 & -1 & -3 \\ 1 & 0 & -1/2 & -7/2 \\ 0 & 1 & 3/2 & 9/2 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 0 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Cette représentation a été obtenue en tronquant la matrice de Hankel

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 2 & 3 & 0 & 0 & 2 & 3 & 6 & 7 & 9 & 10 \\
0 & 2 & 3 & 6 & 7 & 9 & 10 & 14 & 15 & 17 & 18 & 21 & 22 & 24 & 25 \\
2 & 6 & 7 & 14 & 15 & 17 & 18 & 30 & 31 & 33 & 34 & 37 & 38 & 40 & 41 \\
3 & 9 & 10 & 21 & 22 & 24 & 25 & 45 & 46 & 48 & 49 & 52 & 53 & 55 & 56 \\
6 & 14 & 15 & 30 & 31 & 33 & 34 & 62 & 63 & 65 & 66 & 69 & 70 & 72 & 73 \\
7 & 17 & 18 & 37 & 38 & 40 & 41 & 77 & 78 & 80 & 81 & 84 & 85 & 87 & 88 \\
9 & 21 & 22 & 45 & 46 & 48 & 49 & 93 & 94 & 96 & 97 & 100 & 101 & 103 & 104 \\
10 & 24 & 25 & 52 & 53 & 55 & 56 & 108 & 109 & 111 & 112 & 115 & 116 & 118 & 119 \\
14 & 30 & 31 & 62 & 63 & 65 & 66 & 126 & 127 & 129 & 130 & 133 & 134 & 136 & 137 \\
15 & 33 & 34 & 69 & 70 & 72 & 73 & 141 & 142 & 144 & 145 & 148 & 149 & 151 & 152 \\
17 & 37 & 38 & 77 & 78 & 80 & 81 & 157 & 158 & 160 & 161 & 164 & 165 & 167 & 168 \\
18 & 40 & 41 & 84 & 85 & 87 & 88 & 172 & 173 & 175 & 176 & 179 & 180 & 182 & 183 \\
21 & 45 & 46 & 93 & 94 & 96 & 97 & 189 & 190 & 192 & 193 & 196 & 197 & 199 & 200 \\
22 & 48 & 49 & 100 & 101 & 103 & 104 & 204 & 205 & 207 & 208 & 211 & 212 & 214 & 215 \\
24 & 52 & 53 & 108 & 109 & 111 & 112 & 220 & 221 & 223 & 224 & 227 & 228 & 230 & 231
\end{pmatrix}$$

à ses 15 premières lignes et en calculant les rangs des sous-matrices allant de la première colonne à la k-ième. On trouve successivement comme valeurs 1, 2, 3, 3, 3, 4, 4, 4, 4, 4, ... Ceci montre que la première, la seconde, la troisième et la sixième colonne sont indépendantes. Ainsi la série génératrice $f(z)$ et ses sections $S_0 f(z)$, $S_1 f(z)$ et $S_{10} f(z)$ sont indépendantes. Nous faisons alors l'hypothèse que la série est de rang 4 et nous calculons les sections des vecteurs de base, ce qui nous donne des relations plausibles et la représentation linéaire indiquée. Les différentes formules de récurrence sont ensuite validées en revenant à la définition de (s_n). L'existence de cette représentation linéaire à coefficients rationnels montre que $f(z)$ est ($\mathbb{Q}$,2)-régulière de rang 4. Cependant $f(z)$ est à coefficients entiers par construction et elle est donc ($\mathbb{Z}$,2)-régulière de rang 4. Nous aimerions en fournir une représentation linéaire à coefficients entiers.

Pour trouver une représentation linéaire à coefficients entiers, nous cherchons d'abord une matrice K adéquate. Evidemment nous nous précipitons sur les colonnes de la matrice de Hankel qui correspondent à la $\mathbb{Q}$-base et nous extrayons les quatre premières lignes, qui ont le bon goût de fournir un mineur non nul,

$$\det K = \begin{vmatrix} 0 & 0 & 0 & 2 \\ 0 & 2 & 3 & 9 \\ 2 & 6 & 7 & 17 \\ 3 & 9 & 10 & 24 \end{vmatrix} = -4.$$

D'après la valeur de ce mineur les quatre séries $g(z) = 1/4\, f(z)$, $g_0(z) = 1/4\, S_0 f(z)$, $g_1(z) = 1/4\, S_1 f(z)$ et $g_{10}(z) = 1/4\, S_{10} f(z)$ engendrent un $\mathbb{Z}$-module qui contient le $\mathbb{Z}$-module stable défini par $f(z)$. Les sections $S_w f(z)$ pour $w = \varepsilon$, 0, 1, ..., 111 s'expriment en fonction de $g(z)$, $g_0(z)$, $g_1(z)$ et $g_{10}(z)$,

$$f(z)\begin{pmatrix} 4 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad S_0 f(z)\begin{pmatrix} 0 \\ 4 \\ 0 \\ 0 \end{pmatrix}, \quad S_1 f(z)\begin{pmatrix} 0 \\ 0 \\ 4 \\ 0 \end{pmatrix},$$

$$S_{00} f(z)\begin{pmatrix} -8 \\ 12 \\ 0 \\ 0 \end{pmatrix}, \quad S_{01} f(z)\begin{pmatrix} -8 \\ 8 \\ 4 \\ 0 \end{pmatrix}, \quad S_{10} f(z)\begin{pmatrix} 0 \\ 0 \\ 0 \\ 4 \end{pmatrix}, \quad S_{11} f(z)\begin{pmatrix} 4 \\ -4 \\ -2 \\ 6 \end{pmatrix},$$

$$S_{000} f(z)\begin{pmatrix} -24 \\ 28 \\ 0 \\ 0 \end{pmatrix}, \quad S_{001} f(z)\begin{pmatrix} -24 \\ 24 \\ 4 \\ 0 \end{pmatrix}, \quad S_{010} f(z)\begin{pmatrix} -16 \\ 16 \\ 0 \\ 4 \end{pmatrix}, \quad S_{011} f(z)\begin{pmatrix} -12 \\ 12 \\ -2 \\ 6 \end{pmatrix},$$

$$S_{100}f(z)\begin{pmatrix}0\\0\\-8\\12\end{pmatrix},\quad S_{101}f(z)\begin{pmatrix}4\\-4\\-10\\14\end{pmatrix},\quad S_{110}f(z)\begin{pmatrix}12\\-12\\-14\\18\end{pmatrix},\quad S_{111}f(z)\begin{pmatrix}16\\-16\\-16\\20\end{pmatrix}.$$

Il est clair que le pgcd des premières coordonnées est 4, ce qui nous amène à prendre comme premier vecteur $f(z)$ elle-même. De même pour le second vecteur nous utilisons $S_0f(z)$. Jusqu'ici il n'y a rien de neuf par rapport à la base qui a fourni la représentation linéaire. Après avoir soustrait à chaque vecteur une combinaison linéaire convenable de $f(z)$ et $S_0f(z)$, nous obtenons des quadruplets qui ont leurs deux premières coordonnées nulles et dont les deux autres coordonnées sont évidentes car $f(z)$ et $S_0f(z)$ ont leurs deux dernières coordonnées nulles. Le pgcd des troisièmes coordonnées est 2 et nous utilisons comme troisième vecteur de base le vecteur $S_{10}f(z) - f(z) - S_0f(z)$, qui réalise la valeur -2. En utilisant la matrice A_1, nous obtenons $-1/2\,S_1f(z) + 3/2\,S_{10}f(z)$ comme expression de ce vecteur dans l'ancienne base. Pour terminer il suffit de prendre $S_{10}f(z)$. Nous avons ainsi la matrice de changement de base

$$P = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&-1/2&0\\0&0&3/2&1\end{pmatrix}$$

et la nouvelle représentation linéaire

$$A'_0 = \begin{pmatrix}0&-2&-5&-4\\1&3&5&4\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad A'_1 = \begin{pmatrix}0&0&4&3\\0&0&-4&-3\\-2&0&10&7\\3&1&-9&-6\end{pmatrix},$$

$$\lambda' = \begin{pmatrix}0&0&3&2\end{pmatrix},\quad \gamma' = \begin{pmatrix}1\\0\\0\\0\end{pmatrix},$$

qui est à coefficients entiers. Pour vérifier la validité de ce résultat, il suffit de comparer les suites définies par ces deux représentations jusqu'au rang $2^8 - 1 = 257$, d'après le théorème d'égalité page 86.

Chapitre 5

Récurrences mahlériennes

Il est bien connu qu'une série B-régulière à coefficients dans un corps fini vérifie une équation de Mahler. En effet une série B-régulière est la premier élément d'une base de l'espace vectoriel stable par B-section qu'elle engendre. Le vecteur $F(z)$ constitué des séries de cette base est solution de l'équation $F(z) = (A_0 + z\,A_1 + \cdots)F(z^B)$, si A_0, A_1, ... sont les matrices qui expriment les opérateurs de section dans cette base. Par élimination, la première composante satisfait une équation de Mahler, disons scalaire. Ce point de vue géométrique règle tout et ne fournit rien. C'est pourquoi nous revenons sur la preuve de ce résultat de deux façons.

D'une part nous rendons effective la preuve qu'en donne Allouche [3, p. 253] et ceci permet de déterminer l'équation de Mahler minimale de la série à une condition près, qui n'a pu être encore levée.

D'autre part une deuxième preuve qui utilise l'arithmétique développée dans la première partie de ce travail, consiste à introduire une classe d'opérateurs, baptisés B-rationnels, et qui sert d'intermédiaire entre les séries rationnelles et les séries B-régulières. Ces opérateurs ont une écriture fractionnaire, comme les séries rationnelles en une indéterminée. Pour celles-ci on en tire classiquement le fait que les coefficients d'une série rationnelle vérifient une récurrence linéaire à coefficients constants. Pour celles-là nous obtenons un résultat similaire qui conduit aux équations de Mahler.

Enfin la première méthode s'étend aux anneaux par un calcul formel, qui pourrait *a priori* être illusoire et ne fournir que l'équation triviale $0 = 0$. En pratique il donne cependant une équation de Mahler non triviale pour toutes les séries B-régulières à coefficients dans un anneau commutatif rencontrées jusqu'ici.

5.1 Equation minimale

Rappelons l'énoncé qui nous occupe ici.

Théorème 17. *Une série B-régulière $f(z)$ de rang N à coefficients dans un corps $\mathbb{K}$ vérifie une équation de Mahler (non triviale) homogène d'ordre au plus N.*

Démonstration. Nous reprenons la démonstration d'Allouche [3]. Soit $g_1(z)$, $g_2(z)$, ..., $g_N(z)$ une base de l'espace vectoriel $\mathcal{S}$ stable par section engendré par $f(z)$. L'écriture

$$g_j(z) = \sum_{0 \le r < B} z^r S_r g_j(z^B)$$

nous montre que les $g_j(z)$ appartiennent à l'espace vectoriel sur $\mathbb{K}(z)$ engendré par les $g_j(z^B)$. Par récurrence, il en résulte que les $g_j(z^{B^k})$, $j = 1 \ldots N$, $k = 0 \ldots N$, sont tous dans l'espace vectoriel sur $\mathbb{K}(z)$ engendré

par les $g_j(z^{B^N})$. Cet espace est de dimension N sur $\mathbb{K}$, car l'opérateur de Mahler est injectif, et donc de dimension au plus N sur $\mathbb{K}(z)$. Les $N+1$ séries $f(z)$, $f(z^B)$, ..., $f(z^{B^N})$, qui sont des combinaisons linéaires à coefficients dans $\mathbb{K}$ des $g_j(z^{B^k})$, sont dans cet espace et vérifient donc une relation de dépendance linéaire à coefficients dans $\mathbb{K}(z)$, c'est-à-dire une équation de Mahler non triviale homogène d'ordre au plus N. □

La connaissance d'une représentation linéaire de la série B-régulière $f(z)$ détermine une équation de Mahler vérifiée par la série en calquant la démonstration que nous venons de rappeler. Précisément nous notons comme d'habitude la représentation A_0, ..., A_{B-1}, λ, γ, ce qui signifie implicitement que le vecteur colonne γ donne les coordonnées de $f(z)$ dans une base $g_1(z)$, ..., $g_N(z)$ de l'espace stable par section engendré par $f(z)$ et $\lambda_j = g_j(0)$ pour $j = 1 \dots N$. L'égalité

$$g_j(z) = \sum_{0 \le r < B} z^r S_r g_j(z^B)$$

indique que les coordonnées de $g_j(z)$ en fonction des $g_k(z^B)$, qui sont des polynômes en z, s'obtiennent en appliquant la matrice

$$U(z) = \sum_{0 \le r < B} z^r A_r$$

au j-ième vecteur de la base canonique de $\mathbb{K}^N$. En particulier $f(z)$ a pour coordonnées $U(z)\gamma$ en fonction des $g_k(z^B)$. A dire vrai l'expression « coordonnées » n'est pas correcte car les $g_j(z^B)$, qui sont $\mathbb{K}$-indépendants, ne sont peut-être pas $\mathbb{K}(z)$-indépendants. En itérant le processus nous voyons que, en fonction des $g_j(z^{B^N})$, la série $f(z^{B^N})$ s'exprime par le vecteur colonne γ, la série $f(z^{B^{N-1}})$ s'exprime par $U(z^{B^{N-1}})\gamma$, ... la série $f(z)$ s'exprime par $U(z^{B^{N-1}}) \cdots U(z)\gamma$. Il suffit d'exhiber une relation de dépendance linéaire entre ces $N+1$ vecteurs colonnes de $\mathbb{K}(z)^N$ pour obtenir une équation de Mahler.

Il est plus pertinent de ne pas considérer d'emblée la famille constituée de $U(z^{B^{N-1}}) \cdots U(z)\gamma$, ..., $U(z^{B^{N-1}})\gamma$ et γ, mais plutôt successivement les familles (γ), puis $(U(z)\gamma, \gamma)$, ...jusqu'à la famille complète $(U(z^{B^{N-1}}) \cdots U(z)\gamma, \dots, U(z^{B^{N-1}})\gamma, \gamma)$ en cherchant la première qui donne une relation de dépendance non triviale.

Proposition 38. *L'algorithme* `équation_de_mahler` *appliqué à une représentation linéaire de dimension N fournit explicitement une équation de Mahler à coefficients polynomiaux comme annoncée dans le théorème précédent. Cette équation*

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = 0$$

a des coefficients $c_k(z)$ nuls ou de degré inférieur à $NB^N/(B-1)^2$.

Démonstration. Nous venons d'exposer comment procéder. La majoration des degrés résulte simplement des formules de Cramer. □

Exemple 62 : Considérons la suite $(c(n))_{n\ge 0}$ des entiers naturels dont l'écriture en base 3 ne comporte pas le chiffre 1, rangés dans l'ordre croissant. On peut dire que les $c(n)$ fournissent les numérateurs des extrémités gauches de l'ensemble triadique de Cantor [6, p. 186]. Cette série est ($\mathbb{Z}$,2)-régulière et en utilisant les techniques du chapitre 4, nous trouvons une représentation linéaire réduite correspondant à la base $c(z)$, $S_1c(z)$ du $\mathbb{Z}$-module stable et donnée par

$$A_0 = \begin{pmatrix} 3 & 6 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & -3 \\ 1 & 4 \end{pmatrix},$$

Algorithme `équation_de_mahler`

Entrée : une représentation linéaire $A_0, \ldots, A_{B-1}$, λ, γ de la série $(\mathbb{K}, B)$-régulière $f(z)$

Sortie : une équation de Mahler linéaire non triviale vérifiée par $f(z)$

1. poser $v_0 = \gamma$ et $\mathcal{F} = \{\gamma\}$;
2. poser $U(z) = \sum_{0 \le r < B} z^r A_r$;
3. pour k de 1 à N tant que $\mathcal{F}$ est une famille libre faire
   (a) substituer z^B à z dans tous les éléments de $\mathcal{F}$;
   (b) augmenter $\mathcal{F}$ de l'élément $v_k = U(z^{B^k})U(z^{B^{k-1}}) \cdots U(z)\gamma$;
4. exhiber une relation de dépendance linéaire $c_m v_0 + c_{m-1} v_1 + \ldots + c_0 v_m = 0$ entre les éléments de $\mathcal{F} = \{v_0, v_1, \ldots, v_m\}$,
5. renvoyer l'équation $c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_m(z)f(z^{B^m}) = 0$;

fin.

FIG. 5.1
L'algorithme `équation_de_mahler` calcule une équation de Mahler satisfaite par une série B-régulière donnée par une représentation linéaire.

$$\lambda = \begin{pmatrix} 0 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Pour appliquer l'algorithme, nous introduisons d'abord

$$U(z) = A_0 + z\,A_1 = \begin{pmatrix} 3 & 6-3z \\ z & 1+4z \end{pmatrix}$$

et nous considérons

$$\gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad U(z)\gamma = \begin{pmatrix} 3 \\ z \end{pmatrix}.$$

La matrice

$$\begin{pmatrix} 1 & 3 \\ 0 & z \end{pmatrix}$$

est de rang 2 et ne fournit pas d'équation. Nous calculons alors

$$U(z^2)U(z) = \begin{pmatrix} 9+6z-3z^3 & 24+15z-3z^2-12z^3 \\ z+3z^2+4z^3 & 1+4z+10z^2+13z^3 \end{pmatrix}$$

et nous formons la matrice dont les vecteurs colonnes sont γ, $U(z^2)\gamma$ et $U(z^2)U(z)\gamma$,

$$\begin{pmatrix} 1 & 3 & 9+6z-3z^3 \\ 0 & z^2 & z+3z^2+4z^3 \end{pmatrix}.$$

Évidemment les colonnes vérifient une relation de dépendance essentiellement unique, dont les coefficients sont dans l'ordre $3+6z^2+3z^4$, $-(1+3z+4z^2)$ et z. Ainsi $c(z)$ vérifie l'équation

$$zc(z) - (1+3z+4z^2)c(z^2) + 3(1+z)^2 c(z^4) = 0.$$

Numériquement, cette équation permet de calculer les premiers termes de la série,

$$c(z) = 2z + 6z^2 + 8z^3 + 18z^4 + 20z^5 + 24z^6 + 26z^7 + 54z^8 + 56z^9 + 60z^{10} + 62z^{11} + 72z^{12} + \cdots.$$

Il n'y a pas de raison que l'équation obtenue soit d'ordre exactement N, même avec une représentation réduite.

EXEMPLE 63 : Prenons la série ($\mathbb{Z}$,2)-régulière qui admet la représentation linéaire

$$A_0 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Nous obtenons l'équation

$$z\left(2\,z^4 - z^2 + 1\right) f(z) + \left(-4\,z^6 - z^5 + z^3 - 3\,z^2 - 1\right) f(z^2) + \left(2\,z^2 - z + 1\right)\left(1 + z^2\right)\left(z^4 + 1\right) f(z^4) = 0$$

dont les solutions sont données par

$$f(z) = t_1 + t_2\,z + t_1\,z^2 + (3\,t_2 - 2\,t_1)\,z^3 + t_1\,z^4 + t_2\,z^5 + (2\,t_2 - t_1)\,z^6 + (5\,t_2 - 4\,t_1)\,z^7 + t_1\,z^8 + t_2\,z^9 + t_1\,z^{10} + \cdots$$

et forment un espace de dimension 2. L'équation est d'ordre 2 alors que la série est de rang 3.

Comme nous l'avons déjà signalé, le fait que les $g_j(z^B)$ puissent être $\mathbb{K}(z)$-dépendants pose problème. Si nous prenons la série qui donne le nombre de coefficients impairs dans la n-ième ligne du triangle de Pascal [66]

$$I(z) = \prod_{k \geq 0} \left(1 + 2\,z^{2^k}\right)$$

et la série, disons complémentaire,

$$P(z) = \frac{1}{(1-z)^2} - I(z),$$

les méthodes usuelles fournissent une représentation linéaire réduite de dimension 3 pour $P(z)$,

$$A_0 = \begin{pmatrix} 0 & -2 & -4 \\ 1 & 3 & 4 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Ici

$$g_1(z) = P(z) = \frac{1}{(1-z)^2} - I(z),$$

$$g_2(z) = S_0 P(z) = \frac{1+z}{(1-z)^2} - I(z)$$

et

$$g_3(z) = S_{10} P(z) = \frac{3+z}{(1-z)^2} - 2\,I(z).$$

Ces trois séries sont indépendantes sur $\mathbb{Q}$, mais leur rang sur $\mathbb{Q}(z)$ ne vaut que 2. Du coup l'algorithme ne fournit pas l'équation minimale de $P(z)$, comme on pouvait l'espérer, mais un multiple de celle-ci. L'équation minimale, ppcm des opérateurs minimaux pour $1/(1-z)^2$ et $I(z)$, est

$$z^2P(z) - [(1+z^2)^2 + z^2(1+2z)]P(z^2) + (1+z^2)^2(1+2z^2)P(z^4) = 0$$

alors que l'algorithme donne

$$z^2P(z) - \left(3\,z^2 - z + 1\right)\left(z^2 + z + 1\right)P(z^2)$$

$$+ \left(4\,z^2 + 11\,z^4 + 2\,z^8 + 6\,z^6 + 3\right)P(z^4) - 2\,\left(2\,z^4 + 1\right)\left(1 + z^4\right)^2 P(z^8) = 0.$$

On passe de l'une à l'autre en multipliant à gauche par $1 - 2\,M$.

Remarquons que s'il y une relation de dépendance entre les $g_j(z^{B^k})$ (k fixé) avec des coefficients dans $\mathbb{K}(z)$, il y en a aussi une entre les $g_j(z)$. La même astuce que pour les équations de Mahler le fait voir : l'application d'un opérateur de section, ou plutôt de tous les S_w avec w de longueur k, fournit au moins une relation de dépendance non triviale entre les $g_j(z)$.

Il faudrait donc ajouter dans l'algorithme un point 0. pour tester l'indépendance linéaire des $g_j(z)$ sur $\mathbb{K}(z)$. Cependant nous n'apercevons pas de procédure effective pour étudier cette indépendance et ceci explique l'apparition de l'hypothèse (H) dans l'énoncé suivant.

Hypothèse. *Soit $f(z)$ une série $(\mathbb{K}, B)$régulière de rang N. Nous disons que $f(z)$ satisfait l'hypothèse (H) si le sous-espace stable par section engendré par $f(z)$ a même dimension sur $\mathbb{K}(z)$ que sur $\mathbb{K}$.*

Proposition 39. *Soit $f(z)$ une série $(\mathbb{K}, B)$-régulière de rang N.*

1. L'algorithme `équation_de_mahler` *appliqué à toute représentation linéaire réduite de $f(z)$ fournit la même équation $E(z, M)f(z) = 0$.*

2. L'équation $E(z, M)h(z) = 0$ est l'équation minimale de $f(z)$, si l'hypothèse (H) est vérifiée.

3. Pour une représentation linéaire réduite et standard A_r, $0 \leq r < B$, λ, γ donnée, toutes les séries B-régulières éléments de l'espace $\mathcal{K}$ obtenu en faisant varier ${}^t\lambda$ dans $\mathrm{Ker}\,({}^tA_0 - I_N)$ sont solutions de cette équation.

4. Si $f(z)$ vérifie une équation de Mahler linéaire alors tous les éléments de $\mathcal{K}$ vérifient cette équation.

5. Dans l'hypothèse (H), l'équation $E(z, M)h(z) = 0$ est minimale pour l'espace $\mathcal{K}$, ce qui signifie que tout opérateur $P(z, M)$ qui s'annule sur $\mathcal{K}$ est multiple de $E(z, M)$.

Démonstration. D'après un théorème de M.-P. Schützenberger [13, p.38], deux représentations linéaires réduites sont semblables et les deux familles de vecteurs associées à ces représentations par l'algorithme se déduisent l'une de l'autre par un automorphisme linéaire et vérifient donc la même relation de dépendance.

Si $f(z)$ vérifie une équation $P(z, M)f(z) = 0$ d'ordre K, les $f(z^{B^k})$ s'expriment en fonction des $g_j(z^{B^K})$ par les vecteurs colonnes $U(z^{B^{K-1}}) \cdots U(z^{B^k})\gamma$ et l'équation se traduit en une relation de dépendance entre ces vecteurs. Celle que nous avons construite est la première de ce type donc $N \leq K$. Nous venons d'utiliser le fait que N est le rang de $f(z)$, car les $g_j(z^{B^K})$ forment une famille libre, ce qui garantit l'unicité de l'écriture.

Par construction l'équation obtenue ne dépend pas de λ, donc toutes les séries régulières obtenues en faisant varier λ vérifient cette équation.

L'équation $E(z, M)h(z) = 0$ est minimale pour $\mathcal{K}$ puisqu'elle est minimale pour $f(z)$ qui est élément de $\mathcal{K}$. □

Il semble que l'espace $\mathcal{S}$ des solutions de l'équation minimale de $f(z)$, disons $E(z, M)h(z) = 0$, soit exactement $\mathcal{K}$, mais nous n'avons pas trouvé de démonstration de ce fait.

EXEMPLE 64 : La série 2-régulière de rang 3,

$$f(z) = z + z^2 + 2\,z^3 + z^4 + 5\,z^5 + 2\,z^6 + 7\,z^7 + z^8 + 9\,z^9 + 5\,z^{10} + \cdots,$$

définie par la représentation linéaire réduite

$$A_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

a pour équation minimale

$$z^3 h(z) + z^2\left(2\,z^4 - 2\,z^2 - z - 2\right) h(z^2) - \left(4\,z^8 + 5\,z^6 + z^4 - 2\,z^2 - 1\right) h(z^4) + \left(4\,z^8 + 2\,z^4 - 1 - 6\,z^{12}\right) h(z^8) = 0.$$

L'espace des solutions de celle-ci est de dimension 1, ce qui est bien la dimension du sous-espace $\mathcal{K}$ des séries ($\mathbb{Q}$,2)-régulières obtenues en faisant varier ${}^t\lambda$ dans la droite propre de ${}^tA_0$ relative à la valeur propre triple 1.

EXEMPLE 65 : Le nombre de facteurs de longueur donnée de la suite de Thue-Morse [16, 25] a une série génératrice,

$$f(z) = 2\,z + 4\,z^2 + 6\,z^3 + 6\,z^4 + 8\,z^5 + 10\,z^6 + 12\,z^7 + 12\,z^8 + \cdots,$$

qui est ($\mathbb{Z}$,2)-régulière de rang 5 et admet la représentation linéaire

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & -2 & -2 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 3 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & -2 \\ 0 & 0 & 1 & 1 & 7 \\ 1 & 0 & -1 & -1 & -2 \\ 0 & 0 & -1 & -1 & -5 \\ 0 & 1 & 2 & 3 & 5 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 1 & 1 & 2 & 1 & 4 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

La matrice ${}^tA_0$ admet les valeurs propres 0, 1 et 2 de multiplicités respectives 1, 3 et 1. Le sous-espace propre relatif à 1 est de dimension 3, engendré par

$$e_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

et ${}^t\lambda = e_1 + 2\,e_2 + 4\,e_3$. L'espace $\mathcal{K}$ est donc engendré par $f(z)$ et

$$g(z) = 1 - z^2 - 2\,z^3 - z^4 - 2\,z^5 - 3\,z^6 - 4\,z^7 - 3\,z^8 + \cdots$$

qui sont associées à ces deux vecteurs propres. L'équation minimale de $f(z)$ est

$$z\left(2\,z^6-2\,z^4+2\,z^2-1\right)\left(z^2-z+1\right)h(z)$$
$$+\left(-2\,z^{11}-2\,z^{10}-2\,z^9+4\,z^8-4\,z^7-4\,z^6+3\,z^5+3\,z^4-6\,z^3+z^2+z+1\right)h(z^2)$$
$$+\left(4\,z^{13}-4\,z^{12}+8\,z^{11}-4\,z^{10}+4\,z^9+4\,z^7-4\,z^6+8\,z^5-5\,z^4+8\,z^3-6\,z^2+4\,z-3\right)h(z^4)$$
$$-2\,\left(2\,z^3-2\,z^2+2\,z-1\right)\left(z^4+1\right)^2h(z^8)=0$$

et les solutions, données par

$$h(z)=t_1+t_2\,z+(2\,t_2-t_1)\,z^2+(3\,t_2-2\,t_1)\,z^3+(3\,t_2-t_1)\,z^4+(4\,t_2-2\,t_1)\,z^5+(5\,t_2-3\,t_1)\,z^6+\cdots,$$

forment un espace de dimension 2, qui est exactement l'espace $\mathcal{K}$.

Exemple 66 : La série

$$f(z)=1+\sum_{k\geq 0}z^{2^k}\prod_{0\leq\ell<k}\left(1+3z^{2^\ell}\right)$$

est 2-régulière de rang 2 et admet la représentation linéaire

$$A_0=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad A_1=\begin{pmatrix}0&0\\1&3\end{pmatrix},$$

$$\lambda=\begin{pmatrix}1&1\end{pmatrix},\quad \gamma=\begin{pmatrix}1\\0\end{pmatrix}.$$

L'algorithme fournit l'équation

$$zh(z)-(1+z+3z^2)h(z^2)+(1+3z^2)h(z^4)=0,$$

dont l'espace des solutions est de dimension 2 engendré par 1 et $f(z)$. Evidemment 1 vérifie l'équation $h(z)-h(z^2)=0$. D'ailleurs l'opérateur minimal de $f(z)$,

$$z-(1+z+3z^2)M+(1+3z^2)M^2$$

se factorise en

$$[z-(1+3z^2)M][1-M].$$

Nous voyons que l'équation minimale d'un élément de $\mathcal{K}$ n'est pas nécessairement $E(z,M)h(z)=0$.

5.2 Opérateurs B-rationnels

Nous reprenons maintenant le lien entre séries B-régulières et équation de Mahler par une autre voie, en introduisant une algèbre d'opérateurs $\mathbb{A}[[z,M]]$ et une sous-algèbre naturelle de celle-ci, constituée des opérateurs B-rationnels. Cette sous-algèbre explique bien l'apparition de l'opérateur de Mahler dans l'étude des séries B-régulières.

5.2.1 Algèbre des séries en z et M

Considérons une série

$$\sum_{k\geq 0}c_k(z)M^k,$$

dans laquelle les c_k sont des séries formelles à coefficients dans $\mathbb{A}$. Si f est une série formelle de valuation $\omega_z(f)$ strictement positive, la série

$$\sum_{k\geq 0} c_k(z) f(z^{B^k})$$

converge dans $\mathbb{A}[[z]]$ car le terme d'indice k a une valuation supérieure à $B^k\omega_z(f)$. La série proposée définit donc un opérateur linéaire F sur $z\mathbb{A}[[z]]$. Si de plus la série

$$\sum_{k\geq 0} c_k(z)$$

converge dans $\mathbb{A}[[z]]$, alors en écrivant $f = f(0) + g(z)$ avec $\omega_z(g) > 0$ pour $f \in \mathbb{A}[[z]]$, nous avons pour tout K

$$\sum_{k=0}^{K} c_k(z) M^k f = f(0) \sum_{k=0}^{K} c_k(z) + \sum_{k=0}^{K} c_k(z) M^k g$$

ce qui montre que la série donnée converge en f. Ainsi F est défini sur $\mathbb{A}[[z]]$. Inversement si F est défini sur $\mathbb{A}[[z]]$, en appliquant F à 1, nous voyons que la série

$$\sum_{k\geq 0} c_k(z)$$

est convergente.

Proposition 40. *Soit $(c_k)_{k\in\mathbf{N}}$ une suite de séries formelles. La série*

$$\sum_{k\geq 0} c_k(z) M^k$$

converge simplement sur $z\mathbb{A}[[z]]$. Elle converge simplement sur $\mathbb{A}[[z]]$ si et seulement si la série

$$\sum_{k\geq 0} c_k(z)$$

est convergente dans $\mathbb{A}[[z]]$.

Proposition 41. *Il y a unicité de l'écriture d'un opérateur linéaire de $z\mathbb{A}[[z]]$ sous la forme*

$$\sum_{k\geq 0} c_k(z) M^k.$$

Démonstration. Supposons que

$$\sum_{k\geq 0} c_k(z) M^k = 0.$$

L'application de cet opérateur à z^n avec $n \geq 1$ donne l'égalité

$$\sum_{k\geq 0} c_k(z) z^{B^k n} = 0,$$

ce qui montre que les coefficients de c_0 d'indice strictement plus petit que Bn sont nuls. Comme n peut être choisi aussi grand que l'on veut, c_0 est nul. En recommençant le raisonnement on conclut que tous les c_k sont nuls. □

Il n'est pas difficile de voir que les opérateurs sommes des séries que nous étudions forment une sous-algèbre de $\mathrm{End}_{\mathbb{A}}(z\mathbb{A}[[z]])$. De plus l'unicité de l'écriture permet de parler de la valuation (par rapport à M) d'un tel opérateur.

Définition 37. *La sous-algèbre de* $\mathrm{End}_{\mathbb{A}}(z\mathbb{A}[[z]])$ *constituée des opérateurs sommes des séries*

$$\sum_{k\geq 0} c_k(z)M^k.$$

sera notée $\mathbb{A}[[z,M]]$.

La valuation, $\omega_M(F) \in [0,+\infty]$*, d'un* $F \in \mathbb{A}[[z,M]]$ *est le premier indice* k *tel que* $c_k \neq 0$.

Cette notation $\mathbb{A}[[z,M]]$ n'est pas standard parce que M n'est pas une indéterminée mais elle ne pose pas de problème grâce à l'unicité de l'écriture. La définition de $\mathbb{A}[[z,M]]$ étant posée, il ne nous reste plus qu'à dérouler les propriétés comme on le fait classiquement pour l'algèbre des séries formelles. Avec la notion de valuation, nous obtenons l'énoncé classique sur l'intégrité.

Proposition 42. *Si* $\mathbb{A}$ *est intègre, l'algèbre* $\mathbb{A}[[z,M]]$ *est sans diviseurs de 0.*

Etudions la convergence des séries dans $\mathbb{A}[[z,M]]$.

Proposition 43. *Soit*

$$\sum_{n\geq 0} U_n$$

une série à termes dans $\mathbb{A}[[z,M]]$*. La série converge simplement sur* $z\mathbb{A}[[z]]$ *si et seulement si la série*

$$\sum_{n\geq 0} U_n z$$

converge dans $\mathbb{A}[[z]]$*. C'est en particulier le cas si la suite*

$$(\omega_M(U_n))_{n\geq 0}$$

tend vers l'infini avec n.

La série converge simplement sur $\mathbb{A}[[z]]$ *si et seulement si la série*

$$\sum_{n\geq 0} U_n 1$$

converge dans $\mathbb{A}[[z]]$.

Démonstration. Supposons la condition vérifié et soit $f \in \mathbb{A}[[z]]$ de valuation $\omega_z(f)$ strictement positive. Le fait que

$$\sum_{n\geq 0} U_n f(z)$$

converge se traduit par

$$\lim_{n\to+\infty} \omega_z(U_n f) = +\infty.$$

L'inégalité

$$\omega_z(U_n f) \geq \omega_z(U_n z),$$

donne l'équivalence de l'énoncé, puisque la convergence doit en particulier être vérifiée sur z. La condition suffisante est évidente grâce à l'inégalité

$$\omega_z(U_n z) \geq B^{\omega_M(U_n)}.$$

Le second cas est aussi simple. □

EXEMPLE 67 : La série

$$\sum_{n\geq 0} M^n$$

converge sur $z\mathbb{A}[[z]]$, mais pas sur $\mathbb{A}[[z]]$. Sa somme est un opérateur F défini sur $z\mathbb{A}[[z]]$ et A est l'inverse de $1-M$. Plus précisément $1-M$ est défini sur $\mathbb{A}[[z]]$ et la série fournit son inverse à gauche, $(1-M)^{-1}$, d'après les égalités

$$\left(\sum_{n\geq 0} M^n\right)(1-M)f = f \quad \text{pour} \quad f \in \mathbb{A}[[z]],$$

$$(1-M)\left(\sum_{n\geq 0} M^n\right)f = f \quad \text{pour} \quad f \in z\mathbb{A}[[z]].$$

EXEMPLE 68 : L'opérateur

$$A = zM\sum_{n\geq 0} M^n$$

vérifie

$$1-A = 1-zM[1-M]^{-1} = [1-(1+z)M][1-M]^{-1};$$

la série

$$\sum_{n\geq 0}[(1+z)M]^n = \sum_{n\geq 0}(1+z)\cdots(1+z^{B^{n-1}})M^n$$

converge sur $z\mathbb{A}[[z]]$ et $1-(1+z)M$ est inversible sur $z\mathbb{A}[[z]]$, mais pas sur $\mathbb{A}[[z]]$ puisque

$$[1-(1+z)M]\prod_{n\geq 0}\left(1+z^{B^n}\right) = 0,$$

et

$$\begin{aligned}(1-A)^{-1} &= [1-M][1-(1+z)M]^{-1}\\ &= [1-M]\textstyle\sum_{n\geq 0}(1+z)\cdots(1+z^{B^{n-1}})M^n\\ &= 1+\textstyle\sum_{n\geq 1} z(1+z^B)\cdots(1+z^{B^{n-1}})M^n.\end{aligned}$$

Définition 38. *Un $F \in \mathbb{A}[[z,M]]$ est quasi-inversible s'il est somme d'une série $\displaystyle\sum_{k\geq 1} c_k(z)M^k$ telle que*

1. *la série $\displaystyle\sum_{k\geq 1} c_k(z)$ converge ;*
2. *$c_k(0) = 0$ pour tout $k \geq 1$.*

Proposition 44. *Les opérateurs quasi-inversibles forment un idéal à gauche de $\mathbb{A}[[z,M]]$.*

DÉMONSTRATION. En effet par multiplication à gauche, les valuations des coefficients augmentent. □

Proposition 45. *Si A est quasi-inversible, il est défini sur tout $\mathbb{A}[[z]]$, l'opérateur $1-A$ est inversible, la série*

$$\sum_{n\geq 0} A^n$$

converge simplement sur $\mathbb{A}[[z]]$ et sa somme est l'inverse de $1-A$.

DÉMONSTRATION. Le fait que A soit partout défini résulte de la condition sur la convergence de la série des coefficients. D'autre part A a une valuation plus grande que 1, et A^n a donc une valuation plus grande que n, ce qui assure la convergence de la série géométrique $\sum_{n\geq 0} A^n$ sur $z\mathbb{A}[[z]]$. La condition sur les valuations des $c_k(z)$ montre qu'il y aussi convergence sur $\mathbb{A}[[z]]$. □

EXEMPLE 69 : L'opérateur $A = (z + \cdots + z^{B-1})M$ est quasi-inversible. De

$$[1 - A]\frac{1}{1-z} = \frac{1}{1-z} - \frac{z + \cdots + z^{B-1}}{1 - z^B} = \frac{1}{1 - z^B},$$

nous tirons

$$\frac{1}{1-z} = \sum_{n\geq 0}[(z + \cdots + z^{B-1})M]^n \frac{1}{1 - z^B}$$

c'est-à-dire

$$\frac{1}{1-z} = \sum_{n\geq 0}(z + \cdots + z^{B-1})(z^B + \cdots + z^{B(B-1)}) \cdots (z^{B^{n-1}} + \cdots + z^{B^{n-1}(B-1)})\frac{1}{1 - z^{B^{n+1}}},$$

ce qui exprime la classification des entiers naturels suivant le rang, n, du 0 de plus faible poids dans leur écriture en base B.

EXEMPLE 70 : Nous avons vu que la résolution d'une équation de Mahler

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z),$$

avec $c_0(z) \neq 0$, se ramène quand il y a des solutions à une équation disons réduite

$$C_0(z)F(z) + z^{\lambda_1}C_k(z)F(z^B) + \cdots + z^{\lambda_N}F(z^{B^N}) = E(z)$$

et à l'application d'un opérateur contractant. Une autre façon d'énoncer ceci est de remarquer que l'équation réduite s'écrit

$$\left[1 + z^{\lambda_1}\frac{C_k(z)}{C_0(z)}M + \cdots + z^{\lambda_N}\frac{C_N(z)}{C_0(z)}M^N\right]F(z) = \frac{B(z)}{C_0(z)},$$

ce qui fournit la solution sous la forme

$$F(z) = \left[1 + z^{\lambda_1}\frac{C_k(z)}{C_0(z)}M + \cdots + z^{\lambda_N}\frac{C_N(z)}{C_0(z)}M^N\right]^{-1}\frac{B(z)}{C_0(z)}$$

car l'opérateur

$$z^{\lambda_1}\frac{C_k(z)}{C_0(z)}M + \cdots + z^{\lambda_N}\frac{C_N(z)}{C_0(z)}M^N$$

est quasi-inversible. En effet c'est un polynôme en M et les λ_k sont strictement positifs.

5.2.2 Opérateurs B-rationnels

La sous-algèbre qui nous intéresse s'obtient en traduisant les séries rationnelles en opérateurs via la numération en base B. En appliquant les opérateurs ainsi définis à des polynômes, nous retrouverons les séries B-régulières.

Définition 39. *Nous notons $\overline{\sigma}$ l'application linéaire de $A\langle\langle\mathcal{X}\rangle\rangle$ dans $\mathbb{A}[[z, M]]$ définie comme suit :*

$$\overline{\sigma}x_r = z^r M, \quad 0 \leq r < B,$$

$$\overline{\sigma}uv = \overline{\sigma}v\ \overline{\sigma}u \quad \text{pour } u, v \in \mathcal{X}^*.$$

et, si $S \in A\langle\langle\mathcal{X}\rangle\rangle$,

$$\overline{\sigma}S(z, M) = \sum_{w\in\mathcal{X}^*}(S, w)\overline{\sigma}w.$$

La définition est correcte car cette dernière série est convergente dans $\mathbb{A}[[z, M]]$ et définit un opérateur sur $z\mathbb{A}[[z]]$. Remarquez que $\overline{\sigma}$ est un antihomomorphisme (dans la deuxième égalité, il y a transposition de u et v) ; c'est un choix arbitraire. Il tient à ce que, dans l'écriture en base B des entiers naturels, nous considérons que le premier chiffre est le chiffre de poids faible. Un exemple fera vite comprendre l'intérêt de $\overline{\sigma}$ dans le contexte qui nous occupe.

Exemple 71 : Si w est le développement binaire de l'entier dix-huit : $w = \widetilde{18} = 10010$, ce que nous préférons écrire $w = x_1x_0x_0x_1x_0$, nous obtenons l'opérateur $M\,zM\,M\,M\,zM$ et la relation $Mz = z^2M$ donne successivement

$$\begin{array}{rcl} \overline{\sigma}w & = & M\,zM\,M\,M\,zM \\ & = & M\,zM\,M\,z^2M\,M \\ & = & \cdots \\ & = & z^{18}M\,M\,M\,M\,M \end{array}$$

Ce phénomène est général et

$$\overline{\sigma}w = z^{\bar{w}}\,M^{|w|},$$

en notant, rappelons le, $\bar{w}$ la valeur du mot w dans la base B et $|w|$ sa longueur.

Proposition 46. *Les $\overline{\sigma}S$ avec $S \in A\langle\langle\mathcal{X}\rangle\rangle$ sont exactement les*

$$\sum_{k\geq 0} c_k(z)M^k \quad \textit{avec}\ \ c_k = 0\ \ \textit{ou}\ \ \deg c_k < B^k.$$

Démonstration. En effet un mot

$$w = x_{r_{k-1}} \cdots x_{r_0}$$

donne par $\overline{\sigma}$ le terme

$$\overline{\sigma}w = z^{r_0 + r_1B + \cdots + r_{k-1}B^{k-1}}M^k$$

et inversement en décomposant l'exposant de z en base B on retrouve le mot $w \in \mathcal{X}^*$. L'unicité de l'écriture en base B et l'unicité de l'écriture dans $\mathbb{A}[[z, M]]$ montrent qu'un $F \in \mathbb{A}[[z, M]]$ a au plus un antécédent $S \in A\langle\langle\mathcal{X}\rangle\rangle$ par $\overline{\sigma}$. □

Théorème 18. *L'application linéaire $\overline{\sigma}$ induit un isomorphisme de $A\langle\langle\mathcal{X}\rangle\rangle$ sur son image.*

Parmi tous les opérateurs de $\mathbb{A}[[z, M]]$ nous n'utiliserons que les images des séries rationnelles.

Définition 40. *Un opérateur $F \in \mathrm{End}_{\mathbb{A}}(\mathbb{A}[[z]])$ est $(\mathbb{A}, B)$-rationnel s'il est l'image par $\overline{\sigma}$ d'une série rationnelle $S \in A^{\mathrm{rat}}\langle\langle\mathcal{X}\rangle\rangle$.*

Regardons quelques opérateurs $(\mathbb{Z}, B)$-rationnels, images de séries $\mathbb{Z}$-rationnelles rencontrées dans la littérature.

Exemple 72 : Si

$$S = \sum_{w\in\varepsilon+\mathcal{X}_+\mathcal{X}^*} \bar{w}w,$$

son image par $\overline{\sigma}$ est

$$F = \sum_{n\geq 0} nz^nM^{\lambda_B(n)},$$

parce que chaque mot $w \in \varepsilon + \mathcal{X}_+\mathcal{X}^*$ est l'écriture d'exactement un entier n. Nous avons alors $\bar{w} = n$ et l'exposant de M dans le monône correspondant à w est la longueur de $w = \tilde{n}$, qui vaut $\lambda_B(n)$.

Exemple 73 : L'opérateur associé à la série

$$S' = \sum_{w \in \mathcal{X}^*} \bar{w} w$$

est

$$F' = \left[\sum_{n \geq 0} n z^n M^{\lambda_B(n)} \right] [1 - M]^{-1},$$

parce que tous les mots $0 \cdots 0\tilde{n}$ ont pour valeur n.

Exemple 74 : L'image de

$$T = \sum_{w \in \varepsilon + \mathcal{X}_+ \mathcal{X}^*} B^{|w|} w,$$

par $\overline{\sigma}$ est

$$G = \sum_{n \geq 0} z^n (BM)^{\lambda_B(n)}$$

et celle de

$$T' = \sum_{w \in \mathcal{X}^*} B^{|w|} w,$$

par $\overline{\sigma}$ est

$$G' = \left[\sum_{n \geq 0} z^n (BM)^{\lambda_B(n)} \right] [1 - BM]^{-1}.$$

Les séries B-régulières correspondent aux séries rationnelles à support dans $\varepsilon + \mathcal{X}_+ \mathcal{X}^*$ et nous sommes donc amenés à imposer une contrainte similaire aux opérateurs.

Définition 41. *Une série $U \in A\langle\langle \mathcal{X} \rangle\rangle$ est dite B-propre si le coefficient (U, w) est nul dès que w commence par la lettre x_0.*

Un opérateur $F \in \mathbb{A}[[z, M]]$ est B-propre s'il est l'image d'une série B-propre par $\overline{\sigma}$.

Théorème 19. *Une série $f \in \mathbb{A}[[z]]$ est $(\mathbb{A}, B)$-régulière si et seulement si elle est l'image de 1 par un opérateur B-rationnel B-propre, qui est alors unique.*

Démonstration. À la série $f(z) = \sum_n f_n z^n$ sont associés la série rationnelle $S = \sum_n f_n \tilde{n}$ à support dans $\varepsilon + \mathcal{X}_+ \mathcal{X}^*$ et l'opérateur B-rationnel B-propre $F = \sum_n f_n z^n M^{\lambda(n)}$. □

Le théorème a pour corollaire immédiat la proposition suivante.

Proposition 47. *L'image d'une série B-régulière par un opérateur B-rationnel est elle-même B-régulière, dans la mesure où cette image existe.*

La restriction sur l'existence de l'image provient du fait que les opérateurs ne sont pas tous définis sur les constantes. L'existence est assurée si l'opérateur est B-propre ou si la série a une valuation non nulle.

Exemple 75 : L'opérateur B-rationnel associé à la série caractéristique du langage $U = \varepsilon + \mathcal{X}_+ \mathcal{X}^*$ est

$$Z(z, M) = 1 + [1 - (1 + z + \cdots + z^{B-1})M]^{-1} [z + \cdots + z^{B-1}] M.$$

Il fournit la série B-régulière

$$\zeta(z) = Z(z, M).1 = \frac{1}{1 - z}.$$

EXEMPLE 76 : Avec $B = 2$ et $\check{U} = \varepsilon - x_1\{x_0 + x_1\}^*$, nous obtenons l'opérateur

$$T(z, M) = 1 - [1 - (1 - z)M]^{-1}zM = 1 - \sum_{k\geq 0}[(1 - z)M]^k zM$$

et la série de Thue-Morse

$$t(z) = 1 - \sum_{k\geq 0}(1 - z)(1 - z^2)\cdots(1 - z^{2^{k-1}})z^{2^k} = \prod_{k=0}^{+\infty}(1 - z^{2^k}).$$

EXEMPLE 77 : Pour tout polynôme $p \in \mathbb{A}[t_0, \cdots, t_{B-1}]$, la série

$$S = \sum_w p(|w|_{x_0}, \cdots, |w|_{x_{B-1}})w$$

est rationnelle [13, p. 22]. La multiplication à droite par $\mathcal{X}_+$ permet de définir des séries B-propres

$$\sum_{w\in\mathcal{X}_+} p(|w|_{x_0}, |w|_{x_1} - 1\cdots, |w|_{x_{B-1}} - 1)w$$

et nous constatons que, pour tout polynôme $q \in \mathbb{A}[t_0, \cdots, t_{B-1}]$, la série

$$\sum_{n\geq 1} q(|\tilde{n}|_{x_0}, \cdots, |\tilde{n}|_{x_{B-1}})z^n$$

est B-régulière. Par exemple, avec $B = 2$ et

$$G = x_1(\mathcal{X}^* x_0 \mathcal{X}^* - \mathcal{X}^* x_1 \mathcal{X}^*) = \sum_w (|w|_{x_0} - |w|_{x_1})\, x_1 w,$$

nous obtenons ainsi la série ($\mathbb{Z}$,2)-régulière

$$g(z) = \sum_{n\geq 0}(|\tilde{n}|_{x_0} - |\tilde{n}|_{x_1} + 1)z^n = \frac{1}{1 - z}\sum_{k=0}^{+\infty} z^{2^{k+1}}\frac{1 - z^{2^k}}{1 + z^{2^k}}.$$

EXEMPLE 78 : La série rationnelle

$$\sum_{n\geq 1, m\geq 0} n x_1^n x_0^m = x_1^* x_1 x_1^* x_0^*$$

est B-propre. Son image par $\overline{\sigma}$ est

$$\sum_{n\geq 1, m\geq 0} n z^{B^m(B^n-1)} M^{n+m}.$$

En appliquant cet opérateur à 1 ou, plus généralement, à z^k, nous obtenons les séries B-régulières

$$\sum_{n\geq 1, m\geq 0} n z^{B^m(B^n-1)}$$

et

$$\sum_{n\geq 1, m\geq 0} n z^{(k+1)B^{n+m}-B^m}.$$

EXEMPLE 79 : Notons $\check{w}$ le mot miroir du mot $w \in \mathcal{X}$. On sait [13, p. 46] que, si la série $S \in A\langle\langle\mathcal{X}\rangle\rangle$ est rationnelle, la série miroir

$$\check{S} = \sum_w (S, w)\check{w}$$

est aussi rationnelle. En partant de

$$S = \varepsilon + \mathcal{X}_+\mathcal{X}^*,$$

nous trouvons que

$$\overline{\sigma}\check{S}1 = \sum_{n\geq 0} r_B(n)z^n$$

est B-régulière en notant $r_B(n)$ la valeur du miroir de l'écriture de n en base B (si $B = 2$ et $n = 18$ alors $\tilde{n} = 1010$ et $r_2(n) = \overline{0101} = 5$).

5.2.3 Ecriture fractionnaire des opérateurs B-rationnels

Théorème 20. *Soient $\mathbb{K}$ un corps commutatif et F un opérateur B-rationnel à coefficients dans $\mathbb{K}$; il existe un couple (P, Q) d'éléments de $\mathbb{K}[z, M]$ tel que*

$$QF = P$$

avec

$$Q \neq 0 \ \ et \ \ \omega_M(Q) = 0.$$

Démonstration. Le raisonnement est basé sur la propriété de clôture des séries rationnelles. Il suffit de montrer que l'ensemble des opérateurs F qui ont cette propriété contient les polynômes en z et M, est stable par somme, produit et quasi-inverse (ainsi que par multiplication externe, mais c'est évident).

Pour les polynômes, il suffit de prendre $Q = 1$.

En ce qui concerne une somme $F + F'$, si $QF = P$ et $Q'F' = P'$ avec les conditions adéquates, soit $\tilde{Q} = \text{ppcm}(Q, Q') = UQ = U'Q'$; l'écriture

$$\tilde{Q}(F + F') = UQF + U'Q'F' = UP + U'P'$$

montre que $\tilde{Q}$ convient car sa valuation est nulle comme celles de Q et Q'.

De même pour un produit FF', si $\bar{Q} = \text{ppcm}(P, Q') = VP = V'Q'$, nous écrivons

$$VQFF' = VPF' = V'Q'F' = V'P'$$

et $\bar{Q}$ satisfait les conditions demandées, puisque sa valuation est nulle comme celle de Q'.

Enfin si F est quasi-inversible (d'où $\omega_M(F) > 0$) et $QF = P$, un dénominateur possible est $Q - P$ car

$$[Q - P][1 - F]^{-1} = [Q - P]\sum_{n\geq 0} F^n = \sum_{n\geq 0} QF^n - P\sum_{n\geq 0} F^n$$

$$= Q + P\sum_{n\geq 1} F^{n-1} - P\sum_{n\geq 0} F^n = Q.$$

Remarquons que nous avons bien $Q \neq P$, sinon $F = 1$, ce qui est exclu, et $\omega_M(Q - P) = 0$ car $\omega_M(Q) = 0$ et $\omega_M(P) > 0$. □

Exemple 80 : La série rationnelle bien classique,

$$S = \sum_{w\in\mathcal{X}^*} (|w|_{x_0} - |w|_{x_1})\, w,$$

avec $B = 2$ et donc $\mathcal{X} = \{x_0, x_1\}$ admet l'expression rationnelle

$$S = (x_0 + x_1)^*(x_0 - x_1)(x_0 + x_1)^*.$$

Son image par $\overline{\sigma}$ est l'opérateur

$$G = [1 - (1 + z)M]^{-1}[(1 - z)M][1 - (1 + z)M]^{-1}.$$

Cherchons une écriture fractionnaire de G. Nous regardons d'abord le produit FF' avec

$$F = (1-z)M, \quad F' = [1-(1+z)M]^{-1}.$$

Les opérateurs F et F' ont des écritures fractionnaires $QF = P$ et $Q'F' = P'$ en notant

$$Q = 1, \quad P = (1-z)M, \quad Q' = 1-(1+z)M, \quad P' = 1.$$

La preuve du théorème fait calculer

$$\begin{aligned}\bar{Q} &= \text{ppcm}(P, Q') \\ &= (1-z^2)M - (1-z^4)M^2 \\ &= [(1+z)-(1+z^2)M][(1-z)M] = [(1-z^2)M][1-(1+z)M]\end{aligned}$$

ce qui donne l'égalité

$$[(1+z)-(1+z^2)M]FF' = (1-z^2)M.$$

Nous en tirons

$$[(1+z)-(1+z^2)M][1-(1+z)M]G = (1-z^2)M$$

ou encore

$$[(1+z)-2(1+z+z^2)M+(1+z^2)^2M^2]G = (1-z^2)M.$$

Exemple 81 : Dans la même veine, la série

$$S = \sum_{w\in\mathcal{X}^*} |w|_{x_0} w$$

admet l'expression rationnelle

$$S = \mathcal{X}^* x_0 \mathcal{X}^*$$

et donne l'opérateur

$$G = [1-(1+z+\cdots+z^{B-1})M]^{-1} M [1-(1+z+\cdots+z^{B-1})M]^{-1}.$$

En procédant comme ci-dessus, nous obtenons l'égalité :

$$[1-\Sigma^B M][1-\Sigma M]G = M,$$

avec

$$\Sigma = 1+z+\cdots+z^{B-1} \quad \text{et} \quad \Sigma^B = 1+z^B+\cdots+z^{B(B-1)}.$$

Le résultat précédent amène deux commentaires. D'abord nous pourrions espérer que P et Q soient B-rationnels, *id est* dans $\overline{\sigma}\mathbb{K}\langle\mathcal{X}\rangle$, mais $\overline{\sigma}\mathbb{K}\langle\mathcal{X}\rangle$ n'est pas stable par ppcm et cette propriété n'est pas satisfaite.

Exemple 82 : Les deux opérateurs 2-rationnels $1-M$ et $1-zM$ ont pour ppcm

$$-(1+z)+(1+z+z^2)M - z^2M^2$$

et les deux premiers coefficients ne satisfont pas la contrainte sur les degrés, donc leur ppcm n'est pas rationnel.

La considération du ppcm n'est qu'un argument technique, mais reprenons une partie du calcul effectué dans le premier exemple. Avec

$$F = (1-z)M, \quad F' = [1-(1+z)M]^{-1},$$

nous avons vu que

$$[(1+z)-(1+z^2)M]FF' = (1-z^2)M.$$

L'ensemble des Q tels que QFF' soit dans $\mathbb{K}[z, M]$ est un idéal à gauche de $\mathbb{K}[z, M]$ et nous venons de trouver un élément de cet idéal principal, qui est de degré 1 en M. Si cet idéal était engendré par un élément de $\mathbb{K}[z]$ non nul, FF' serait dans $\mathbb{K}[z, M]$ et ce n'est pas le cas puisque

$$FF' = (1-z)M \sum_{n\geq 0} \frac{1-z^{2^n}}{1-z} M^n = \sum_{n\geq 0} \frac{1-z^{2^{n+1}}}{1+z} M^{n+1}$$

et qu'il y a unicité de l'écriture des opérateurs rationnels. Ainsi

$$(1+z) - (1+z^2)M$$

est un générateur de l'idéal et bien que ses coefficients soient premiers entre eux, le coefficient $1+z$ ne satisfait pas la contrainte sur les degrés qui caractérise les opérateurs rationnels.

Ensuite d'après le théorème, si F est un opérateur B-rationnel à coefficients dans $\mathbb{K}$, nous pouvons trouver P et U dans $\mathbb{K}(z)[M]$ tels que

$$(1-U)F = P.$$

Dans l'exemple précédent, nous avons ainsi

$$[1 - \frac{1+z^2}{1+z} M]FF' = (1-z)M.$$

Cependant F, F' et donc FF' sont dans $\mathbb{Z}[z][[M]]$ et il est naturel de se demander s'il est possible de prendre P et U dans $\mathbb{Z}[z][M]$. Ce serait un analogue du théorème de Fatou pour les séries rationnelles en une indéterminée. Cela n'est pas possible puisque $1-U$ serait multiple de $(1+z)-(1+z^2)M$ par un polynôme de $\mathbb{Z}[z]$.

L'écriture fractionnaire des opérateurs B-rationnels a pour application immédiate le lien entre séries B-régulières et équations de Mahler, dont nous obtenons ainsi une seconde démonstration.

Théorème 21. *Une série B-régulière f, à coefficients dans un corps commutatif $\mathbb{K}$, vérifie une équation B-Mahler*

$$Af = b$$

*non triviale (*id est $A \neq 0$*) avec un second membre, b, polynôme. Quitte à augmenter l'ordre de l'équation, on peut supposer que $b = 0$.*

Rappelons qu'une telle équation est de la forme

$$\sum_{k=0}^{N} c_k(z) f(z^{B^k}) = b(z),$$

les coefficients c_k étant des polynômes.

Démonstration. Cette propriété résulte simplement de l'écriture fractionnaire des opérateurs : si $QF = P$ et $f = F1$, $Qf = P1$ avec des notations sous-entendues. En appliquant l'opérateur (cf. page 27)

$$P_{B,n} = \text{ppcm}(1-M, z^{B-1}-M, \cdots, z^{(B-1)n}-M),$$

qui annule 1, z, $\cdots$, z^n, si b est de degré n, on se ramène à une équation homogène. □

EXEMPLE 83 : Considérons à nouveau la suite $(c(n))_{n\geq 0}$ des entiers naturels dont l'écriture en base 3 ne comporte pas le chiffre 1, rangés dans l'ordre croissant. Le langage correspondant dans $\mathcal{X}_3$ est $\mathcal{C}$ défini par

$$\mathcal{C} = \varepsilon + \mathcal{C}\{x_0 + x_2\},$$

ce qui se traduit par les relations de récurrence

$$\begin{array}{rcl} c(2n) & = & 3\,c(n) \\ c(2n+1) & = & 3\,c(n) + 2. \end{array}$$

Si

$$c(z) = \sum_{n\geq 0} c(n) z^n = 2\,z + 6\,z^2 + 8\,z^3 + \cdots,$$

ces relations montrent qu'une base du $\mathbb{Z}$-module engendrée par l'orbite de $c(z)$ sous l'action de $\mathcal{X}_2^*$ est constituée de

$$\begin{array}{rcl} e_0(z) & = & c(z) \\ e_1(z) & = & 1/(1-z). \end{array}$$

Avec les notations déjà employées

$$\lambda = \begin{pmatrix} 0 & 1 \end{pmatrix} \text{ et } \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$$\begin{array}{rclrcl} S_0 e_0 & = & 3e_0, & S_1 e_0 & = & 3e_0 + 2e_1 \\ S_0 e_1 & = & e_1, & S_1 e_1 & = & e_1, \end{array}$$

$$A_0 = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix},$$

$$\Xi = \begin{pmatrix} 3\,(x_0 + x_1) & 0 \\ 2\,x_1 & x_0 + x_1 \end{pmatrix} \text{ et } \Xi_+ = \begin{pmatrix} 3\,x_1 & 0 \\ 2\,x_1 & x_1 \end{pmatrix}.$$

En posant

$$\begin{array}{rcl} U & = & [3\,(x_0 + x_1)]^* \\ V & = & [x_0 + x_1]^* \end{array}$$

nous trouvons

$$\Xi^* = \begin{pmatrix} U & 0 \\ 2\,V x_1 U & V \end{pmatrix},$$

$$I + \Xi_+ \Xi^* = \begin{pmatrix} \varepsilon + 3\,x_1 U & 0 \\ 2\,x_1 U + 2\,x_1 V x_1 U & \varepsilon + x_1 V \end{pmatrix},$$

$$\begin{array}{rcl} S & = & \lambda(I + \Xi_+ \Xi^*)\gamma \\ & = & 2\,x_1[\varepsilon + [x_0 + x_1]^* x_1][3\,(x_0 + x_1)]^* \end{array}$$

et $c(z)$ est l'image de 1 par l'opérateur

$$F = 2\,[1 - 3\,(1+z)M]^{-1}[1 + zM[1 - (1+z)M]^{-1}]zM.$$

Comme

$$[z - (1+z^2)M][1 - 3\,(1+z)M]F = 2\,[z - M]zM,$$

$c(z)$ vérifie l'équation

$$[z - (1+z^2)M][1 - 3\,(1+z)M]c(z) = 0.$$

L'équation

$$[z - (1+z^2)M]f(z) = 0,$$

donne

$$f(z) = \frac{Cz}{1 - z^2}$$

et nous voyons que $C = 2$. Ainsi

$$[1 - 3\,(1 + z)M]c(z) = \frac{2\,z}{1 - z^2},$$

ce que nous aurions bien entendu pu établir directement en utilisant les relations de récurrence. En résolvant l'équation nous obtenons l'expression explicite

$$c(z) = 2 \sum_{n \geq 0} \frac{3^n z^{2^n}}{(1 - z)(1 + z^{2^n})}.$$

5.3 Extension aux anneaux

Si l'anneau de référence n'est pas intègre, il n'y a pas de raison qu'une série B-régulière soit mahlérienne même si l'anneau est nœthérien. Nous allons voir qu'il y a toujours une équation de Mahler vérifiée par la série, avec toutefois le risque que cette équation se réduise à $0 = 0$. En pratique ce ne sera pourtant pas le cas.

Introduisons $B\,N^2 + 2N$ indéterminées $a_{r,i,j}$, λ_j, γ_i avec $0 \leq r < B$, $1 \leq i, j \leq N$. La série générique B-régulière de rang N est à coefficients dans $\mathbb{Z}[a, \lambda, \gamma]$ et définie par la représentation linéaire

$$A_r = (a_{r,i,j})_{1 \leq i,j \leq N}\,,$$
$$\lambda = (\lambda_j)_{1 \leq j \leq N}\,, \quad \gamma = (\gamma_i)_{1 \leq i \leq N}\,.$$

L'algorithme `équation_de_mahler` donne son équation minimale,

$$c_0(z)g(z) + c_1(z)g(z^B) + \cdots + c_N(z)g(z^{B^N}) = 0.$$

Le coefficient $c_k(z)$ est un polynôme de degré $\displaystyle\sum_{\ell=1}^{N-1} \ell B^\ell + \sum_{\ell=1}^{k-1} B^\ell$. De plus $c_k(z)$ est une forme N-aire en γ et une forme $(k+1)$-aire par rapport à a. Par exemple pour $N = 2$ et $B = 2$, le coefficient c_0 vaut

$$\begin{aligned} c_0(z) = &\left[\gamma_2^2 a_{0,1,2} + \gamma_2\gamma_1 a_{0,1,1} - \gamma_1\gamma_2 a_{0,2,2} - \gamma_1^2 a_{0,2,1}\right] \\ &+ z^2\left[\gamma_2\gamma_1 a_{1,1,1} + \gamma_2^2 a_{1,1,2} - \gamma_1^2 a_{1,2,1} - \gamma_1\gamma_2 a_{1,2,2}\right]. \end{aligned}$$

Maintenant pour une série $(\mathbb{A}, B)$-régulière donnée par une représentation linéaire de dimension N, nous substituons aux $a_{r,i,j}$, λ_j, γ_i les éléments correspondants de $\mathbb{A}$ et nous obtenons ainsi une équation de Mahler. Evidemment il se pourrait bien que tous les coefficients de l'équation soient nuls.

Appliquons ceci à des séries B-automatiques. Puisque l'équation est indépendante de λ, il est inutile de le préciser et c'est pourquoi nous parlons de B-machines dans les exemples qui suivent. En interprétant 0 et 1 comme des entiers, nous obtenons une équation à coefficients entiers. Seule la donnée du vecteur ligne λ, qui correspond à la fonction de sortie, détermine l'anneau utilisé. Celui-ci étant donné, nous avons une équation à coefficients dans le sous-anneau premier $\mathbb{Z}/(\kappa)$, si l'anneau est de caractéristique κ.

Exemple 84 : Avec la 2-machine définie par

$$A_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

nous obtenons l'équation

$$f(z) - \left(1 + z^2\right)(1 + z)\, f(z^4) = 0.$$

EXEMPLE 85 : La série de Baum-Sweet à coefficients dans $\mathbb{F}_2$ est algébrique de degré 3 et admet un développement en fraction continuée dont les quotients partiels ont des degrés bornés, ce qui est remarquable. La suite des coefficients est 2-automatique et la 2-machine de Baum-Sweet [3, p. 247], donnée par la représentation linéaire

$$A_0 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

a pour équation minimale

$$z^2 f(z) - \left(1 + z^3 + z^4\right) f(z^2) + z^6 f(z^4) + \left(1 + z^4\right) f(z^8) = 0.$$

Sur ces exemples l'équation minimale de la série générique ne devient triviale dans aucun anneau.

Chapitre 6

Critères de B-régularité

Le résultat le plus frappant de la théorie des suites automatiques est le théorème de Christol, Kamae, Mendès France et Rauzy, qui relie deux notions *a priori* étangères. Rappelons en l'énoncé [3, 18].

Théorème 22. *Une série formelle $f(z)$ à coefficients dans le corps fini $\mathbb{F}_q$ est q-automatique si et seulement si elle est algébrique sur le corps des fractions rationnelles $\mathbb{F}_q(z)$.*

Nous avons consacré le chapitre précédent à l'extension du sens direct de ce théorème aux séries B-régulières. Ce chapitre porte sur la réciproque.

Ce théorème a déjà reçu de nombreuses applications [2, 4, 54], aussi nous contenterons nous d'en citer une qui est peu connue.

Exemple 86 : Le n-ième nombre de Bell ϖ_n, est le nombre de partitions d'un ensemble à n éléments. La série génératrice exponentielle des nombres de Bell est bien connue [22],

$$\widehat{\varpi}(z) = \sum_{n\geq 0} \varpi_n \frac{z^n}{n!} = e^{e^z-1}.$$

La série génératrice ordinaire

$$\varpi(z) = \sum_{n\geq 0} \varpi_n z^n = 1 + z + 2\,z^2 + 5\,z^3 + 15\,z^4 + 52\,z^5 + \cdots$$

possède un développement en fraction continuée de Jacobi dont l'expression est très simple [32, chap. 5] [37, chap. 5],

$$\varpi(z) = \cfrac{1}{1 - 1.z - \cfrac{1.z^2}{1 - 2.z - \cfrac{2.z^2}{1 - 3.z - \cfrac{3.z^2}{\ddots}}}}$$

Cette formule s'obtient en représentant une partition par un chemin valué obtenu par l'intermédiaire d'un diagramme assez naturel (cf. figure 6.1). A chaque bloc de la partition est associé le segment dont les extrémités sont le plus petit et le plus grand élément du bloc.

Supposons que nous réduisions les coefficients modulo un nombre premier p ; la fraction continuée devient alors finie et la série génératrice est rationnelle. La suite des nombres de Bell réduits modulo p est donc périodique.

Introduisons maintenant une contrainte sur les partitions considérées. Nous demandons que deux segments associés à des blocs différents soient ou bien disjoints ou bien l'un dans l'autre, ce qui définit la notion de

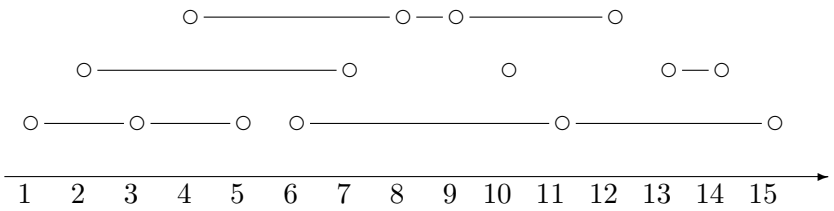

FIG. 6.1
Le diagramme ci-dessus est associé à la partition de $[1, 15]$ dont les blocs sont $\{1, 3, 5\}$, $\{2, 7\}$, $\{4, 8, 9, 12\}$, $\{6, 11, 15\}$, $\{10\}$ et $\{13, 14\}$. Chaque bloc fournit un intervalle visualisé par un segment horizontal, le plus petit intervalle qui contient le bloc.

partition non chevauchantes [35]. La série génératrice ordinaire du nombre de partitions non chevauchantes, ϖ_n^*, d'un ensemble à n éléments

$$\varpi^*(z) = \sum_{n\geq 0} \varpi_n^*\, z^n = 1 + z + 2\,z^2 + 5\,z^3 + 14\,z^4 + 43\,z^5 + \cdots,$$

a pour développement en fraction continuée de Jacobi

$$\varpi^*(z) = \cfrac{1}{1 - 1.z - \cfrac{1.z^2}{1 - 2.z - \cfrac{1.z^2}{1 - 3.z - \cfrac{1.z^2}{\ddots}}}}$$

En la réduisant modulo p, nous voyons apparaître une fraction continuée périodique et $\varpi^*(z)$ est donc un algébrique de degré 2 sur le corps $\mathbb{F}_p(z)$, c'est-à-dire une série p-automatique. En travaillant modulo 2, on trouve par exemple la récurrence [35, p. 431]

$$f_0 = 1, \quad f_{2n+1} = 1, \quad f_{2n+2} = 1 - f_n.$$

Le théorème de Christol, Kamae, Mendès France et Rauzy, pour plaisant qu'il soit, n'est cependant pas satisfaisant sur certains points. D'abord il impose que la caractéristique du corps des coefficients soit la base de numération, ce qui n'est guère naturel. Remarquons en passant qu'il revient au même de dire q-automatique ou p-automatique, si p est la caractéristique de $\mathbb{F}_q$. La suite du nombre de partitions hexaires d'un entier n'est pas 2-automatique si on la réduit modulo 2, par contre elle est alors 6-automatique. Ensuite ce procédé de réduction modulo un entier n'a pas de raison d'être limité aux modules premiers et la suite du nombre de partitions binaires d'un entier est 2-automatique quand on la réduit modulo 2, mais aussi modulo 4, 8, 16 ou 32. Enfin nous aimerions disposer d'un énoncé similaire pour des suites d'entiers ou de nombres complexes.

Comme nous l'avons vu au chapitre précédent les équations fonctionnelles qui sont naturelles dans le contexte des séries régulières sont les équations de Mahler et non les équations algébriques, comme pourrait le faire penser le théorème de Christol, Kamae, Mendès France et Rauzy. La confusion vient de ce que tout série formelle $f(z)$ de $\mathbb{F}_q[[z]]$ vérifie $f(z^q) = f(z)^q$. Nous cherchons donc un critère, une condition suffisante, pour qu'une série formelle solution d'une équation de Mahler

$$c_0(z)\, f(z) + c_1(z)\, f(z^B) + \cdots + c_N(z)\, f(z^{B^N}) = b(z)$$

soit B-régulière.

Commençons par un critère évident et simple, qui est relativement à part et que nous ne citons que pour mémoire.

Théorème 23. *Si une série formelle à coefficients dans un anneau commutatif, $f \in \mathbb{A}[[z]]$ est solution d'une équation B-Mahler*

$$[1 - A]f = b$$

avec $A \in \mathbb{A}[z, M]$ quasi-inversible B-rationnel et $b(z) \in \mathbb{A}[[z]]$ B-régulière, alors $f(z)$ est B-régulière.

DÉMONSTRATION. En effet A est quasi-inversible et comme il est B-rationnel son quasi-inverse $(1 - A)^{-1}$ l'est aussi. Il en résulte que $f = (1 - A)^{-1}b$ est B-régulière. □

Tous les autres critères que nous donnons portent sur le coefficient $c_0(z)$, que nous pouvons supposer non nul d'après un résultat du chapitre 3. Nous commençons par développer un critère pour le cas où $c_0(z)$ vaut essentiellement 1. Il est facile mais important car il couvre beaucoup d'exemples. Nous l'étendons ensuite en un critère général, dont les suivants ne sont que des cas particuliers. Nous montrons ainsi qu'une série formelle à coefficients dans un corps fini et vérifiant une équation B-Mahler est B-régulière quand la caractéristique du corps divise B. Cet énoncé est une généralisation directe du théorème de Christol, Kamae, Mendès France et Rauzy, dans lequel B est exactement la caractéristique du corps. Nous donnons ensuite un autre critère, plus technique, pour le cas où la caractéristique ne divise pas B et nous étendons ces résultats aux anneaux de caractéristique non nulle. Enfin nous établissons un critère pour les séries à coefficients dans un corps algébriquement clos, ce qui nous permet par exemple de considérer des suites d'entiers. On peut trouver dans [10] des cas particuliers de nos résultats.

Les conditions que nous donnons sur le coefficient $c_0(z)$ sont suffisantes pour obtenir une série B-régulière, mais il n'y a pas de raison qu'elles soient nécessaires. Cependant elles n'en sont pas loin comme le montre un exemple simple.

6.1 Critère facile

Donnons d'abord un énoncé qui montrera bien le but que nous poursuivons.

Théorème 24. *Si $f(z)$ est un série formelle à coefficients dans un anneau commutatif nœthérien $\mathbb{A}$, vérifiant une équation B-Mahler de la forme*

$$z^\gamma f(z) + \sum_{k=1}^{N} c_k(z) f(z^{B^k}) = b(z),$$

où $b(z)$ est une série B-régulière, alors $f(z)$ est B-régulière.

EXEMPLE 87 : Si $(c(n))_{n\geq 0}$ est la suite strictement croissante des entiers naturels dont l'écriture en base 3 ne comporte pas le chiffre 1 et

$$c(z) = \sum_{n\geq 0} c(n) z^n = 2z + 6z^2 + 8z^3 + 18z^4 + \cdots = \frac{2}{1-z} \sum_{k\geq 0} \frac{3^k z^{2^k}}{1 + z^{2^k}},$$

la série $c(z)$ vérifie

$$zc(z) - (1 + 3z + 4z^2)c(z^2) + 3(1 + z^2)^2 c(z^4) = 0$$

donc est 2-régulière, ce que nous savions par ailleurs [6].

Ce résultat est facilement généralisable à des vecteurs de séries formelles,

$$F(z) = \begin{pmatrix} f_1(z) \\ \vdots \\ f_d(z) \end{pmatrix}.$$

Pour cela il faut d'abord définir ce qu'est un vecteur de séries formelles B-régulier. Il suffit d'étendre les opérateurs de section composante par composante et de calquer les définitions du cas unidimensionnel, en demandant que les sections engendrent un sous-module de $\mathbb{A}[[z]]^d$ de type fini. Remarquons que les formules sur les opérateurs de section se généralisent sans problème, comme on le voit en explicitant les produits matriciels. En particulier si $A(z)$ est une matrice carrée de séries formelles et $F(z)$ un vecteur de séries formelles nous avons

$$S_r\left[A(z)F(z^B)\right] = (S_rA)(z)F(z).$$

Ensuite la notion de vecteur mahlérien apparaît d'elle-même ; un vecteur de séries formelles est B-mahlérien s'il satisfait une équation de Mahler

$$C_0(z)F(z) + C_1(z)F(z^B) + \cdots + C_N(z)F(z^{B^N}) = 0$$

à coefficients des matrices carrées de fractions rationnelles non toutes nulles. Nous arrivons ainsi à un énoncé qui généralise directement le précédent.

Théorème 25. *Si l'anneau $\mathbb{A}$ est nœthérien et si $F(z) \in \mathbb{A}[[z]]^d$ est un vecteur de séries formelles vérifiant une équation B-Mahler de la forme*

$$z^\gamma F(z) + \sum_{k=1}^{N} C_k(z)F(z^{B^k}) = E(z)$$

dans laquelle les coefficients des matrices $C_1(z)$, …, $C_N(z)$ sont des polynômes et $E(z)$ est un vecteur de séries formelles B-régulier, alors le vecteur $F(z)$ et en particulier ses composantes sont B-réguliers.

Démonstration. Notons D le maximum des degrés des coefficients des matrices $C_1(z), \ldots, C_N(z)$, puis $\mathcal{C}$ le $\mathbb{A}$-module engendré par les z^ℓ pour $\ell = -\gamma \ldots \max(1, D-\gamma)$. Ensuite soit $\mathcal{H}$ le module stable engendré par $E(z)$ et enfin $\mathcal{G}$ le module somme des $z^\ell\mathcal{H}$ pour ℓ entre $-\gamma$ et $\max(1, D-\gamma)$. Le point élémentaire mais crucial est que

$$S_r z^\ell \mathcal{C} \subset \mathcal{C}, \quad S_r z^\ell \mathcal{G} \subset \mathcal{G} \quad \text{pour } \ell = -\gamma, \ldots, \max(0, D-\gamma).$$

Pour ce qui est de $\mathcal{C}$, nous pourrions aussi écrire

$$S_r\mathcal{C}\mathcal{C} \subset \mathcal{C}.$$

Les deux types d'inclusion se traitent de la même façon. Prenons le second qui est plus compliqué. Il suffit de considérer les $S_r z^\ell z^{\ell'} h$ avec $h \in \mathcal{H}$, $-\gamma \le \ell, \ell' \le \max(1, D-\gamma)$, et donc les $S_r z^m h$ avec $m \in [-2\gamma, 2\max(1, D-\gamma)]$. Or

$$S_r z^m h = \sum_{s+t \equiv r \bmod B} z^{(s+t)\div B} S_s(z^m) S_t h$$

(rappelons que $u \div B$ est le quotient entier de u par B) et cette somme se réduit au terme d'indice s tel que $s \equiv m \bmod B$. Ainsi

$$S_r z^m h = z^{m'} S_t h$$

avec $m' = \epsilon + \lfloor m/B \rfloor$ et $\epsilon = 0$ ou 1. Nous en tirons

$$-\gamma \leq -\frac{2\gamma}{B} \leq m' \leq \epsilon + \left\lfloor \frac{2\,\max(1, D-\gamma)}{B} \right\rfloor \leq \max(1, D-\gamma).$$

La dernière inégalité pose un léger problème. Si $B \geq 3$, nous avons $1 + \lfloor 2\,x/B \rfloor \leq x$ si $x \geq 1$ et le seul cas à considérer est celui où $B = 2$, $\epsilon = 1$ et $m \geq 1$. Nous avons alors $s = t = 1$ et $r = 0$, ce qui implique que m est impair et donc inférieur à $2\,\max(1, D-\gamma) - 1$. Mais dans ce cas

$$S_0 z^m h = z\, S_1 z^m S_1 h = z^{(m+1)/2} S_1 h$$

et

$$m' = \frac{m+1}{2} \leq \frac{2\,\max(1, D-\gamma) - 1 + 1}{2} = \max(1, D-\gamma).$$

La propriété de stabilité est donc acquise.

Ce point étant établi, nous allons montrer que le module de type fini, $\mathcal{M}$, constitué des

$$V = W + \sum_{k=0}^{N} A_k M^k F,$$

où W est un vecteur de $\mathcal{G}$ et les A_k sont des matrices carrées à coefficients dans $\mathcal{C}$, est stable par section. Comme

$$F = z^{-\gamma} E - \sum_{k=1}^{N} z^{-\gamma} C_k M^k F$$

est dans $\mathcal{M}$ et $\mathbb{A}$ est nœthérien, il en résultera bien que le vecteur F est B-régulier. La section $S_r V$ d'un vecteur V de la forme ci-dessus s'écrit

$$S_r W + S_r A_0 \left[z^{-\gamma} E - \sum_{k=1}^{N} z^{-\gamma} C_k M^k F \right] + \sum_{k=1}^{N} [S_r A_k] M^{k-1} F$$

c'est-à-dire

$$S_r W + S_r z^{-\gamma} A_0 E - \sum_{k=1}^{N} S_r [z^{-\gamma} A_0 C_k] M^{k-1} F + \sum_{k=1}^{N} [S_r A_k] M^{k-1} F.$$

Le terme $S_r W$ est dans $\mathcal{G}$ car le module $\mathcal{G}$ est stable par section. Le terme $z^{-\gamma} E$ est dans $\mathcal{G}$ et les coefficients de A_0 sont dans $\mathcal{C}$ donc des combinaisons linéaires des z^ℓ avec ℓ entre $-\gamma$ et $\max(0, D-\gamma)$; ainsi $S_r z^{-\gamma} A_0 E$ est dans $\mathcal{G}$. Ensuite les coefficients de $z^{-\gamma} C_k$ et de A_0 sont dans $\mathcal{C}$ donc $S_r[z^{-\gamma} A_0 C_k]$ est dans $\mathcal{C}$. Enfin $S_r A_k$ est dans $\mathcal{C}$, comme on le voit en prenant $\ell = 0$ dans la petite formule qui nous sert de fondement. Nous constatons bien que $S_r V$ est dans $\mathcal{M}$ pour tout V dans $\mathcal{M}$. □

Ce résultat s'applique essentiellement à des suites définies par récurrence suivant le résidu modulo une puissance de B. Donnons un exemple pour bien montrer au lecteur de quoi il s'agit.

Exemple 88 : Supowit et Reingold [67] ont rencontré, dans l'étude de l'appariement euclidien ("matching"), la récurrence

$$\left\{ \begin{array}{lcl} C_{4n} & = & a(C_{2n+1} + C_{2n-1}) + b \\ C_{4n+1} & = & a(C_{2n+1} + C_{2n}) \\ C_{4n+2} & = & a(C_{2n+1} + C_{2n+1}) + b \\ C_{4n+3} & = & a(C_{2n+2} + C_{2n+1}) \end{array} \right.$$

dans laquelle $a = 1/\sqrt{2}$ et $b = \sqrt{3}$, avec les conditions initiales $C_0 = C_1 = 0$, $C_2 = b$ et $C_3 = ab$. Clairement b n'est qu'un facteur d'échelle et nous pouvons le prendre égal à 1.

Notons $f(z)$ la série génératrice de la suite (C_n) et $f_w(z)$ la section $S_{2,w}f(z)$. La récurrence fournit le système

$$\left\{\begin{array}{lcl} f_{00}(z) &=& a\,(1+z)f_1(z^2)+1/(1-z)\\ f_{01}(z) &=& a\,f_1(z^2)+a\,f_0(z^2)\\ f_{10}(z) &=& 2a\,f_1(z^2)+1/(1-z)\\ f_{11}(z) &=& a\,f_0(z^2)/z+a\,f_1(z^2)\end{array}\right.$$

et si nous exprimons $f_0(z)$ et $f_1(z)$ en fonction des $f_w(z)$ ($w = 00, \ldots, 11$) nous obtenons un système d'inconnue

$$F(z)=\begin{pmatrix} f_{00}(z)\\ f_{01}(z)\\ f_{10}(z)\\ f_{11}(z)\end{pmatrix}$$

qui s'écrit

$$z\,F(z)=a\,C_1(z)F(z^2)+E(z)$$

en posant

$$C_1(z)=\begin{pmatrix} 0 & z(1+z) & 0 & z^2(1+z)\\ z & z & z^2 & z^2\\ 0 & 2\,z & 0 & 2\,z^2\\ 1 & z & z & z^2\end{pmatrix},\quad E(z)=\begin{pmatrix} z/(1-z)\\ 0\\ z/(1-z)\\ 0\end{pmatrix}.$$

Le vecteur $E(z)$ est B-régulier et le théorème permet de dire qu'il en est de même de $F(z)$. Il en est donc de même pour chacune de ses composantes et aussi de $f(z)$.

Le résultat obtenu est important car il couvre quasiment tous les exemples de récurrence *diviser pour régner*. Nous donnons donc l'énoncé équivalent pour les suites.

Proposition 48. *Soit (u_n) une suite à valeurs dans un anneau nœthérien. Si cette suite est définie par un système de relations de récurrence de la forme*

$$u_{B^K n+\ell}=\sum_{0\le k<K}\sum_{j=-J}^{J} a_{\ell,k,j}u_{B^k n+j}+v_{\ell,n}$$

pour n assez grand, dans lequel K et J sont fixés, ℓ parcourt les entiers de 0 à B^K-1, les suites $(v_{\ell,n})_n$ sont B-régulières et les $a_{\ell,k,j}$ sont dans l'anneau de référence, alors elle est B-régulière.

6.2 Critère général

Nous étudions maintenant des équations

$$c_0(z)f(z)+c_1(z)f(z^B)+\cdots+c_N(z)f(z^{B^N})=b(z)$$

dans lesquelles le coefficient $c_0(z)$, toujours non nul, peut avoir des racines autres que 0.

Nous pourrions comme dans le paragraphe précédent considérer des équations vectorielles

$$C_0(z)\,F(z)+C_1(z)F(z^B)+\cdots+C_N(z)F(z^{B^N})=E(z).$$

En prémultipliant les deux termes de l'équation par la comatrice de $C_0(z)$, nous obtenons une équation de la forme

$$\Delta(z)\,F(z)+C'_1(z)F(z^B)+\cdots+C'_N(z)F(z^{B^N})=E'(z),$$

où $\Delta(z)$ est le déterminant de $C_0(z)$. Une adaptation facile des conditions imposée à $c_0(z)$ dans nos critères donne des conditions portant sur $\Delta(z)$ pour que $F(z)$ soit un vecteur B-régulier. Cependant il pourrait se faire que $\Delta(z)$ soit nul même si la matrice $C_0(z)$ n'est pas nulle. De plus nous ne connaissons pas d'exemple naturel de cette situation. Nous préférons donc nous limiter aux équations scalaires pour simplifier les écritures.

Nous voulons obtenir l'énoncé suivant.

Théorème 26. *Soit $\mathbb{A}$ un anneau commutatif nœthérien et $f(z)$ une série formelle à coefficients dans $\mathbb{A}$, qui vérifie une équation de Mahler linéaire*

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z)$$

avec un second membre $b(z)$, qui est une série B-régulière.

Nous supposons que

1. *le coefficient de plus bas degré de c_0 est inversible dans $\mathbb{A}$,* id est

$$c_0(z) = Cz^\gamma g(z)$$

   avec C inversible, $\gamma \geq 0$ et $g(0) = 1$,

2. *l'ensemble des*

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B) g(z)} \right) = S_{r_K} \frac{1}{g} \left(S_{r_{K-1}} \frac{1}{g} \left(\cdots S_{r_1} \frac{1}{g} \right) \right),$$

   avec $K \geq 0$ et $0 \leq r_k < B$ pour $k = 1, \cdots, K$, est contenu dans un module de type fini.

Alors $f(z)$ est $(\mathbb{A}, B)$-régulière.

L'idée sous-jacente est fort simple. Nous posons

$$f(z) = \frac{h(z)}{\prod_{k\geq 0} g(z^{B^k})}$$

et nous reportons cette expression dans l'équation. Ceci fournit une équation dont $h(z)$ est solution,

$$C\, z^\gamma h(z) + c_1(z)\, h(z^B) + c_2(z)\, g(z)\, h(z^{B^2}) + \cdots + c_N(z) \prod_{1\leq k<N} g(z^{B^k})\, h(z^{B^N}) = b(z) \prod_{k\geq 1} g(z^{B^k}),$$

à laquelle s'applique le critère facile. En effet C est inversible et le second membre est B-régulier comme produit de deux séries B-régulières (le produit infini est B-régulier car on peut lui appliquer le critère facile). Ainsi $h(z)$ est une série B-régulière et il suffit que le produit infini

$$G(z) = \frac{1}{\prod_{k\geq 0} g(z^{B^k})}$$

soit B-régulier pour que la série $f(z)$ soit B-régulière.

Or l'étude de la B-régularité d'un produit infini repose sur le lemme suivant, qui fournit la clé du théorème.

Lemme 8. *Le produit infini* $G(z) = \dfrac{1}{\prod_{k\geq 0} g(z^{B^k})}$ *est* B*-régulier si et seulement si l'ensemble des fractions rationnelles*

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B) g(z)} \right) = S_{r_K} \frac{1}{g} \left(S_{r_{K-1}} \frac{1}{g} \left(\cdots S_{r_1} \frac{1}{g} \right) \right),$$

avec $K \geq 0$ *et* $0 \leq r_k < B$ *pour* $k = 1, \cdots, K$*, engendre un module de type fini.*

Démonstration. L'égalité

$$S_{r_K} \cdots S_{r_1} G(z) = \left[S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z) g(z^B) \cdots g(z^{B^{K-1}})} \right) \right] G(z)$$

montre que la division par $G(z)$ fait passer du module stable par section engendré par $G(z)$ au module engendré par les fractions ci-dessus, d'où l'équivalence. □

Ce lemme a aussi le mérite de montrer que l'on ne peut pas espérer obtenir un meilleur critère dans la mesure où l'on ne considère que le coefficient $c_0(z)$. En effet dès que $c_0(z)$ ne satisfait pas le point *2.* du théorème, le produit infini $G(z)$ n'est pas B-régulier alors qu'il vérifie l'équation

$$c_0(z)\, G(z) = C\, z^\gamma\, G(z^B).$$

6.3 Caractéristique non nulle

Pour utiliser le critère dans un anneau fini, nous allons chercher des conditions pour que les

$$S_{r_K} \frac{1}{g} S_{r_{K-1}} \frac{1}{g} \cdots S_{r_1} \frac{1}{g}$$

admettent tous une même période pour la suite de leurs coefficients. Rappelons que la période d'une fraction rationnelle a/b, où $b(0) = 1$, est la période des coefficients de son développement en série formelle. Nous avons étudié cette notion au chapitre 1 et nous utilisons les résultats qui y sont établis.

Définition 42. *Si* a *est un entier plus grand que 2 et* ℓ *un entier plus grand que 1,* $\lambda_a^-(\ell)$ *est l'exposant de la première puissance de* a *qui surpasse* ℓ*, c'est-à-dire* $\lceil \ln \ell / \ln a \rceil$*.*

Cette notation est à rapprocher de la notation $\lambda_a(\ell)$, déjà introduite (cf. page 68). Nous avons $\lambda_a^-(\ell) = \lambda_a(\ell)$ sauf si ℓ est une puissance de a, auquel cas $\lambda_a^-(\ell) = \lambda_a(\ell) - 1$.

Proposition 49. *Soit d'une part* $B = p^\alpha b$ *un entier naturel supérieur ou égal à 2, avec* b *non divisible par* p*, et d'autre part* $g(z)$ *un polynôme sur le corps* $\mathbb{F}_q$ *de caractéristique* p*, avec* $g(0) \neq 0$*, dont la période est* T *et qui se décompose en*

$$\prod_i g_i^{m_i}$$

et enfin

$$\mu = \max_i m_i.$$

La période de

$$g(z) g(z^B) g(z^{B^2}) \cdots g(z^{B^{K-1}})$$

vaut

$$TB^{K-1}p^{\epsilon} \quad \textit{avec} \begin{cases} -1 \leq \epsilon \leq \alpha & \textit{si } \alpha > 0, \\ 1 - \lambda_p^-(\mu) \leq \epsilon \leq \lambda_p^-(K) & \textit{si } p \textit{ ne divise pas } B \ (\alpha = 0). \end{cases}$$

De plus le minorant est atteint dans ces inégalités si b a des facteurs communs avec chacune des périodes des facteurs g_i.

DÉMONSTRATION. Commençons d'abord par supposer que $g = h^m$, avec h irréductible, ce qui fait que

$$g(z)g(z^B)g(z^{B^2})\cdots g(z^{B^{K-1}}) = h(z)^m h(z^b)^{p^\alpha m} h(z^{b^2})^{p^{2\alpha} m} \cdots h(z^{b^{K-1}})^{p^{(K-1)\alpha} m}.$$

Le ppcm des périodes des facteurs irréductibles est $b^{(K-1)}t$, si t est la période de h, car la substitution de z^b à z fait apparaître des facteurs de période bt dans tous les cas et de période t à l'occasion. Quant à l'ordre de multiplicité de chaque facteur il est égal à m, $p^\alpha m$, $\cdots$ ou $p^{(K-1)\alpha}m$, suivant le facteur $h(z)$, $h(z^b)$, $\cdots$ dans lequel il figure, sauf peut-être pour les facteurs irréductibles dont la période est première avec b, car il peuvent apparaître dans plusieurs facteurs $h(z^{b^\ell})$. Dans ce cas, le maximum possible est

$$m + p^\alpha m + \cdots + p^{(K-1)\alpha} m = \begin{cases} m\,\frac{p^{K\alpha}-1}{p^\alpha - 1} & \text{si } \alpha \neq 0, \\ mK & \text{si } \alpha = 0. \end{cases}$$

Par contre si b et t ne sont pas premiers entre eux tous les $h(z^{b^\ell})$ ont des facteurs premiers distincts et les multiplicités sont bien les m, $p^\alpha m$, $\cdots$ ou $p^{(K-1)\alpha}m$.

Ainsi la période de $g(z)g(z^B)g(z^{B^2})\cdots g(z^{B^{K-1}})$ vaut $b^{K-1}tp^\ell$, avec

$$\lambda_p^-(mp^{(K-1)\alpha}) \leq \ell \leq \lambda_p^-\left(m\,\frac{p^{K\alpha}-1}{p^\alpha - 1}\right) \qquad \text{si } p \text{ divise } B,$$

et

$$1 \leq \ell \leq \lambda_p^-(mK) \qquad \text{si } p \text{ ne divise pas } B,$$

puisque il faut prendre pour ℓ la première puissance de p supérieure à toutes les multiplicités des facteurs irréductibles. De plus la borne gauche est atteinte quand au moins un diviseur premier de b est un diviseur de T car les facteurs irréductibles sont alors tous distincts, d'après le corollaire de la proposition 6 page 18.

Passons ensuite au cas général. Si $g = \prod_i g_i^{m_i}$ avec des g_i irréductibles, la période de $g(z)$ est $T = \tau p^{\lambda_p^-(\mu)}$, en notant τ le ppcm des périodes des g_i et μ le plus grand des m_i. D'autre part le ppcm des résultats précédents fournit la période de $g(z)g(z^B)g(z^{B^2})\cdots g(z^{B^{K-1}})$.

Premièrement, dans le cas où p divise B, nous obtenons $\tau b^{K-1}p^\lambda$, avec

$$\lambda_p^-(\mu p^{(K-1)\alpha}) \leq \lambda \leq \lambda_p^-(\mu\,\frac{p^{K\alpha}-1}{p^\alpha - 1}),$$

ou l'inégalité plus large

$$\log_p \mu + (K-1)\alpha \leq \lambda \leq \log_p \mu + K\alpha$$

et la période s'écrit

$$\tau b^{K-1}p^\lambda = \tau p^{\lambda_p^-(\mu)} b^{K-1} p^{(K-1)\alpha} p^{\lambda - \lambda_p^-(\mu) - (K-1)\alpha} = TB^{K-1}p^\epsilon$$

avec

$$-1 < \epsilon \leq \alpha.$$

Deuxièmement, si p ne divise pas B, la période est $\tau b^{K-1}p^\lambda$, avec

$$1 \leq \lambda \leq \lambda_p^-(\mu K).$$

Dans ce cas la période vaut

$$\tau b^{K-1} p^{\lambda} = \tau b^{K-1} p^{\lambda_p^-(\mu)} p^{\lambda - \lambda_p^-(\mu)} = T B^{K-1} p^{\epsilon}$$

avec

$$1 - \lambda_p^-(\mu) \leq \epsilon \leq \lambda_p^-(K).$$

Enfin on peut garantir que la borne gauche est atteinte dans les encadrements si c'est le cas pour chacun des facteurs g_i de g et il suffit pour cela que b ait un facteur commun avec chacune des périodes de ces facteurs irréductibles. □

6.3.1 Premier critère pour les corps finis

Nous étendons d'abord le critère donné par le théorème de Christol, Kamae, Mendès France et Rauzy, dans lequel la caractéristique p est exactement la base de numération B.

Théorème 27. *Si $f(z)$ est une série formelle à coefficients dans le corps $\mathbb{F}_q$, de caractéristique p, vérifiant une équation de Mahler linéaire (non triviale),*

$$\sum_{k=0}^{N} c_k(z) f(z^{B^k}) = b(z),$$

avec un second membre B-régulier et si p divise B alors $f(z)$ est B-régulière.

Démonstration. Comme nous l'avons déjà dit, nous pouvons supposer $c_0 \neq 0$, ce qui permet d'utiliser le critère général. Les $g(z^{B^{K-1}}) \cdots g(z^B) g(z)$ admettent tous comme période $T B^{K-1} p^{\epsilon}$, où ϵ est défini comme dans la proposition 49. Si p divise B, nous avons $0 \leq \epsilon \leq \alpha$, en notant α la valuation p-adique de B. Comme l'application d'un opérateur de B-section divise la période par B (plus précisément la période passe de τ à $\tau/\mathrm{pgcd}(\tau, B)$) les

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B) g(z)} \right)$$

ont une période qui divise $T p^{\epsilon}$ et donc $T p^{\alpha}$. Ils sont donc tous dans un espace vectoriel de dimension finie. La B-régularité en découle. □

6.3.2 Deuxième critère pour les corps finis

Si p ne divise pas B, la démonstration ne fonctionne plus parce que le ϵ de la proposition 49 peut atteindre la valeur $\lambda_p(K)$, qui n'est pas bornée. Cependant ceci n'est qu'une majoration et si tous les facteurs irréductibles des

$$g(z^{B^{K-1}}) \cdots g(z^{B^2}) g(z)$$

sont distincts, la conclusion subsiste. C'est le cas si la partie de B étrangère à p a des diviseurs communs avec chacune des périodes des facteurs irréductibles de $g(z)$.

Théorème 28. *Soit $f(z)$ une série formelle à coefficients dans $\mathbb{F}_q$ et vérifiant une équation B-Mahler*

$$c_0(z) f(z) + c_1(z) f(z^B) + \cdots + c_N(z) f(z^{B^N}) = b(z).$$

dans laquelle

$$c_0(z) = C z^{\gamma} g(z)$$

avec C inversible, $\gamma \geq 0$, $g(0) = 1$ et $b(z)$ une série B-régulière.

Si B et chacune des périodes des facteurs irréductibles de g admettent un diviseur premier commun, autre que la caractéristique p, alors $f(z)$ est B-régulière.

Démonstration. Le dernier point de la proposition 49 montre que ϵ a la valeur minimale $1-\lambda_p^-(\mu)$ et, comme dans le premier critère, les

$$S_{r_K}\cdots S_{r_1}\left(\frac{1}{g(z^{B^{K-1}})\cdots g(z^B)g(z)}\right)$$

ont une période qui divise $Tp^{1-\lambda_p^-(\mu)}$ et sont donc dans un espace de dimension finie. □

Exemple 89 : Le polynôme $g(z)=1+z^2+z^3$ de $\mathbb{F}_2[z]$ admet la période 7. Une série formelle de $\mathbb{F}_4[[z]]$, qui vérifie une équation de la forme

$$z^\gamma(1+z^2+z^3)f(z)+c_1(z)f(z^{21})+c_2(z)f(z^{441})=b(z),$$

est donc 21-régulière. (Ici $p=2$, $q=4$, $B=21$ et $T=7$.)

Nous avons obtenu le meilleur résultat possible dans la mesure où nous ne considérons que le coefficient $c_0(z)$ dans l'équation de Mahler, comme le montre l'énoncé suivant.

Proposition 50. *Si la caractéristique du corps $\mathbb{F}_q$ ne divise pas B, si la partie de B étrangère à p est première avec l'une des périodes des facteurs irréductibles de $g(z)$, alors la série*

$$f(z)=\prod_{k\geq 0}\frac{1}{g(z^{B^k})}\in\mathbb{F}_q[[z]]$$

n'est pas $(\mathbb{F}_q,B)$-régulière.

Commençons par un exemple.

Exemple 90 : Il est bien connu de l'honorable lecteur, qui a eu la patience de nous suivre jusqu'ici, que le polynôme irréductible

$$g(z)=1+z^2+z^3\in\mathbb{F}_2[z],$$

admet la période $T=7$. Si nous prenons $B=3$, la congruence

$$B^2=9\equiv 2 \bmod 7,$$

montre que $g(z)$ est facteur de $g(z^9)$ d'après le corollaire 3 de la page 18. Il est donc aussi facteur de $g(z^{81})$, $\ldots$, $g(z^{9^\ell})$, $\ldots$ et le polynôme

$$g(z^{3^{K-1}})\cdots g(z^3)g(z)$$

a donc pour période

$$7.3^{K-1}.2^\epsilon$$

avec

$$\epsilon\geq\lambda_2(\lfloor(K+3)/2\rfloor)>-1+\log_2 K.$$

En effet d'une part $g(z^{3^k})$ a pour période $T.3^k$ et le ppcm des périodes est 7.3^{K-1}, d'autre part $g(z)$ apparaît dans un terme sur deux et donc avec une multiplicité en $K/2$, précisément $1+\lfloor(K-1)/2\rfloor$.

Les séries

$$S_{r_K}\cdots S_{r_1}\left(\frac{1}{g(z^{3^{K-1}})\cdots g(z^9)g(z)}\right)$$

ont donc une période de l'ordre de K et comme ceci n'est pas borné, elles ne sont pas dans un sous-espace vectoriel de dimension finie de $\mathbb{F}_2[[z]]$. D'après le lemme 8 page 130, la série

$$f(z)=\prod_{k\geq 0}\frac{1}{1+z^{2.3^k}+z^{3.3^k}}\in\mathbb{F}_2[[z]]$$

n'est pas ($\mathbb{F}_2$,3)-régulière.

Passons au cas général.

DÉMONSTRATION. Comme pour l'exemple précédent, il suffit de montrer que les

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B) g(z)} \right)$$

ont des périodes non bornées. On peut supposer que $g(z)$ est un polynôme irréductible car la présence de facteurs distincts ou multiples ne fait qu'accroître les périodes. D'après le corollaire 3 page 18, le polynôme $g(z)$ est facteur de $g(z^{B^k})$ si et seulement si B^k est congru à une puissance de q modulo T. Cependant p ne divise pas T (on peut montrer que T divise $q^d - 1$ si d est le degré de $g(z)$), et il suffit de prendre 1 comme puissance de q modulo T pour conclure que $g(z)$ est facteur de tous les $g(z^{B^k})$ tels que k soit multiple de l'ordre de B modulo T. Ainsi les séries

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B) g(z)} \right)$$

ont une période de l'ordre de K et le résultat en découle. □

6.3.3 Critère pour les quotients $\mathbb{Z}/(p^a)$

Pour établir des propriétés de B-régularité si l'anneau est un quotient $\mathbb{Z}/(p^a)$ avec p premier, nous utilisons encore des propriétés de périodicité. Comme nous avons déjà étudié le cas du corps $\mathbb{F}_p$, elles vont résulter du lemme suivant.

Lemme 9. *Soit p un nombre premier et $g \in \mathbb{Z}/(p^{a+1})[z]$ avec $g(0) \notin (p^a)$. Si g admet la période t dans $\mathbb{Z}/(p^a)$, alors g admet la période pt dans $\mathbb{Z}/(p^{a+1})$.*

DÉMONSTRATION. Si g admet la période t dans $\mathbb{Z}/(p^a)$, il divise $z^t - 1$ *id est*

$$z^t = 1 + g(z)h(z) + p^a m(z),$$

avec $h, m \in \mathbb{Z}/(p^{a+1})[z]$, et, en élevant à la puissance p, cela donne

$$z^{pt} = 1 + g(z)H(z) + p^{a+1}M(z) = 1 + g(z)H(z),$$

ce qui montre que pt est une période de g. □

Définition 43. *Soit $g \in \mathbb{Z}/(m)$, avec $g(0)$ inversible ; si p est un diviseur premier de m, nous notons $T(g,p)$ la période de g dans $\mathbb{Z}/(p)$.*

Proposition 51. *Soit p un nombre premier et f une série formelle sur $\mathbb{Z}/(p^a)$, qui vérifie une équation B-Mahler*

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z).$$

avec un second membre B-régulier.

Nous supposons que

1. *le coefficient de plus bas degré de c_0 est inversible dans $\mathbb{Z}/(p^a)$, id est*

$$c_0(z) = Cz^\gamma g(z)$$

   avec C inversible, $\gamma \geq 0$ et $g(0) = 1$;

2. *l'une des deux conditions suivantes est vérifiée :*

- $p \mid B$,
- *pour chaque facteur irréductible g_i de g, il existe un nombre premier p', différent de p, tel que $p' \mid B$ et $p' \mid T(g_i, p)$.*

Alors f est $(\mathbb{Z}/(p^a), B)$-régulière.

DÉMONSTRATION. D'après les conditions imposées, le polynôme $g(z^{B^{K-1}}) \cdots g(z^B)g(z)$ admet, dans $\mathbb{Z}/(p)$ la période $T(g,p)B^{K-1}p^\epsilon$ avec ϵ indépendant de K. D'après le lemme, ce polynôme admet dans $\mathbb{Z}/(p^a)$ la période $T(g,p)B^{K-1}p^{\epsilon+a}$. Il en résulte que les

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B)g(z)} \right),$$

avec $K \geq 1$, $0 \leq r_k < B$ pour $k = 1, \cdots, K$, sont toutes des séries périodiques admettant la période $T(g,p)p^{\epsilon+a}$. Elles forment donc un ensemble fini et la B-régularité de f en découle. □

6.3.4 Critère pour un anneau de caractéristique $m \neq 0$

Pour passer à un module m, qui n'est pas une puissance de nombre premier, il suffit d'utiliser la proposition qui suit et le théorème des restes chinois.

Proposition 52. *Une série formelle à coefficients dans un anneau produit de deux anneaux commutatifs est B-régulière si et seulement si ses deux séries composantes sont B-régulières.*

Si nous utilisons un anneau commutatif de caractéristique $m \neq 0$, le critère général s'applique encore en supposant que le polynôme c_0 est à coefficients dans le sous-anneau premier $\mathbb{Z}/(m)$. Ceci n'est pas une vaine généralisation puisque nous avons vu que toute suite automatique vérifie une équation de Mahler dont les coefficients sont dans le sous-anneau premier.

Théorème 29. *Soient $\mathbb{A}$ un anneau commutatif nœthérien de caractéristique*

$$m = \prod_{k=1}^{K} p_k^{a_k}$$

et f une série formelle à coefficients dans $\mathbb{A}$, qui vérifie une équation de Mahler

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z),$$

où $b(z)$ est une série B-régulière.

Nous supposons que

1. *le polynôme c_0 est à coefficients dans $\mathbb{Z}/(m)$;*
2. *le coefficient de plus bas degré de c_0 est inversible dans $\mathbb{Z}/(m)$,* id est

$$c_0(z) = Cz^\gamma g(z)$$

avec C inversible, $\gamma \geq 0$ et $g(0) = 1$;

3. *pour chaque nombre premier p_k l'une au moins des deux conditions suivantes est vérifiée :*
   - *$p_k \mid B$,*
   - *pour chaque facteur irréductible g_i de g, il existe un nombre premier p', différent de p_k, tel que $p' \mid B$ et $p' \mid T(g_i, p_k)$.*

Alors $f(z)$ est $(\mathbb{Z}/(m), B)$-régulière.

EXEMPLE 91 : Soient $\mathbb{A}$ un anneau commutatif nœthérien de caractéristique $m > 0$ et $f \in \mathbb{A}[[z]]$ une série formelle qui vérifie

$$z^\gamma(1+z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z),$$

avec un second membre B-régulier. Comme $g(z) = 1 + z$ a pour période 2 modulo tout nombre premier différent de 2, la série f est B-régulière si B est pair et à la condition que les diviseurs premiers de m soient des diviseurs premiers de B si B est impair.

EXEMPLE 92 : Considérons la suite d'entiers $(u_n)_{n\geq 0}$ définie par les conditions initiales

$$u_0 = 0, \quad u_1 = 1$$

et la relation de récurrence

$$u_n = u_{n-1} + u_{n-2} + u_{\lfloor n/2 \rfloor}.$$

Clairement u_n est plus grand que le nombre de Fibonacci F_{n-1} et la série génératrice

$$u(z) = z + 2\,z^2 + 4\,z^3 + 8\,z^4 + 14\,z^5 + 26\,z^6 + 44\,z^7 + 78\,z^8 + \cdots$$

n'est pas ($\mathbb{Z}$,2)-régulière car ses coefficients ont une croissance trop forte. Par contre réduite modulo tout entier $m \geq 2$ cette série est 2-régulière.

Si m est une puissance de 2, la caractéristique est $p = 2$ et nous sommes dans le cas où p divise B. Ainsi $u(z)$ est ($\mathbb{Z}/(2^k)$,2)-régulière pour tout k.

Si m est une puissance d'un nombre premier impair p, les périodes des facteurs du polynôme $1 - z - z^2$ modulo p sont paires, comme nous allons le voir bientôt. Ainsi le second cas du théorème s'applique et $u(z)$ est ($\mathbb{Z}/(p^k)$,2)-régulière pour tout nombre premier impair p et tout k.

La série $u(z)$ étant 2-régulière modulo tout nombre primaire, elle est 2-régulière modulo tout entier $m \geq 2$.

Il nous reste à démontrer notre assertion sur la période de $1 - z - z^2$ modulo un premier impair p. Si le polynôme $1 - z - z^2$ se factorise en $(\alpha - z)(\beta - z)$ avec $\alpha, \beta \in \mathbb{F}_p$, les deux facteurs ont pour périodes les ordres de α et β dans $\mathbb{F}_p^*$. Comme $\alpha\beta = -1$ est dans le sous-groupe engendré par α et β, ces ordres sont pairs. Si le polynôme $1 - z - z^2$ est irréductible sur $\mathbb{F}_p$, ses racines vérifient $\zeta^2 = \zeta + 1$ et donc $\zeta^{2p} = \zeta^p + 1$. Il en résulte que ζ^p est l'une des deux racines de $1 - z - z^2$. Si $\zeta^p = \zeta$ alors ζ est dans $\mathbb{F}_p$, ce qui est exclus. Il ne reste que la possibilité $\zeta^p = -1/\zeta$ et $\zeta^{p+1} = -1$, ce qui fait que ζ est d'ordre pair et la période de $1 - z - z^2$ est paire.

6.3.5 Application aux partitions B-aires

Une partition B-aire est une partition d'entier dont tous les sommants sont des puissances de B. Par exemple les partitions ternaires de 16 sont 1^{16}, $1^{13}3$, $1^{10}3^2$, 1^73^3, 1^43^4, 13^5, 1^79, 1^439, 13^29 (l'écriture s^k signifie que le sommant s apparait k fois dans la partition ; 13^29 désigne la partition $1 + 3 + 3 + 9$). Si $p_{B,n}$ est le nombre de partitions B-aires de l'entier n, nous avons donc $p_{3,16} = 9$. Plus généneralement la série génératrice $p_B(z)$ de la suite $(p_{B,n})_{n\in\mathbb{N}}$ est

$$p_B(z) = \sum_{n=0}^{+\infty} p_{B,n} z^n = \prod_{k=0}^{+\infty} \frac{1}{1 - z^{B^k}}$$

et elle vérifie l'équation de Mahler

$$(1 - z)\, p_B(z) = p_B(z^B).$$

Proposition 53. *La série des partitions B-aires, $p_B(z)$, est B-régulière modulo m si et seulement si chaque diviseur premier de m divise B.*

Démonstration. Comme $g(z) = 1-z$ a pour période 1 quel que soit l'anneau utilisé, la deuxième condition du critère ne fournit rien. Mais la première donne la B-régularité. Inversement si la série est B-régulière modulo m, elle est B-régulière modulo un diviseur premier p de m. D'après la proposition 50, il est nécessaire que chacun de ces p divise B. □

Exemple 93 : La série génératrice des partitions 6-aires est 6-régulière modulo tous les entiers de la forme $2^k 3^\ell$.

Exemple 94 : La suite du nombre de partitions binaires réduite modulo une puissance de 2 est 2-régulière. Voici la suite $(p_{2,n})$ réduite modulo 8 (chaque ligne comporte 64 termes). La pauvreté du nombre de blocs de taille donnée, typique des suites automatiques [20], saute aux yeux.

11
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446622
6644226622446644224466226644226622446622664422446644226622446644
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446644
2244662266442244664422662244662266442266224466442244662266442266
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446622
6644226622446644224466226644226622446622664422446644226622446644
2244662266442244664422662244662266442266224466442244662266442266
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446644
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446622
6644226622446644224466226644226622446622664422446644226622446644
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446644
2244662266442244664422662244662266442266224466442244662266442266
2244662266442244664422662244662266442266224466442244662266442244
6644226622446644224466226644226622446622664422446644226622446644
...

La suite $(p_{2,n})$ réduite modulo 8 peut être définie grâce au 2-automate

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & \mathbf{1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & \mathbf{1} & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 & \mathbf{1} & \mathbf{1} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \mathbf{1} & 0 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 1 & 1 & 0 & 4 & 2 & 0 & 6 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

En particulier une légère étude de cet automate montre que la valeur de $p_{2,2n}$ modulo 8 ne dépend que de la parité de la valuation dyadique, $v_2(n)$, et de la somme des bits de n , $s_2(n)$, comme indiqué ci-après.

$s_2(n)$ \ $v_2(n)$	pair	impair
pair	6	4
impair	2	4

Ceci est à rapprocher des congruences de Churchhouse [19], qui relient $p_2(4n)$ et $p_2(n)$. La preuve de Rödseth [7, p. 161] utilise clairement le opérateurs de section et revient à chercher des relations de dépendance dans le module stable engendré par $p_2(z)$ modulo une puissance de 2.

6.4 Corps algébriquement clos

Pour appliquer le critère général dans un corps algébriquement clos $\mathbb{K}$, dont la caractéristique est nulle ou ne divise pas B, nous cherchons des conditions sur les pôles des

$$S_{r_K}\left(\frac{1}{g}\left(S_{r_{K-1}}\frac{1}{g}\cdots S_{r_1}\frac{1}{g}\right)\right).$$

Théorème 30. *Soient $\mathbb{K}$ un corps algébriquement clos, dont la caractéristique est nulle ou ne divise pas B, et f une série formelle à coefficients dans $\mathbb{K}$, vérifiant une équation de Mahler*

$$c_0(z)f(z)+c_1(z)f(z^B)+\cdots+c_N(z)f(z^{B^N})=b(z)$$

dans laquelle c_0 est non nul et b est une série B-régulière.

Si c_0 n'a comme racines (hormis 0) que des racines de l'unité dont l'ordre n'est pas premier avec B, alors f est B-régulière.

Précisons que le mot ordre est pris au sens de la théorie des groupes. Une racine d'ordre a est donc ici une racine primitive a-ième de l'unité.

Démonstration. Posons, comme d'habitude,

$$c_0(z)=Cz^\gamma g(z)$$

et soit $\mathcal{Z}$ l'ensemble des racines de g. Il engendre un sous ensemble stable par $(z\mapsto z^B)$ et fini, $\mathcal{B}$, dont nous supposons, pour la commodité de la démonstration, qu'il ne comporte qu'un cycle $\mathcal{C}$.

L'hypothèse est que les racines de g, les éléments de $\mathcal{Z}$, sont dans $\mathcal{B}$ mais pas dans $\mathcal{C}$. En effet un nombre, m, qui est premier avec B divise un $B^\ell-1$ (car B est dans le groupe des inversibles modulo m). Ainsi un entier qui n'est pas premier avec B s'écrit bm, où b a des facteurs premiers qui sont des facteurs premiers de B et divise un B^k $(k\geq 1)$, et m divise un $B^\ell-1$ $(\ell\geq 1)$.

Nous allons appliquer le critère général, en montrant que les

$$S_{r_K}\cdots S_{r_1}\left(\frac{1}{g(z^{B^{K-1}})\cdots g(z^B)g(z)}\right),$$

avec $K\geq 1$ et $0\leq r_k<B$, sont dans l'espace vectoriel, de dimension $(\mu+1)\operatorname{Card}\mathcal{B}$, constitué des fractions rationnelles de partie entière nulle, dont les pôles sont dans $\mathcal{B}$ et ont un ordre plus petit que μ, si μ est l'ordre maximum des racines de g. L'idée est fort simple : l'opérateur de Mahler éloigne les racines du cycle et les opérateurs de section les en rapprochent. L'hypothèse va permettre de contrôler les ordres de multiplicité.

Soient $\mathcal{Z}_k$ l'ensemble des racines B^k-ièmes des éléments de $\mathcal{Z}$ et $\mathcal{B}_k$ la réunion de $\mathcal{B}$ et des $\mathcal{Z}_\ell$ pour $\ell=1,\cdots,k$. Les racines α de $g(z^{B^\ell})$ sont les éléments de $\mathcal{Z}_\ell$ et ont pour ordre celui de leur père d'ordre ℓ, α^{B^ℓ}, comme racine de g. Donc

$$g(z^{B^{K-1}})\cdots g(z^B)g(z)$$

a des racines qui sont dans $\mathcal{Z} \cup \mathcal{Z}_1 \cdots \cup \mathcal{Z}_{K-1}$. De plus ces racines ont une multiplicité inférieure à μ. En appliquant un opérateur de B-section S_{r_1}, les racines font toutes un pas vers le cycle $\mathcal{C}$ et prennent la place de leur père. Elles reçoivent comme ordre le maximum des ordres de leur fratrie, donc au plus μ pour les pères des éléments de $\mathcal{Z}$ comme pour les éléments de $\mathcal{Z} \cup \mathcal{Z}_1 \cup \cdots \cup \mathcal{Z}_{K-2}$. En appliquant ensuite S_{r_2}, $\cdots$, S_{r_K}, toutes les racines vont revenir dans $\mathcal{B}$ (et même $\mathcal{B}$ privé des éléments les plus éloignés du cycle). En outre les ordres de multiplicité sont toujours majorés par μ et cette borne sera atteinte si K est assez grand, car tous les éléments de $\mathcal{C}$ ont alors un ordre qui vaut μ. □

Exemple 95 : Appelons I_n (respectivement P_n) le nombre de coefficients binomiaux impairs (resp. pairs) dans la ligne d'indice n du triangle de Pascal. Les deux séries génératrices associées sont respectivement ($s(n)$ est la somme des bits de n) [66]

$$I(z) = \sum_{n\geq 0} 2^{s(n)} z^n = \prod_{k\geq 0} \left(1 + 2z^{2^k}\right),$$

$$P(z) = \sum_{n\geq 0} (n + 1 - 2^{s(n)}) z^n = \frac{1}{(1-z)^2} - I(z).$$

Les deux séries sont 2-régulières parce que $I(z)$ et $1/(1-z)^2$ le sont [6, p. 188], d'ailleurs $I(z)$ vérifie

$$I(z) = (1 + 2z) I(z^2)$$

et le critère s'applique, mais $P(z)$ vérifie

$$(1 - z^2)^2 P(z) = (1 - z^2)^2 (1 + 2z) P(z^2) + z^2$$

et le critère ne convient pas.

Cependant l'équation minimale homogène de $P(z)$ est

$$z^2 P(z) - [(1 + z^2)^2 + z^2(1 + 2z)] P(z^2) + (1 + z^2)^2 (1 + 2z^2) P(z^4) = 0$$

et les conditions d'application du critère sont satisfaites.

Exemple 96 : Si B vaut 2, les racines de l'unité qui nous intéressent sont celles qui ont un ordre pair, c'est-à-dire -1, i, $-i$, $-j$, $-j^2$, *etc.* Ainsi une série formelle f vérifiant

$$(1 + z) f(z) + c_1(z) f(z^2) + \cdots + c_N(z) f(z^{2^N}) = 0$$

est 2-régulière, le prototype étant $1 - z$.

Exemple 97 : Toujours avec $B = 2$, considérons la suite (u_n) définie par

$$u_0 = 0, \;\; u_1 = 1, \;\; u_2 = 2$$

et la relation de récurrence

$$u_n = -u_{n-3} + u_{\lfloor n/2 \rfloor}, \;\; \text{pour} \;\; n \geq 3.$$

Sa série génératrice est solution de

$$(1 + z^3) u(z) = (1 + z) u(z) + z(1 + z)$$

c'est-à-dire

$$(1 - z + z^2) u(z) = z + u(z^2),$$

donc est ($\mathbb{Z}$,2)-régulière, puisque les racines du coefficient $c_0(z) = 1 - z + z^2$ sont les racines de l'unité d'ordre 6.

Une fois de plus les conditions du théorème ne sont que suffisantes. Cependant le résultat obtenu est le meilleur possible, si nous nous limitons à considérer le coefficient $c_0(z)$.

Proposition 54. *Si certaines racines de $c_0(z)$ ne sont pas des racines de l'unité ou sont des racines de l'unité dont l'ordre est premier avec B, le produit infini*

$$f(z) = \prod_{k\geq 0} \frac{1}{c_0(z^{B^k})}$$

vérifie l'équation

$$c_0(z)f(z) = f(z^B)$$

mais n'est pas B-régulier.

Démonstration. Pour obtenir ce résultat, nous utilisons encore la formule

$$S_{r_K}\cdots S_{r_1} f(z) = \left(S_{r_K}\cdots S_{r_1} \prod_{0\leq k<K} \frac{1}{c_0(z^{B^k})} \right) f(z).$$

Si $c_0(z)$ possède des racines qui ne sont pas racines de l'unité, nous considérons l'une d'elles, α, dont aucune des puissances B-ièmes itérées α^B, α^{B^2}, ... n'est racine de $c_0(z)$. Alors

$$S_{r_K}\cdots S_{r_1} \frac{1}{c_0(z)\cdots c_0(z^{B^{K-1}})}$$

admet pour pôle α^{B^K} et en faisant varier K, nous obtenons une infinité de pôles. L'ensemble de ces fractions rationnelles ne peut pas être dans un module de type fini car il n'y aurait alors qu'un ensemble fini de pôles.

Si $c_0(z)$ n'a comme racines que des racines de l'unité mais dont l'une au moins a un ordre premier avec B, nous considérons une telle racine α. Pour K assez grand la fraction

$$S_{r_K}\cdots S_{r_1} \frac{1}{c_0(z)\cdots c_0(z^{B^{K-1}})}$$

admet pour pôles tous les éléments du B-cycle défini par α. Ici nous utilisons donc un ensemble fini de pôles, mais en faisant croître K, nous augmentons indéfiniment les ordres de ces pôles et ceci empêche à nouveau que ces fractions restent dans un module de type fini. □

Dans le cas où le corps de référence est le corps des nombres complexes, nous pouvons aussi employer des arguments de croissance. Par exemple, si a est premier avec B, le produit infini

$$\prod_{k=0}^{+\infty} \frac{1}{\Phi_a(z^{B^k})},$$

où $\Phi_a(z)$ est le polynôme cyclotomique d'indice a, n'est pas B-régulier car ses coefficients ne sont pas $O(n^\alpha)$, mais ont une croissance en $\exp(\ln^2 n)$ comme nous le verrons dans la troisième partie.

6.5 Différents types de récurrence

Les deux derniers chapitres ont été consacrés au lien entre les récurrences typiques des suites régulières et les récurrences mahlériennes. Notre but est ici de bien faire sentir au lecteur les différences de nature entre ces types de récurrence. Nous supposons que l'anneau de référence est un corps et nous prenons souvent $B = 2$ pour simplifier.

Nous avons vu que les récurrences typiques des séries régulières relient u_n, u_{2n}, u_{2n+1}, u_{4n}, ... et que l'on peut imposer de prendre un système de relations, qui d'une part garantit que la suite est bien définie et d'autre part n'est pas redondant. De plus la taille d'un tel système est exactement le rang de la série augmenté de 1. En pratique il est bien rare que l'on parte d'un tel système.

Par exemple au code Gray est associé la fonction g qui à un entier n associe la valeur en binaire standard de l'écriture Gray de n. On peut définir cette fonction par les formules [32, chap. 3]

$$g(0) = 0, \quad g(2^k + n) = 2^k + g(2^k - 1 - n) \text{ si } 0 \le n < 2^k.$$

Comme la suite $(g(n))$ est 2-régulière de rang 3, on peut aussi donner un système de 4 équations qui la définit complètement,

$$\begin{aligned} g(4n) &= 2\,g(2n), \\ g(4n+1) &= -4\,g(n) + 3\,g(2n) + g(2n+1), \\ g(4n+2) &= -4\,g(n) + g(2n) + 3\,g(2n+1), \\ g(4n+3) &= 2\,g(2n+1). \end{aligned}$$

Ce système est typique d'une suite 2-régulière et correspond aux récurrences dont nous avons parlé dans le chapitre 3.

On peut aussi jouer sur le fait que la série est de rang 3 pour obtenir une récurrence d'une forme légérement différente et moins systématique,

$$\begin{aligned} g(8n) &= 4\,g(2n), \\ g(8n+1) &= -4\,g(n) + 5\,g(2n) + g(2n+1), \\ g(8n+2) &= -2\,g(8n) + 3\,g(8n+1), \\ g(8n+3) &= -g(8n) + 2\,g(8n+1), \\ g(8n+4) &= 16\,g(n) - 16\,g(2n) + 6\,g(4n+1), \\ g(8n+5) &= -g(8n) + g(8n+1) + g(8n+4), \\ g(8n+6) &= g(8n) - g(8n+1) + g(8n+4), \\ g(8n+7) &= 2\,g(8n) - 2\,g(8n+1) + g(8n+4). \end{aligned}$$

Remarquons que si toutes les équations étaient de la même forme que les trois dernières, nous aurions affaire à une série rationnelle.

À côté de cela, nous avons rencontré des récurrences mahlériennes

$$u_n = \sum_{j=1}^{J} a_j u_{n-j} + \sum_{k=1}^{K} b_k u_{\lfloor n/2^k \rfloor} + \sum_{\ell=1}^{L} c_\ell u_{\lceil n/2^\ell \rceil} + \sum_{m=1}^{M} d_m u_{n/2^m},$$

où $u_x = 0$ si x n'est pas entier naturel. Le fait d'utiliser des u_x, $u_{\lfloor x \rfloor}$ ou $u_{\lceil x \rceil}$ ne change rien qualitativement ; nous obtenons toujours une équation de Mahler,

$$(1 - a(z))u(z) = b(z) + \sum_{i=1}^{N} p_i(z) u(z^{2^i}),$$

pour la série génératrice.

Nous avons vu que toute suite régulière vérifie une récurrence mahlérienne ; par exemple la suite $(g(n))$ associée au code Gray est solution de la récurrence

$$g(n) = -g(n-3)$$

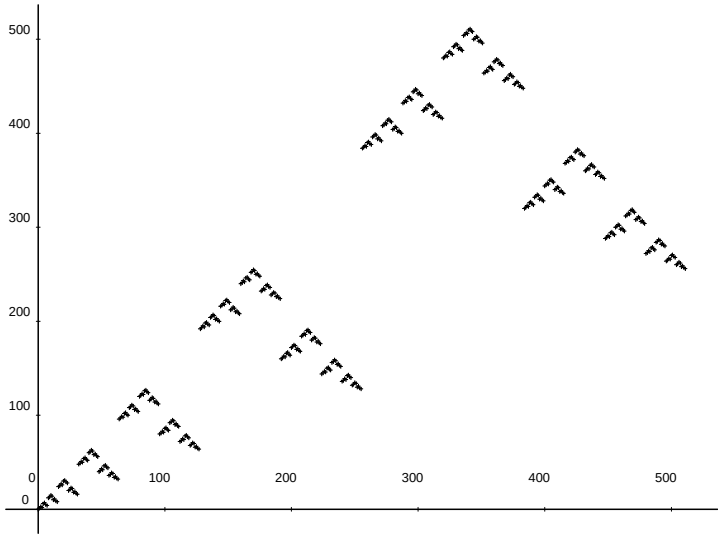

FIG. 6.2
La suite du code Gray montre une répétition de motifs typique des suites B-régulières. De plus l'aspect *réfléchi* du code Gray saute aux yeux.

$$+ g(n/2) + 3\,g((n-1)/2) + 2\,g((n-2)/2) + 2\,g((n-3)/2) + 3\,g((n-4)/2) + g(n-5)/2)$$
$$+ 2\,g(n/4) + 2\,g((n-1)/4) + 2\,g((n-2)/4) + 2\,g((n-3)/4) + 2\,g((n\ -4)/4)$$
$$+ 2\,g((n-5)/4) + 2\,g((n-6)/4) + 2\,g((n-7)/4)$$

ou encore, avec un traitement par cas,

$$\begin{aligned}
g(4n) &= -g(4n-3) + g(2n) + 2\,g(2n-1) + 3\,g(2n-2) + 2\,g(n) + 2\,g(n-1),\\
g(4n+1) &= -g(4n-2) + 3\,g(2n) + 2\,g(2n-1) + g(2n-2) + 2\,g(n) + 2\,g(n-1),\\
g(4n+2) &= -g(4n-1) + g(2n+1) + 2\,g(2n) + 3\,g(2n-1) + 2\,g(n) + 2\,g(n-1),\\
g(4n+3) &= -g(4n) + 3\,g(2n+1) + 2\,g(2n) + g(2n-1) + 2\,g(n) + 2\,g(n-1).
\end{aligned}$$

La présence des termes en $4n-3$, $2n-1$, $2n-2$, ... fait que ce système ne donne pas une récurrence typique de séries 2-régulières et est donc qualitativement différent du premier que nous avons donné.

Ce dernier chapitre avait pour but de formuler une réciproque, c'est-à-dire de caractériser les récurrences mahlériennes qui peuvent s'écrire sous forme de récurrence régulière. Nous avons essentiellement rencontré trois cas. D'abord le cas facile : si la récurrence est de la forme

$$u_n = c_{1,0}\,u_{n/2} + c_{1,1}\,u_{(n-1)/2} + \cdots + c_{2,0}\,u_{n/4} + \cdots$$

alors la suite est 2-régulière. Ensuite la généralisation directe du théorème de Christol, Kamae, Mendès France et Rauzy : si le corps est fini et si sa caractéristique divise B, alors la suite est B-régulière. Enfin plusieurs cas (corps fini ou corps algébriquement clos), que nous pouvons regrouper en un seul : si la relation de récurrence linéaire

$$r_n = a_1\,r_{n-1} + a_2\,r_{n-2} + \cdots + a_m\,r_{n-m}$$

définit des suites périodiques et si la période T n'est pas première avec B, alors la suite est B-régulière. Cette formulation est réductrice, car les pôles des fractions rationnelles utilisées ne sont pas nécessairement simples et les suites peuvent avoir une complexité un peu plus grande que la simple périodicité. Cependant ce dernier cas et cette image nous semblent exprimer au mieux la nature des suites B-régulières. Elles vérifient des relations de récurrence perturbées par rapport au cas classique,

$$u_n = a_1\, u_{n-1} + a_2\, u_{n-2} + \cdots + a_m\, u_{n-m} + c_{1,0}\, u_{n/B} + c_{1,1}\, u_{(n-1)/B} + \cdots ,$$

mais la perturbation est en résonance avec la récurrence classique. Il en résulte que les suites B-régulières ont un comportement qui, au premier abord, peut sembler périodique parce qu'il y a une répétition de motifs. Cet aspect est bien sensible sur la figure 6.2, qui illustre la fonction g du code Gray.

Troisième partie

Aspect asymptotique

Le comportement asymptotique des suites mahlériennes est fondamental en analyse d'algorithmes, où abondent les récurrences *diviser pour régner*, comme dans le tri-fusion, les réseaux de tri ou la transformation de Fourier discrète. La combinatoire fournit aussi des suites mahlériennes dont l'étude asymptotique a suscité de nombreuses recherches, par exemple celles liées aux partitions binaires ou aux dénombrements en rapport avec l'écriture binaire des entiers. En toute généralité ces suites ont un comportement complexe et des variations souvent violentes, mais les exemples issus de la nature se laissent apprivoiser et montrent un comportement assez régulier.

On peut distinguer essentiellement deux classes. D'un côté sont les suites à croissance lente, c'est-à-dire ici de type polynomial. Cette classe comprend avant tout les suites B-régulières. Un des points frappants de leur comportement est la présence de fluctuations périodiques, qui se traduit par une autosimilitude de leur graphe. D'autre part sont des suites à croissance rapide, soit de type exponentiel comme les suites rationnelles, soit de type subexponentiel mais surpolynomial en $\exp(\ln^2 n)$. Ce dernier type est mathématiquement le plus intéressant de cette classe, par les techniques qu'il utilise. Ici encore on rencontre des fluctuations périodiques, mais il se présente une superposition entre l'invariance par changement d'échelle et une périodicité de nature arithmétique.

Notre approche est fondée sur un théorème de factorisation qui amène à étudier d'abord les séries B-régulières puis des produits infinis mahlériens. Pour celles-ci les méthodes de théorie analytique des nombres et spécialement les formules de Mellin-Perron permettent d'obtenir des développements asymptotiques complets moyennant quelques conditions techniques qui sont réalisées dans la pratique. Le dernier chapitre, le chapitre 8, illustre le cas des produits infinis. Une méthode de col dans le contexte d'une infinité de cols, couplée avec une analyse locale fondée sur la transformation de Mellin, fournit un développement asymptotique complet. On peut parler de méthode du cercle à la Hardy et Ramanujan, mais les développements analytiques sont très différents.

La complexité des suites mahlériennes exclut la possibilité de ramener systématiquement leur comportement à un petit nombre de formes asymptotiques classiques, comme pour les fonctions rationnelles, algébriques ou holonomes. Cependant nous décrivons un certain nombre de cadres typiques dans lesquels l'analyse asymptotique est réalisable et ces cas sont les plus importants dans les applications rencontrées jusqu'ici.

Chapitre 7

Asymptotique des suites mahlériennes

Le but de ce chapitre est de présenter quelques idées générales utiles dans l'étude du comportement asymptotique des suites mahlériennes à valeurs complexes. En pratique nous aurons souvent affaire à des suites à valeurs rationnelles voire entières. Toute série mahlérienne est le quotient d'une série B-régulière et d'un produit infini et ce théorème de structure conduit à une classification un peu simpliste, mais qui permet d'attaquer le problème. En premier lieu sont donc les séries B-régulières, dont l'asymptotique a déjà donné lieu a de nombreux exemples dans la littérature. Leur traitement repose soit sur des méthodes élémentaires soit sur des techniques de la théorie analytique des nombres comme la formule de Perron. Les deux approches sont complémentaires et si notre préférence va clairement à la seconde qui fait espérer un traitement unifié, il n'en reste pas moins que les techniques élémentaires permettent de dégrossir le problème et de préparer l'application de techniques plus sophistiquées. Nous nous appesantissons sur deux points ; d'une part l'ordre de croissance des suites B-régulières et l'abscisse de convergence de la série de Dirichlet associée, d'autre part le prolongement méromorphe de cette série et la répartition de ses pôles. Ces quantités dépendent essentiellement des valeurs propres des matrices d'une représentation linéaire.

Le domaine des produits infinis mahlériens, $\prod 1/\phi(z^{B^k})$, est moins bien défriché. Certains types sont surabondamment représentés alors que d'autres semblent avoir été negligés jusqu'ici. On rencontre deux cas dans la nature. Dans le premier, le polynôme $\phi(z)$ n'a que des racines de module strictement plus petit que 1 et le produit infini définit une fonction méromorphe dans le disque unité, dont les pôles s'agglutinent sur le cercle unité. Ce cas, que nous baptisons *cas interne*, est sans grand mystère et la méthode de soustraction des singularités [42, chap. 11] suffira à le traiter. Le second, le *cas modulaire* dans lequel les racines du polynôme $\phi(z)$ sont de module 1, se réduisait jusqu'ici à l'exemple des partitions B-aires d'entiers. Ce sujet a déjà été étudié par de nombreux auteurs, comme K. Mahler et ceci justifie en partie que nous appelions *mahlériennes* les séries qui nous occupent. Le dernier chapitre, qui est le fruit d'une collaboration avec Ph. Flajolet et l'application de ses idées, prolonge les travaux de N. G. De Bruijn sur ce sujet. Comme on le voit, ceci n'épuise pas les possibilités et nous introduisons aussi le *cas externe*, pour lequel nous ne donnons qu'un résultat grossier.

7.1 Classification

D'après l'étude menée au chapitre 3, l'équation minimale d'une série mahlérienne,

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z),$$

a un coefficient $c_0(z)$ qui n'est pas nul et sa résolution se scinde en deux parties : d'abord le traitement d'un système linéaire qui donne la dimension de l'espace des solutions et la partie basse des solutions puis l'application d'une récurrence mahlérienne qui permet de calculer autant de termes que l'on veut de la partie haute. On peut encore dire que cette deuxième phase est la recherche d'un point fixe par itération d'un opérateur contractant dans l'espace des séries formelles et il en résulte que les solutions définissent des fonctions méromorphes dans le disque unité, qui ne peuvent avoir comme pôles que les zéros du coefficient $c_0(z)$ et leurs racines B-ièmes itérées. Nous allons étendre et préciser ce résultat en insistant particulièrement sur l'analyticité des solutions.

Soit donc une série mahlérienne $f(z)$ solution de l'équation

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z)$$

dans laquelle $c_0(z)$ est non nul, les $c_k(z)$ sont des polynômes et $b(z)$ est une série B-régulière. En reprenant les notations employées dans la preuve du théorème 6 page 46, où nous nous limitions à prendre pour $b(z)$ un polynôme, nous avons

$$f(z) = \underline{f}(z) + z^{D-\delta_0+1}F(z),$$

si $\underline{f}(z)$ désigne la partie basse et $F(z)$ la partie haute de $f(z)$. Cette partie haute vérifie l'équation contractante

$$C_0(z)F(z) = E(z) + \sum_{k=1}^{N} z^{\lambda_k} C_k(z) F(z^{B^k}),$$

dans laquelle les λ_k sont supérieurs ou égaux à 1, les C_k ont une valuation nulle et $E(z)$ est une série B-régulière.

Rappelons que nous avons défini une famille de polynômes, qui devient ici une famille de séries B-régulières, (u_w) de valuation nulle et une famille d'entiers (n_w) indexées par les mots sur $[1, N]$, en posant, si $E(z)$ est de valuation β et $E(z) = z^\beta \tilde{E}(z)$,

$$u_\epsilon(z) = \tilde{E}(z), \quad u_{kw}(z) = C_k(z)u_w(z^{B^k}),$$

$$n_\epsilon = \beta, \quad \text{et } n_{kw} = \lambda_k + Bn_w.$$

Ainsi la partie haute s'exprime formellement par

$$F(z) = \sum_{w\in[1,N]^*} \frac{z^{n_w} u_w(z)}{\prod_{j=0}^{|w|} C_0(z^{B^j})},$$

la somme étant indexée par les mots w sur l'alphabet $[1, N]$.

Posons maintenant

$$\rho\, C_0(z) = \Gamma(z),$$

de façon que $\Gamma(0) = 1$ et soit

$$G(z) = F(z) \prod_{j\geq 0} \Gamma(z^{B^j}).$$

Le produit infini $\prod \Gamma(z^{B^j})$ est B-régulier et définit une fonction analytique dans le disque unité. Quant à la série $G(z)$, elle est donnée par le développement

$$G(z) = \sum_{w\in[1,N]^*} z^{n_w} u_w(z)\, \rho^{|w|+1} \prod_{j>|w|} \Gamma(z^{B^j})$$

et définit une fonction analytique dans le disque unité, car elle converge normalement dans tout disque centré à l'origine et de rayon $\rho < 1$, comme on le voit par de grossières majorations du même type que celles de la page 46. D'autre part $G(z)$ satisfait l'équation

$$G(z) = \rho E(z) \prod_{j\geq 1} \Gamma(z^{B^j}) + \sum_{k=1}^{N} z^{\lambda_k} \left[C_k(z) \prod_{1\leq j<k} \Gamma(z^{B^j}) \right] G(z^{B^k}).$$

Cette équation mahlérienne ressortit au critère facile du chapitre 6, car le coefficient de $G(z)$ est 1 et le second membre est B-régulier comme produit de la série B-régulière $\rho E(z)$ et d'un produit infini évidemment B-régulier. La série $G(z)$ est donc B-régulière.

La série $f(z)$, qui était notre point de départ, s'écrit

$$f(z) = \underline{f}(z) + z^{D-\delta_0+1} \frac{G(z)}{\prod_{j\geq 0} \Gamma(z^{B^j})}.$$

En réduisant au même dénominateur, nous obtenons, avec

$$H(z) = \underline{f}(z) \prod_{j\geq 0} \Gamma(z^{B^j}) + z^{D-\delta_0+1} G(z),$$

la formule

$$f(z) = \frac{H(z)}{\prod_{j\geq 0} \Gamma(z^{B^j})}.$$

Comme la série $H(z)$ est évidemment B-régulière et analytique dans le disque unité, nous aboutissons ainsi à un théorème de structure des séries mahlériennes.

Théorème 31 (Théorème de structure)**.** *Une série mahlérienne est le quotient d'une série et d'un produit infini qui sont B-réguliers et analytiques dans le disque unité.*

Si $f(z)$ est solution de l'équation mahlérienne

$$c_0(z)f(z) + c_1(z)f(z^B) + \cdots + c_N(z)f(z^{B^N}) = b(z),$$

où $c_0(z) \neq 0$, les $c_k(z)$ sont des polynômes et $b(z)$ est une série mahlérienne, alors il existe une série B-régulière $H(z)$ telle que

$$f(z) = \frac{H(z)}{\prod_{j\geq 0} \Gamma(z^{B^j})},$$

en notant $c_0(z) = \rho\, z^{\delta_0}\Gamma(z)$, avec $\rho \neq 0$ et $\Gamma(0) = 1$,

Nous avons légérement modifié l'étude de la page 46 en n'imposant pas que $b(z)$ soit un polynôme, mais seulement une série B-régulière. Bien entendu, toute série mahlérienne vérifie une équation homogène et nous pourrions imposer $b(z) = 0$. Autoriser une plus grande complexité dans le second membre permet d'abaisser l'ordre de l'équation et évite d'introduire des racines parasites dans le coefficient $c_0(z)$.

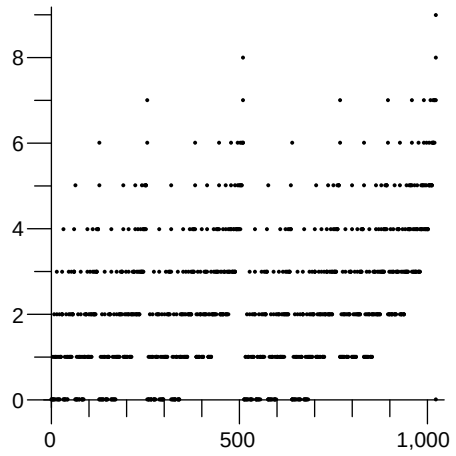

FIG. 7.1
La suite $(e_{11}(n))$ associe à un entier le nombre d'occurrences du motif 11 dans son écriture binaire. Son comportement asymptotique est bien difficile à décrire même si l'on comprend sa structure globale. Le graphique fait sentir une certaine périodicité en $\lg n$, si l'on superpose, avec un changement d'echelle adéquat, les tranches limitées par deux puissances de 2 consécutives.

7.2 Séries B-régulières

La classification qui est le cadre de ce chapitre confine pour beaucoup la difficulté dans l'étude des suites régulières, puisque pour les trois autres cas nous disposons d'une expression explicite en produit infini. D'ailleurs on peut à bon droit s'interroger sur la pertinence d'un développement asymptotique pour certaines suites à l'aspect assez chaotique comme la suite $(e_{11}(n))$ qui donne le nombre d'apparitions du motif 11 dans l'écriture binaire d'un entier n (cf. figure 7.1).

En pratique on est amené à lisser ces suites par application de l'opérateur de sommation. Par exemple la suite $(\nu(n))$ qui donne la somme des bits d'un entier a des variations violentes mais la suite $(S(n))$ qui représente la somme de tous les bits des entiers entre 1 et n a un comportement assez lisse puisque [27]

$$S(n) = \frac{1}{2}\, n \lg n + o(n \lg n).$$

Remarquons d'abord qu'une suite régulière (u_n) vérifie $u_n = O(n^\alpha)$ pour un certain α [6]. Cette majoration permet de considérer la série de Dirichlet

$$u(s) = \sum_{n=1}^{+\infty} \frac{u_n}{n^s}.$$

Une technique utilisée systématiquement par Flajolet *et alii* [33, 34], dans l'étude de certaines sommes liées aux développements binaires et qui sont en fait des suites 2-régulières, consiste à

invoquer la formule de Perron [8, 68] dans la version

$$\sum_{1\le k<n}\left(1-\frac{k}{n}\right)\,v_k=\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}v(s)n^s\frac{ds}{s(s+1)}.$$

Idéalement cette formule s'applique à la série génératrice des différences secondes et les singularités de l'intégrande sont connues, ce qui permet par des calculs de résidus d'obtenir une série asymptotique comme approximation de u_n. Dans les bons cas ce développement est même convergent.

En pratique $v(s)$ est plutôt la série génératrice des différences premières et on a donc un développement asymptotique pour la fonction sommatoire de la suite (u_n). Considérons par exemple [34, p. 8] le nombre γ_n de 1 dans la représentation en code Gray, le code binaire réfléchi, de l'entier n. La suite des différences arrière $\delta_n=\gamma_n-\gamma_{n-1}$ vérifie $\delta_{2k}=\delta_k$ et $\delta_{2k+1}=(-1)^k$. Sa série de Dirichlet est donc

$$\delta(s)=\frac{2^s\,L(s)}{2^s-1}\qquad\text{avec}\qquad L(s)=\sum_{k=0}^{+\infty}\frac{(-1)^k}{(2k+1)^s}.$$

D'après la formule de Perron, la fonction sommatoire

$$G_N=\sum_{n<N}\gamma_n$$

est donnée par

$$G_N=\frac{N}{2i\pi}\int_{2-i\infty}^{2+\infty}\frac{2^s\,L(s)}{2^s-1}\,N^s\frac{ds}{s(s+1)}.$$

L'intégrande est méromorphe avec un pôle double en 0 de résidu

$$\frac{1}{2}\lg N+\lg\{\Gamma(1/4)/\Gamma(3/4)\}-\frac{3}{4}-\frac{1}{2\ln 2},$$

un pôle simple en chaque $\chi_k=2ik\pi/\ln 2$ et un pôle simple en -1. Rappelons que lg est le logarithme en base 2. On trouve ainsi

$$G_N=\frac{1}{2}\,N\lg N+N\,F(\lg N)$$

où $F(u)$ est une fonction 1-périodique donnée par la série de Fourier

$$F(u)=2\lg\Gamma\left(\frac{1}{4}\right)-\frac{3}{2}-\lg\pi+\frac{1}{\ln 2}\sum_{k\neq 0}\frac{L(\chi_k)}{\chi_k(\chi_k+1)}\,\exp(2ik\pi u).$$

Evidemment la série de Fourier provient des pôles χ_k et c'est leur disposition régulière qui produit une fonction périodique.

7.2.1 Abscisse de convergence absolue

L'abscisse de convergence absolue de la série de Dirichlet et l'ordre de croissance de la suite sont liés et interviennent de façon importante dans l'application de la formule de Perron. Comme pouvait le faire penser [30], ces quantités dépendent des valeurs propres des matrices d'une représentation linéaire réduite de la suite.

Définition 44. *Le rayon spectral, $\rho(u)$ ou ρ, d'une suite B-régulière (u_n) est le maximum des rayons spectraux des matrices d'une représentation linéaire réduite A_0, A_1, ..., c'est-à-dire le maximum des modules des valeurs propres des A_r. Si la suite est de rang N, l'infimum sur toutes les normes de $\mathbb{C}^N$ du maximum des normes des matrices d'une représentation réduite, $\max_r\|A_r\|$, est noté $\rho_+(u)$ ou ρ_+.*

Cette définition est correcte parce que deux représentations linéaires réduites sont semblables : les spectres sont les mêmes et un changement de bases fait passer d'une norme à une autre. Remarquons d'ailleurs que l'utilisation de représentations linéaires non réduites ne fait qu'introduire des valeurs propres supplémentaires [13, p. 39] et augmente les normes.

Rappelons que $\lambda_B(n)$ ou plus simplement $\lambda(n)$ est le nombre de chiffres de l'écriture de l'entier n en base B et que $\lambda(n)$ vaut $\log_B n$ à 1 près. En conséquence $\rho^{\lambda(n)}$ est équivalent à l'infini à $n^{\log_B \rho}$.

Proposition 55. *Une suite B-régulière de rang N et de représentation linéaire réduite A_0, A_1, ..., λ, γ, satisfait*

$$|u_n| \leq \|\lambda\|\|\gamma\|\rho_+(u)^{\lambda(n)}.$$

Démonstration. Munissons l'espace $\mathbb{C}^N$ d'une norme $\|\ \|$. La même notation, $\|\ \|$, désigne la norme induite sur les endomorphismes de $\mathbb{C}^N$, c'est-à-dire les matrices de type $N \times N$, et sur le dual de $\mathbb{C}^N$, c'est-à-dire les matrices lignes. Si un entier n s'écrit en base B

$$\tilde{n} = \epsilon_\ell \cdots \epsilon_0,$$

le terme d'indice n de la suite vaut

$$u_n = \lambda A_{\epsilon_\ell} \cdots A_{\epsilon_0} \gamma,$$

et une majoration brutale donne

$$|u_n| \leq \|\lambda\|\|A_{\epsilon_\ell}\| \cdots \|A_{\epsilon_0}\|\|\gamma\|,$$

c'est-à-dire

$$|u_n| \leq \|\lambda\|\|\gamma\| \prod_{0 \leq r < B} \|A_r\|^{|\tilde{n}|_r}.$$

Il suffit alors de majorer chaque norme $\|A_r\|$ par la plus grande d'entre elles. De plus le raisonnement est indépendant de la norme de $\mathbb{C}^N$ utilisée, ce qui permet de majorer encore par la borne inférieure des majorants obtenus. □

Ce résultat est décevant car les exemples tirés de la nature faisaient plutôt espérer un énoncé du type suivant.

Une suite B-régulière (u_n) de rayon spectral $\rho(u)$ vérifie, pour tout $\epsilon > 0$, une inégalité

$$|u_n| \leq C[\rho(u) + \epsilon]^{\lambda(n)},$$

où C est une constante qui dépend de ϵ mais pas de n.

Cependant cet énoncé simple et de bon goût est faux, comme le montre l'exemple suivant.

Exemple 98 : Considérons la suite 2-régulière (u_n) définie par la représentation linéaire non standard (nous supposons α et β non nuls),

$$A_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \alpha \\ 0 & 0 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & \beta & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Comme on le voit, cette représentation est fondée sur l'utilisation de matrices nilpotentes. Avec $r = \alpha\beta$, la série génératrice ordinaire est

$$f(z) = z + z^2 + z^4 + rz^5 + z^8 + rz^{10} + z^{16} + rz^{20} + r^2z^{21} + z^{32}$$

$$+ rz^{40} + r^2z^{42} + z^{64} + rz^{80} + r^2z^{84} + r^3z^{85} + \cdots$$

et son rang est 4. Nous préférons employer une représentation standard comme

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & r & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 & 1 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Le rayon spectral est évidemment 1. Les puissances de 2 fournissent la valeur 1 ; les entiers de la forme $n = 1 + 4 + \cdots + 4^k$ donnent $u_n = r^k$ et le choix de α et β est arbitraire. Il semble donc que la considération du rayon spectral ne soit pas adéquate.

Cependant en posant $A'_0 = A_0A_0$, $A'_1 = A_0A_1$, $A'_2 = A_1A_0$, $A'_3 = A_1A_1$, nous obtenons une représentation linéaire standard en base 4, parce que la précédente est standard en base 2. Qui plus est cette nouvelle représentation est réduite. Les matrices

$$A'_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \quad A'_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & r & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$A'_2 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & r & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A'_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

donnent un rayon spectral, le maximum de 1 et $|r|$, qui correspond au bon ordre de croissance.

Ce dernier exemple montre qu'il peut être utile de considérer non seulement les représentations en base B mais aussi en base B^2, B^3, *etc.* En augmentant la longueur des produits, on peut espérer faire croître le rayon spectral de la représentation et diminuer les normes. Le résultat précédent donne une majoration avec un nouveau et meilleur ρ_+ qui vaut

$$\inf_{\ell} \inf_{\|\ \|} \max_{|w|=\ell} \|A_w\|^{1/\ell}.$$

Nous avons tendance à penser que ceci n'est pas trop loin du supremum sur ℓ des rayons spectraux des représentations réduites en base B^ℓ.

La recherche d'un minorant nécessite un petit rappel d'algèbre. Le passage à la forme normale de Jordan pour une matrice A revient à décomposer l'espace en une somme directe de sous-espaces stables par l'opérateur A. Précisément chaque bloc de taille t

$$J(\mu, t) = \begin{pmatrix} \mu & 1 & & & \\ & \mu & 1 & & \\ & & \ddots & \ddots & \\ & & & \mu & 1 \\ & & & & \mu \end{pmatrix},$$

correspond à un sous-espace stable dans lequel l'opérateur induit par $A - \mu I_t$ est nilpotent d'indice t. Ce sous-espace est A-cyclique, ou A-monogène suivant les auteurs, engendré par un vecteur κ.

Avec l'écriture que nous avons choisi pour le bloc $J(\mu,t)$, le vecteur κ est le dernier vecteur de base e_t et la base est donnée par $(A-\mu)e_t = e_{t-1}$, $(A-\mu)e_{t-1} = e_{t-2}$, *etc.* La présence d'un tel bloc implique que $(X-\mu)^t$ divise le polynôme minimal de A. Pour ℓ plus grand que t, la puissance ℓ-ième de $J(\mu,t)$ s'écrit

$$J(\mu,t)^\ell = \begin{pmatrix} \mu^\ell & \ell\mu^{\ell-1} & \binom{\ell}{2}\mu^{\ell-2} & \cdots & \binom{\ell}{t-1}\mu^{\ell-t+1} \\ & \mu^\ell & \ell\mu^{\ell-1} & \ddots & \\ & & \ddots & \ddots & \\ & & & \mu^\ell & \ell\mu^{\ell-1} \\ & & & & \mu^\ell \end{pmatrix}$$

et le terme dominant du point de vue asymptotique ($\mu \neq 0$),

$$\binom{\ell}{t-1}\mu^{\ell-t+1} \underset{\ell\to+\infty}{\sim} \frac{1}{(t-1)!\mu^{t-1}}\,\mu^\ell \ell^{t-1},$$

est la composante de $A^\ell\kappa$ sur $e_1 = (A-\mu)^{t-1}\kappa$.

Définition 45. *L'ordre de multiplicité, $\tau(u)$ ou τ, d'une suite B-régulière (u_n) est la taille maximale des blocs de Jordan relatifs aux valeurs propres de module $\rho(u)$ dans les formes normales de Jordan des matrices d'une représentation linéaire réduite A_0, A_1, ... de la suite. C'est encore le maximum des ordres de multiplicité dans les polynômes minimaux des A_r des valeurs propres de module $\rho(u)$.*

Exemple 99 : Considérons la suite (T_n) liée au coût du tri fusion dans le cas le pire. Elle admet la représentation linéaire réduite et standard (cf. page 83)

$$A_0 = \begin{pmatrix} 0 & 0 & 4 & 4 & 12 \\ 1 & 0 & -5 & -8 & -16 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 5 & 6 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & -12 & -4 & -36 \\ 0 & 0 & 15 & 6 & 48 \\ 1 & 0 & -3 & -6 & -16 \\ 0 & 0 & -5 & -2 & -16 \\ 0 & 1 & 3 & 5 & 11 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Les deux matrices A_0 et A_1 ont pour formes normales de Jordan

$$J_0 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad J_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

Pour chacune d'elles la valeur propre qui fournit le rayon spectral est 2 et il y a exactement un bloc de Jordan associé, qui est de taille 2. Ainsi la suite (T_n) a pour rayon spectral $\rho = 2$ et pour ordre de multiplicité $\tau = 2$.

Il faut faire ici une petite remarque technique. Dans la partie 2, nous avons considéré des suites B-régulières (u_n) dont le premier terme u_0 n'avait aucune raison d'être nul. Ici nous considérons la

série de Dirichlet associée et donc la suite (v_n) définie par $v_0 = 0$ et $v_n = u_n$ si $n \geq 1$. Ce changement modifie *a priori* le rang, les valeurs propres, les multiplicités de celles-ci, mais certainement pas le comportement asymptotique. Or nous sommes en train de relier celui-ci et celles-là. Une discussion similaire à celle de la page 70, où nous comparions les opérateurs S_0 et S'_0, montre que la suite (v_n) admet une représentation A'_0, A'_1, …, λ', γ', avec

$$A'_0 = \left(\begin{array}{c|c} A_0 & 0 \\ \hline & 1 \end{array}\right), \quad A'_r = \left(\begin{array}{c|c} A_r & 0 \\ \hline & 0 \end{array}\right),$$

pour $0 < r < B$, si (u_n) admet la représentation linéaire A_0, A_1, …, λ, γ. Il en résulte que le rang de (v_n) est à 1 près celui de (u_n), car les deux suites jouent des rôles symétriques. Surtout le rayon spectral et la multiplicité sont conservés, car la valeur propre 1 figure déjà dans A_0 et nous ajoutons seulement un bloc de Jordan de taille 1. D'ailleurs le nombre $\rho_+(u)$ n'est pas modifié non plus. Plus généralement, cette argumentation montre que le fait de modifier les premiers termes de la suite (u_n) ne change pas les nombres $\rho(u)$, $\rho_+(u)$ et $\tau(u)$; leur utilisation dans l'étude asymptotique de cette suite n'est donc pas une incohérence.

Nous mettons en place une classification, qui va permettre, dans la majorité des cas, de fournir une minoration d'une suite B-régulière (u_n) valable pour une infinité de n.

Définition 46. *Soit (u_n) une suite B-régulière de rayon spectral ρ, de multiplicité τ et dont A_0, A_1, …, λ, γ est une représentation linéaire réduite.*

- *Nous disons que la suite (u_n) ressortit au cas marginal si elle vérifie les conditions suivantes.*
  1. *Il n'y a qu'une valeur propre μ des A_r qui réalise le rayon spectral ($|\mu| = \rho$) et il n'y a qu'un bloc de Jordan relatif à μ, dans les formes normales de Jordan des A_r, qui a la taille τ.*
  2. *Cet unique bloc $J(\mu, \tau)$ est associé à la matrice A_0.*
  3. *Le vecteur κ qui engendre le sous-espace associé au bloc $J(\mu, \tau)$ vérifie*

$$\lambda A_v (A_0 - \mu)^{\tau - 1} \kappa = 0,$$

  pour tout mot v qui n'est pas dans x_0^*.
- *La suite (u_n) appartient au cas hypermarginal si elle réunit les conditions suivantes.*
  1. *Il n'y a qu'une valeur propre, μ, qui réalise le rayon spectral et elle est simple.*
  2. *Cette valeur propre n'apparaît que dans le spectre de A_0.*
  3. *Le vecteur propre κ relatif à μ vérifie*

$$\lambda A_v \kappa = 0,$$

  pour tout mot v qui n'est pas dans x_0^*.
- *La suite (u_n) rentre dans le cas ordinaire si elle n'appartient pas au cas marginal.*

Exemple 100 : Considérons le cas des suites nulles à partir d'un certain rang. En terme de série génératrice ordinaire, il s'agit des polynômes. Il est facile de constater qu'un polynôme $f(z)$ de degré d est une série B-régulière de rang au moins $\lambda(d)+1$ [13, p. 114]. De plus les opérateurs de section d'indice non nul induisent sur le sous-espace stable par section engendré par $f(z)$ des opérateurs nilpotents car $S_r^{\lambda(d)+1} g(z) = 0$ pour

$r \neq 0$ et $g(z)$ polynôme de degré au plus d. Pour l'opérateur de section S_0, nous remarquons de la même façon que $(S_0 - 1)S_0^{\lambda(d)} g(z) = 0$ si $g(z)$ est un polynôme de degré au plus d car $S_0^{\lambda(d)} g(z)$ est une constante. Ainsi la valeur propre 1 est simple et zéro est valeur propre de multiplicité $\mathrm{rg}(f) - 1$.

Le rayon spectral est donc 1 et la multiplicité τ vaut 1, puisque la valeur propre 1 est simple. Si nous utilisons une représentation linéaire réduite A_0, A_1, …, λ, γ, la série $f(z)$ correspond au vecteur colonne γ et la série 1 correspond à une constante près au vecteur colonne $\kappa = A_0^{\lambda(d)}\gamma$. Ce κ est donc un vecteur propre de A_0 relatif à la valeur propre 1. Cependant toute application d'un opérateur de section S_r avec r non nul annule la série 1, ce qui fait que $A_v\kappa = 0$ et *a fortiori* $\lambda A_v \kappa = 0$ pour tout mot v qui n'est pas dans x_0^*. Ainsi les suites nulles à partir d'un certain rang entrent dans le cas hypermarginal.

La terminologie que nous employons exprime l'espoir que le cas marginal n'est pas fréquent et que le cas hypermarginal se réduit quasiment aux suites nulles à partir d'un certain rang. Rien n'est moins sûr, et il serait peut être utile de tenir compte du second module des valeurs propres. Cependant la difficulté qu'il y a de construire une représentation réduite satisfaisant toutes les contraintes du cas marginal ou du cas hypermarginal nous fait espérer que la nature, qui sait rester simple dans sa splendeur, ne nous poussera pas dans cette nécessité. D'autre part la recherche du cas dans lequel entre une suite B-régulière donnée est aisée en pratique.

Exemple 101 : Considérons la suite 2-régulière (u_n) définie par la représentation réduite standard

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Les valeurs propres de A_0 sont 1 et 2 et celles de A_1 sont 0, 1, $-j$ et $-j^2$. Le module maximum correspond donc à la valeur propre 2 de A_0, qui est simple. Nous avons donc $\rho = 2$ et $\tau = 1$. Le vecteur κ, vecteur propre de A_0 relatif à la valeur propre 2, est le troisième vecteur de base. Dans ce cas particulier, si la suite est marginale, elle est hypermarginale. La troisième condition de la définition signifie alors que A_0, A_1, λ, κ est une représentation linéaire de la série 1, c'est-à-dire de la suite 1, 0, 0, 0, *etc.* Comme celle-ci est de rang 1, il suffit de calculer les termes de la suite définie par A_0, A_1, λ, κ jusqu'au rang 31, d'après le théorème d'égalité (cf. page 86). Or les premières valeurs sont

$$0,\ 0,\ 0,\ 1,\ 0,\ 1,\ 2,\ 3,\ 0,\ 1,\ \ldots$$

et la suite ressortit donc au cas ordinaire. Comme nous allons le voir, ceci implique que u_n a un comportement en n pour une infinité d'entiers n (cf. figure 7.2).

Proposition 56. *Soit (u_n) une suite B-régulière de rayon spectral ρ et d'ordre de multiplicité τ.*

Si la suite est de type ordinaire, il existe une infinité d'entiers n et une constante non nulle, C, telles que

$$|u_n| \geq C\, \rho^{\lambda(n)}\, \lambda(n)^{\tau-1}.$$

Si la suite n'est pas de type hypermarginale, il existe une infinité d'entiers n et une constante non nulle, C, telles que

$$|u_n| \geq C\, \rho^{\lambda(n)}.$$

La démonstration est un peu technique et nous allons commencer par un exemple.

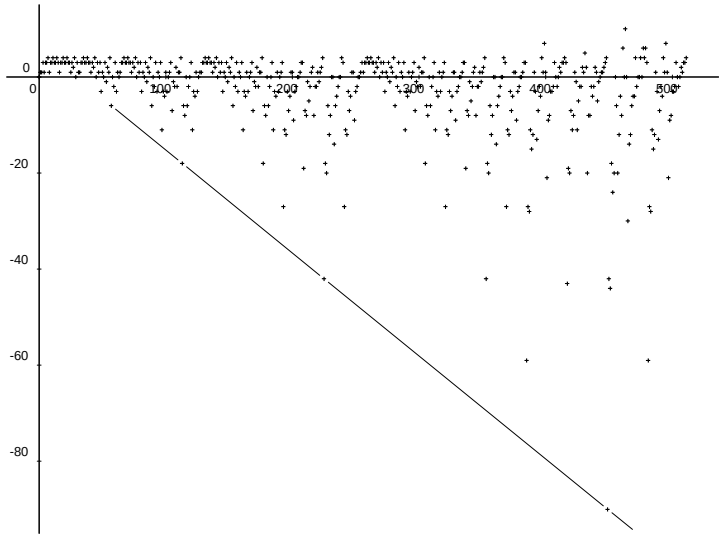

FIG. 7.2
La suite définie par la représentation linéaire réduite

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

est de type ordinaire. Elle n'a qu'une valeur propre dominante, 2, qui est simple. Nous attendons donc un comportement en $2^{\lambda(n)}\lambda(n)^0 \asymp n$ pour une infinité d'entiers. Ce comportement apparaît par exemple pour les entiers $7.2^\ell + 1$, d'écriture binaire $1^3 0^\ell 1$, comme on le constate sur le dessin.

EXEMPLE 102 : Nous avons donné page 156 une représentation linéaire réduite de la suite (T_n) liée au tri fusion. En conservant les mêmes notations, nous pouvons utiliser A_0 ou bien A_1 pour notre propos, car ces deux matrices ont un bloc de Jordan de taille 2 relatif à la valeur propre 2. Nous choisissons arbitrairement A_0. La matrice de passage P tel que $P^{-1}J_0P = A_0$ est

$$P = \begin{pmatrix} 1/2 & 1/2 & -2/25 & 1/2 & -1/2 \\ 0 & 0 & 1/2 & 0 & 1 \\ -4/25 & -3/25 & -3/25 & 4/25 & 4/25 \\ 1/5 & 2/5 & 2/5 & 4/5 & 4/5 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

La matrice J_0^ℓ vaut

$$J_0^\ell = \begin{pmatrix} 1 & \ell & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2^\ell & 2^{\ell-1}\ell & 0 \\ 0 & 0 & 0 & 2^\ell & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

et la matrice $A_0^\ell = P^{-1} J_0^\ell P$ est donc

$$\begin{pmatrix} 4-3\,2^\ell+2\,2^{\ell-1}\ell & 4-4\,2^\ell+4\,\ell 2^{\ell-1} & 4+4\,\ell-4\,2^\ell+4\,2^{\ell-1}\ell & 4-4\,2^\ell+8\,2^{\ell-1}\ell & 4+8\,\ell-4\,2^\ell+8\,2^{\ell-1}\ell \\ 4\,2^\ell-4-3\,2^{\ell-1}\ell & 5\,2^\ell-4-6\,2^{\ell-1}\ell & -5-4\,\ell+5\,2^\ell-6\,2^{\ell-1}\ell & 4\,2^\ell-4-12\,2^{\ell-1}\ell & -4-8\,\ell+4\,2^\ell-12\,\ell 2^{\ell-1} \\ 0 & 0 & 1 & 0 & 0 \\ 1-2^\ell+2^{\ell-1}\ell & 1-2^\ell+2\,2^{\ell-1}\ell & 1+\ell-2^\ell+2\,2^{\ell-1}\ell & 1+4\,2^{\ell-1}\ell & 2\,\ell+4\,2^{\ell-1}\ell \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Cette dernière matrice comporte des termes en $2^{\ell-1}\ell$. Choisissons arbitrairement une colonne qui comporte de tels termes, par exemple la troisième. Cette troisième colonne s'extrait en multipliant à droite par le troisième vecteur de base, qui est $A_1 A_0 \gamma$,

$$A_0^\ell A_1 A_0 \gamma = \begin{pmatrix} 4+4\,\ell-4\,2^\ell+4\,2^{\ell-1}\ell \\ -5-4\,\ell+5\,2^\ell-6\,2^{\ell-1}\ell \\ 1 \\ 1+\ell-2^\ell+2\,2^{\ell-1}\ell \\ 0 \end{pmatrix}.$$

Les coefficients de $2^{\ell-1}\ell$ dans ce dernier vecteur fournissent le vecteur

$$\begin{pmatrix} 4 \\ -6 \\ 0 \\ 2 \\ 0 \end{pmatrix},$$

qui est proportionnel à la troisième colonne de la matrice

$$P^{-1} = \begin{pmatrix} 8 & 8 & 10 & -7 & 16/25 \\ -8 & -8 & -15 & 8 & -41/25 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 1 & 5 & -1 & 33/50 \\ 0 & 1 & 0 & 0 & -1/2 \end{pmatrix}.$$

D'ailleurs ceci est vrai quel que soit la colonne choisie, parce qu'il n'y a qu'un bloc de Jordan de taille 2 relatif à la valeur propre 2. Ce vecteur n'est rien d'autre que $(A_0 - 2)\kappa$ en appelant κ le quatrième vecteur colonne de P^{-1}, qui engendre le sous-espace relatif à ce bloc de taille 2. La forme linéaire de vecteur ligne

$$\lambda A_1 = \begin{pmatrix} 0 & 1 & 3 & 5 & 11 \end{pmatrix}$$

ne s'annule pas sur ce vecteur des coefficients de $2^{\ell-1}\ell$, ce qui implique que cette suite ressortit au cas ordinaire. Nous obtenons ainsi

$$\lambda A_1 A_0^\ell A_1 A_0 \gamma = 3 + \ell + 4\,2^{\ell-1}\ell$$

et le coefficient de $2^{\ell-1}\ell$ n'est pas nul. Ceci montre que

$$T_{2^{\ell+2}+2} \underset{\ell\to+\infty}{\sim} 4\,2^{\ell-1}\ell.$$

Passons maintenant au cas général.

Démonstration. Nous choisissons une représentation linéaire réduite, standard et typique, comme au chapitre 4 section 4.4. La dimension de cette représentation linéaire A_0, A_1, …, λ, γ est N et A_w désigne le produit $A_{w_\ell} \cdots A_{w_1}$ si w est le mot $w_\ell \cdots w_1$.

Le point crucial est que l'ensemble des $A_w\gamma$ avec $w \in \mathcal{X}^*$ engendre $\mathbb{C}^{N\times 1}$ et l'ensemble des λA_w avec $w \in \mathcal{X}^*$ engendre $\mathbb{C}^{1\times N}$ parce que la représentation est réduite [13, p. 37]. Plus précisément le ressort de la démonstration est la proposition 28 de la page 86.

Commençons par une version approximative, que nous critiquerons ensuite. Parmi les matrices A_0, A_1, ..., il est possible de choisir une matrice, disons A, qui donne un bloc de Jordan relatif à une valeur propre μ de module ρ de taille maximale τ. Ce bloc correspond à un sous-espace de $\mathbb{C}^N$ engendré par un certain vecteur κ et une base de ce sous-espace est constituée de κ, $(A-\mu)\kappa$, ..., $(A-\mu)^{\tau-1}\kappa$. Pour ℓ plus grand que τ, les matrices A^ℓ comportent des coefficients en $\mu^\ell\ell^{\tau-1}$. Si de tels coefficients apparaissent dans la colonne j, nous utilisons un mot w tel que $A_w\gamma$ soit le j-ième vecteur de base $\mathbb{C}^{N\times 1}$. La multiplication de la matrice A^ℓ à droite par le j-ième vecteur de base, qui est $A_w\gamma$, fournit un vecteur de $\mathbb{C}^{N\times 1}$, dont certains coefficients sont en $\mu^\ell\ell^{\tau-1}$. Le vecteur des coefficients de ce $\mu^\ell\ell^{\tau-1}$ est $(A-\mu)^{\tau-1}\kappa$ et son orthogonal est un hyperplan de $\mathbb{C}^{1\times N}$. Nous pouvons trouver un mot v tel que $\lambda A_v(A-\mu)^{\tau-1}\kappa$ ne soit pas nul, parce que les λA_w engendrent l'espace $\mathbb{C}^{1\times N}$ et ne sont donc pas tous dans un hyperplan. Le produit $\lambda A_v A^\ell A_w\gamma$ est la valeur de la suite sur un entier $n = B^\ell n_0 + t$ si n_0 est la valeur du mot v et t est la valeur du mot w. Cette valeur s'exprime par une combinaison linéaire des coefficients de A^ℓ qui comporte effectivement un terme en $\mu^\ell\ell^{\tau-1}$ et en faisant varier ℓ, nous obtenons bien une infinité d'entiers n pour lesquels u_n vérifie une inégalité

$$|u_n| \geq C\,\rho^{\lambda(n)}\,\lambda(n)^{\tau-1}.$$

A dire vrai, il y a quelques points douteux dans ces affirmations. D'abord il se pourrait que le mot v commence par des 0 et ne fournisse pas une écriture d'entier. Ceci est un faux problème parce que la représentation est standard et la relation $\lambda A_0 = \lambda$ permet d'éliminer les zéros de tête.

Ensuite il se pourrait que le seul mot v, ne commençant pas par des zéros et tel que $\lambda A_v(A-\mu)^{\tau-1}\kappa$ ne soit pas nul, ce mot donc soit le mot vide. Si la suite est de type ordinaire, un terme en $\mu^\ell\ell^{\tau-1}$ est tout de même garanti. En effet ou bien nous utilisons un bloc de Jordan d'une matrice A_r qui n'est pas A_0 et même si v est le mot vide nous avons une écriture d'entier ; ou bien nous sommes obligés de prendre la matrice A_0 mais il y a plusieurs blocs de Jordan adéquats, les deux vecteurs $(A-\mu)^{\tau-1}\kappa$ sont indépendants, leur orthogonal est de dimension $N-2$ et il est impossible que seul parmi les λA_v le vecteur ligne λ ne soit pas dans cet orthogonal ; ou bien nous devons prendre la matrice A_0, elle n'a qu'un bloc de Jordan adéquat, mais il existe un mot v qui comporte des chiffres non nuls tel que $\lambda A_v(A-\mu)^{\tau-1}\kappa$ ne soit pas nul.

Si la suite est dans le cas marginal sans être dans le cas hypermarginal, il est encore possible de garantir un terme en μ^ℓ. Si le bloc de Jordan relatif à μ a une taille τ qui vaut au moins deux, nous utilisons $(A-\mu)^{\tau-2}\kappa$ au lieu de $(A-\mu)^{\tau-1}\kappa$ et comme ces deux vecteurs sont indépendants, nous sommes certains de trouver un mot v, qui n'est pas dans 0^*, pour lequel $\lambda A_v(A-\mu)^{\tau-2}\kappa$ n'est pas nul, ce qui donne un terme en $\mu^\ell\ell^{\tau-2}$. Si la valeur propre μ est simple, il est possible de trouver, d'après le point *3.* de la définition du cas marginal, un mot v, qui à nouveau n'est pas dans 0^*, et pour lequel $\lambda A_v\kappa$ n'est pas nul d'où un terme en μ^ℓ.

Enfin, si la forme normale de Jordan de la matrice A ne comporte qu'un bloc de taille τ relatif aux valeurs propres de module ρ ou s'il y en a plusieurs mais tous relatifs à la même valeur propre μ de module ρ, la conclusion est atteinte, car nous avons, pour le cas ordinaire, une égalité asymptotique de la forme

$$u_n \sim C\mu^\ell\ell^{\tau-1}$$

pour tous les $n = B^\ell n_0 + t$. Il faut préciser que la constante C qui apparaît dans cette égalité asymptotique est non nulle parce que, même s'il y a plusieurs valeurs propres à considérer, les vecteurs propres utiles sont indépendants, ce qui empêche les phénomènes d'annulation. Cependant il se pourrait qu'à la matrice A correspondent plusieurs blocs de taille τ relatifs à différentes valeurs propres μ_1, ..., μ_m de module ρ. Dans ce cas le raisonnement donne seulement, dans le cas ordinaire,

$$u_n = C_1\mu_1^\ell\ell^{\tau-1} + \cdots + C_m\mu_m^\ell\ell^{\tau-1} + o(\rho^\ell\ell^{\tau-1}),$$

avec des C_k non nuls. En simplifiant par $\rho^\ell\ell^{\tau-1}$ et en mettant en valeur les arguments, qui sont distincts deux à deux modulo 2π, nous sommes ramenés à prouver qu'il existe une constante C tels que

$$\left|C_1e^{i\ell\alpha_1} + \cdots + C_me^{i\ell\alpha_m}\right| \geq C$$

pour une infinité de ℓ. Le cas marginal non hypermarginal amène la même remarque et le petit lemme technique qui suit permet de conclure, pour le cas ordinaire comme pour le cas marginal non hypermarginal.

En effet ce lemme montre que la somme

$$C_1 e^{i\ell\alpha_1} + \cdots + C_m e^{i\ell\alpha_m}$$

tend en moyenne de Cesàro vers la somme des $|C_k|^2$ et ne tend donc pas vers 0, ce qui est exactement la propriété demandée. □

Lemme 10. *Soient C_1, ..., C_m des nombres complexes non nuls et α_1, ..., α_m des réels non congrus modulo 2π. Le polynôme trigométrique*

$$f(t) = C_1 e^{i\alpha_1 t} + \cdots + C_m e^{i\alpha_m t}$$

vérifie

$$\lim_{N\to+\infty} \frac{1}{N} \sum_{n=0}^{N-1} |f(n)|^2 = \lim_{T\to+\infty} \frac{1}{T} \int_0^T |f(t)|^2\, dt = \sum_{k=1}^{m} |C_k|^2.$$

Démonstration. Le module au carré de $f(n)$ vaut

$$|f(n)|^2 = \sum_k |C_k|^2 + \sum_{k\neq\ell} C_k \overline{C_\ell}\, e^{in(\alpha_k-\alpha_\ell)}.$$

Par hypothèse aucune des différences $\alpha_k - \alpha_\ell$ n'est congrue à 0 modulo 2π et il en résulte que les sommes

$$\sum_{n=0}^{N-1} e^{in(\alpha_k-\alpha_\ell)}$$

restent des $O(1)$ quand N tend vers l'infini. Ainsi

$$\frac{1}{N} \sum_{n=0}^{N-1} |f(n)|^2$$

tend vers la somme des $|C_k|^2$, qui est la moyenne quadratique de $f(t)$. □

En fait, tout nous pousse à croire que $\rho^{\lambda(n)}\lambda^{\tau-1}(n)$, ou si l'on préfère $n^{\log_B \rho} \log_B^{\tau-1} n$, est le bon ordre de grandeur de la suite (u_n), disons génériquement. Ceci signifie que la suite a un équivalent asymptotique

$$u_n \sim n^{\log_B \rho} \log_B^{\tau-1} n\ F(\log_B n),$$

avec une fonction F qui est 1-périodique à cause des relations de récurrence vérifiées par la suite (u_n). Bien entendu ce résultat est encore hors d'atteinte, mais tous les exemples issus de la nature corroborent ce sentiment.

Exemple 103 : Le nombre de coefficients binomiaux impairs dans les n premières lignes du triangle de Pascal vaut [66]

$$u_n = \sum_{0\leq k<n} 2^{\nu(k)}.$$

La suite (u_n) est 2-régulière de rang 2 et admet la représentation réduite

$$A_0 = \begin{pmatrix} 3 & 6 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & -6 \\ 1 & 5 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

La matrice A_0 a évidemment comme valeur propre 3 et 1 et A_1 a pour valeur propre 2 et 3, ce qui fait que $\rho(u) = 3$. De plus les deux matrices sont diagonalisables et $\tau = 1$. Nous attendons donc un comportement en $n^{\lg 3}$. Effectivement Stolarsky a montré que

$$\frac{1}{3}\, n^{\lg 3} < u_n < 3\, n^{\lg 3}$$

et Flajolet *et alii* ont précisé ce résultat [34].

Exemple 104 : Nous avons déjà donné (cf. page 108) une représentation réduite de la suite 2-régulière (u_n) qui à un entier n associe le nombre de facteurs de longueur n du mot de Thue-Morse. Les réduites de Jordan associées sont

$$J_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad J_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

et le rayon spectral vaut donc $\rho = 2$ avec $\tau = 1$. Nous attendons un comportement en n. De Luca et Varricchio [25, p. 341] ont montré que

$$3\, n \leq u_n \leq \frac{10}{3}\, n.$$

Théorème 32. *L'abscisse de convergence absolue σ_a de la série de Dirichlet associée à une suite B-régulière de rayon spectral $\rho(u)$, qui n'est pas hypermarginale, vérifie*

$$0 \leq \log_B \rho(u) \leq \sigma_a \leq 1 + \log_B \rho_+(u).$$

Démonstration. L'inégalité $|u_n| \leq C\, \rho_+(u)^{\lambda(n)}$ donne, pour s de partie réel σ,

$$\left|\frac{u_n}{n^s}\right| \leq C\, \frac{n^{\log_B \rho_+(u)}}{n^\sigma}$$

et la série de Dirichlet converge absolument si $\sigma > 1 + \log_B \rho_+(u)$. Nous avons ainsi $\sigma_a \leq 1 + \log_B \rho_+(u)$.

Inversement, si la suite n'est pas hypermarginale, la minoration $|u_n| \geq C\, \rho(u)^{\lambda(n)}$, valable pour une infinité d'entiers, donne une inégalité

$$\left|\frac{u_n}{n^s}\right| \geq C'\, \frac{n^{\log_B \rho(u)}}{n^\sigma}$$

et il ne peut y avoir convergence que si ce dernier terme a pour limite 0, ce qui impose $\sigma > \log_B \rho(u)$ et fournit $\sigma_a \geq \log_B \rho(u)$.

La minoration par 0, vient du fait que 1 est toujours valeur propre de la matrice A_0, avec les notations usuelles, ce qui garantit l'inégalité $\rho(u) \geq 1$. □

Exemple 105 : Si (u_n) est B-régulière, il en est de même de la suite $(\alpha^{\lambda(n)} u_n)$. On peut ainsi décaler l'abscisse de convergence de la série de Dirichlet associée de $\log_B |\alpha|$.

La fonction ζ de Riemann correspond à la suite de rang 2 définie par la représentation

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Nous avons $\rho = 1$, $\tau = 1$ et le cas est ordinaire. L'abscisse de convergence absolue est $\sigma_a = 1$, c'est-à-dire la borne supérieure dans l'encadrement précédent.

Dans l'autre sens, la suite caractéristique des puissances de 2 est de rang 2, admet la représentation

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

et fournit la série

$$\sum_{k\geq 0} \frac{1}{2^{ks}}.$$

Ici encore le cas est ordinaire, $\rho = 1$, $\tau = 1$ et l'abscisse de convergence absolue, $\sigma_a = 0$, est la borne inférieure de l'encadrement précédent.

7.2.2 Demi-réseaux

L'apparition d'une fonction périodique est usuelle dans l'étude du comportement des suites B-régulières. Cela tient à la disposition régulière des singularités dans l'intégrande de la formule de Perron, comme le montre le résultat suivant qui est bien connu des régularistes patentés [5] mais ne semble pas avoir été énoncé dans toute sa généralité jusqu'ici. Remarquons que l'ordre d'un pôle χ est majoré par k s'il est de multiplicité 0, 1, ... ou k. Si l'ordre est 0, alors χ n'est pas pôle.

Théorème 33 (Théorème des demi-réseaux)**.** *Soit $u(s)$ la série de Dirichlet associée à une suite B-régulière, dont une représentation linéaire réduite est A_0, A_1, ... Cette série se prolonge en une fonction méromorphe dans le plan complexe. Les pôles de ce prolongement sont dans les demi-réseaux gauches obtenus en translatant d'un entier négatif les logarithmes en base B des valeurs propres non nulles de la matrice $Q = A_0 + A_1 + \cdots$. De plus les ordres des pôles sont majorés par les ordres de multiplicité des valeurs propres correspondantes comme racines du polynôme caractéristique de Q.*

L'apparition de la matrice Q n'est pas nouvelle. Nous avons considéré, page 92, la condensée d'une série B-régulière $f(z)$,

$$Kf(t) = \sum_{\ell\geq 1} \left(\sum_{B^{\ell-1}\leq n<B^{\ell}} f_n \right) t^{\ell}.$$

En explicitant les termes de la suite (f_n) en fonction d'une représentation linéaire A_0, A_1, ..., la condensée s'exprime sous la forme

$$\begin{aligned} Kf(t) &= \sum_{\ell\geq 1} \sum_{\epsilon_0,\ldots,\epsilon_{\ell-1}} \lambda A_{\epsilon_{\ell-1}} \cdots A_{\epsilon_1} \gamma \, t^{\ell} \\ &= t\,\lambda \sum_{\ell\geq 1} \left(t\,[A_0 + \cdots + A_{B-1}]\right)^{\ell-1} \ \gamma \\ &= t\,\lambda\,[I_N - t\,Q]^{-1}\,\gamma \\ &= \frac{t}{\chi_Q(t)}\,\lambda\,C(t)\gamma\ , \end{aligned}$$

si $C(t)$ est la comatrice de $I - tQ$ et $\chi_Q(t)$ le polynôme caractéristique de Q. Ainsi les pôles de la série de Dirichlet sont parmi les logarithmes des pôles de la série condensée et leurs décalés vers la gauche.

DÉMONSTRATION. Dans l'espace vectoriel stable par section défini par la suite, nous considérons une base constituée de sous-suites de la suite (u_n), plus précisément de sections de la suite, comme indiqué dans le théorème des récurrences typiques page 84. Sans perte de généralité, (u_n) est le premier élément de la base. Les matrices A_0, A_1, ... sont les matrices des opérateurs de section dans cette base.

Introduisons ensuite les séries de Dirichlet $u_1(s), \dots, u_N(s)$ associées aux différentes suites qui constituent la base. En particulier $u_1(s)$ est la série associée à la suite (u_n). L'utilisation de sous-suites garantit que toutes ces séries ont une abscisse de convergence absolue inférieure à σ_a, l'abscisse de convergence absolue de $u_1(s)$. Nous pouvons donc considérer le vecteur ligne de série de Dirichlet

$$U(s) = \begin{pmatrix} u_1(s) & \dots & u_N(s) \end{pmatrix},$$

qui est analytique dans le demi-plan droit $\sigma > \sigma_a$, en notant σ la partie réelle de s comme il est d'usage.

Chaque série $u_i(s)$, composante de $U(s)$, se décompose en B séries de Dirichlet, suivant les résidus modulo B des indices,

$$u_i(s) = \sum_{n\geq 0} \frac{u_{i,n}}{n^s} = \sum \frac{u_{i,Bn}}{(Bn)^s} + \sum \frac{u_{i,Bn+1}}{(Bn+1)^s} + \cdots .$$

Le développement des $1/(1+r/Bn)^s$ par la formule du binôme donne un développement uniformément convergent en n,

$$\frac{1}{\left(1+\dfrac{r}{Bn}\right)^s} = 1 - \frac{r\,s}{B}\,\frac{1}{n} + \frac{r\,s(s+1)}{2\,B^2}\,\frac{1}{n^2} + \cdots + \frac{(-1)^k\,r^k}{B^k}\binom{s+k-1}{k}\frac{1}{n^k} + \cdots$$

et des séries de la forme

$$\frac{(-1)^k\,r^k}{B^k}\binom{s+k-1}{k}\sum_n \frac{u_{i,Bn+r}}{n^{s+k}}.$$

Les $u_{i,Bn+r}$ s'expriment linéairement en les $u_{j,n}$ grâce aux matrices A_r et nous obtenons ainsi

$$U(s)(B^s\,\mathrm{I}_N - Q) = B^s \sum_{r=1}^{B-1} \frac{U_r}{r^s} + \sum_{r=1}^{B-1}\sum_{k=1}^{+\infty}(-1)^k\binom{s+k-1}{k}\left(\frac{r}{B}\right)^k U(s+k)A_r,$$

avec $Q = A_0 + A_1 + \cdots$. Le second membre de cette égalité converge normalement pour $\sigma \geq \sigma_a - 1 + \epsilon$, parce que $U(s)$ a une limite quand σ tend vers $+\infty$, et définit donc une fonction, $V(s)$, analytique dans le demi-plan $\sigma > \sigma_a - 1$. La multiplication à gauche par la comatrice $C(B^s)$ de $B^s\,I_N - Q$ fournit l'égalité

$$\det(B^s\,I_N - Q)\,U(s) = C(B^s)\,V(s),$$

ce qui montre que $U(s)$ vérifie une équation fonctionnelle infinie. Cette équation permet de prolonger $U(s)$ en une fonction méromorphe dans le plan complexe, par une récurrence qui fait gagner une unité vers la gauche à chaque pas. Les seuls pôles possibles de $U(s)$ sont les s tels que B^s soit valeur propre de Q et leurs décalés vers la gauche par un entier. Quand aux ordres de multiplicités, il proviennent des ordres de multiplicité de B^s comme racine du polynôme caractéristique de Q. Il faut toutefois remarquer qu'il peut y avoir des phénomènes de superposition des demi-réseaux.

Enfin les valeurs propres de Q sont indépendantes de la représentation réduite utilisée puisque deux telles représentations sont semblables. □

EXEMPLE 106 : Soit ω une racine B-ième de l'unité et $u(s)$ la série de Dirichlet

$$u(s) = \sum_{n\geq 1} \frac{\omega^{\nu(n)}}{n^s},$$

où $\nu(n)$ est la somme des chiffres de n en base B. La suite $(\omega^{\nu(n)})$ est B-régulière de rang 1 (ou 2 si on annule le terme d'indice 0) avec des matrices A_r qui se réduisent aux nombres ω^r.

Si $\omega = 1$, la matrice Q est le nombre B et nous attendons des pôles, au plus simples, en les $1 + 2ik\pi - \ell$ avec k entier relatif et l entier naturel. Comme $u(s)$ est la fonction ζ de Riemann, seul 1 est réellement pôle.

Si ω est une racine B-ième de l'unité différente de 1, la matrice Q est le nombre 0 et la fonction $u(s)$ est entière, comme l'indique Allouche et Cohen [5, p. 533].

Exemple 107 : Nous considérons des déplacements sur la demi-droite des entiers naturels. Le point de départ est 0 et le point d'arrivée un entier n. Les déplacements se font par des sauts vers l'avant ou l'arrière et d'amplitude des puissances de 2. L'écriture binaire de n fournit une trajet en $\nu(n)$ sauts, le nombre de bits de valeur 1 dans n. Cependant nous cherchons le trajet le court, c'est-à-dire avec le nombre minimum de sauts, que nous appelons w_n. Ainsi pour $n = 14$, l'écriture binaire $14 = 8 + 4 + 2$ donne un trajet en 3 sauts, mais avec $14 = 16 - 2$ nous avons un trajet en $w_{14} = 2$ sauts, ce qui est bien le minimum car 14 n'est pas une puissance de 2.

La suite (w_n) apparaît dans différents contextes [55, 56]. Elle peut être définie par $w_0 = 0$, $w_n = 1$ si $n = 2^k$ et $w_n = 1 + \min(w_{n-2^k}, w_{2^{k+1}-n})$ si $2^k < n < 2^{k+1}$. De plus elle est 2-régulière de rang 4 et une représentation linéaire réduite est donnée par

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\lambda = \begin{pmatrix} 0 & 1 & 1 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Au vu de l'inégalité $1 \leq w_n \leq \nu(n) \leq \lambda(n)$, valable pour $n \geq 1$, il est clair que l'abscisse de convergence absolue de la série de Dirichlet associée

$$w(s) = \sum_{n \geq 1} \frac{w_n}{n^s}$$

vaut 1. D'ailleurs $\rho(w) = 1$ et $\tau(w) = 2$. La matrice

$$Q = A_0 + A_1 = \begin{pmatrix} 1 & 0 & -1 & -1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

admet pour valeurs propres -1, 1 et 2, les deux premières étant simples et la seconde double. En prenant les logarithmes et en posant $\chi = i\pi / \ln 2$ pour simplifier, nous voyons apparaître comme pôles éventuels les $(2\,k + 1)\chi - \ell$, les $2\,k\chi - \ell$ et les $1 + 2\,k\chi - \ell$ avec k entier relatif et ℓ entier naturel. Les multiplicités sont respectivement 1, 1 et 2. En tenant compte des collisions, il s'avère que $w(s)$ se prolonge en une fonction méromorphe dans le plan complexe dont les pôles sont parmi les $1 + 2\,k\chi$, les $2\,k\chi - \ell$ et les $(2\,k + 1)\chi - \ell$, avec des multiplicités majorées respectivement par 2, 3 et 1, et toujours k entier relatif et ℓ entier naturel.

7.3 Cas interne

Après les séries B-régulières, nous entamons l'étude des produits infinis

$$\prod_{k \geq 0} \frac{1}{\phi(z^{B^k})},$$

en commençant par le cas interne. Notre classification est plutôt une idée directrice qu'un plan strict et nous ne limitons pas à des produits infinis pour ce cas.

Supposons que la série $f(z)$ vérifie une équation, à coefficients tous polynomiaux,

$$c_0(z)f(z) + \cdots + c_N(z)f(z^{B^N}) = b(z)$$

dans laquelle $c_0(z)$ a des racines, dont au moins une est de module strictement plus petit que 1. Cette équation apparaît comme un perturbation de l'équation

$$c_0(z)r(z) = b(z)$$

et le comportement des coefficients va être qualitativement du même type que pour la solution rationnelle de celle-ci.

Exemple 108 : La suite (u_n), définie par les conditions initiales $u_0 = 0$, $u_1 = 1$ et la récurrence

$$u_n = u_{n-1} + u_{n-2} + u_{\lceil n/2 \rceil}$$

est une perturbation de la suite de Fibonacci. La série génératrice associée, $f(z)$, vérifie l'équation

$$(1 - z - z^2)f(z) = z + (1 + z)f(z^2)$$

et ceci fournit par itération

$$f(z) = \frac{z}{1 - z - z^2} + \frac{1}{(1 - z - z^2)(1 - z^2 - z^4)} \left[z^2(1 + z) + (1 + z)(1 + z^2)g(z)\right]$$

avec

$$g(z) = \frac{z^4}{1 - z^4 - z^8} + \frac{z^8(1 + z^4)}{(1 - z^4 - z^8)(1 - z^8 - z^{16})} + \frac{z^{16}(1 + z^4)(1 + z^8)}{(1 - z^4 - z^8)(1 - z^8 - z^{16})(1 - z^{16} - z^{32})} + \cdots$$

Notons $\phi = \dfrac{1 + \sqrt{5}}{2}$ le nombre d'or, ce qui fait que les racines de $1 - z - z^2$ sont $\alpha = 1/\phi$ et $\beta = -\phi$. Comme $g(z)$ est analytique dans le disque $|z| < \alpha^{1/4}$, la méthode de soustraction des singularités donne le développement

$$u_n \underset{n \to +\infty}{=} C\phi^n + (c_+ + (-1)^n c_-)\phi^{n/2} + O(\phi^{n/4}).$$

Les quantités C, c_+, c_- s'expriment en fonction de ϕ, $g(1/\phi)$, *etc*; par exemple

$$C = \frac{2\phi + 1}{\sqrt{5}} + \frac{\phi^4}{2} g(1/\phi)$$

et numériquement

$$C \simeq 2.0996360882.$$

Qualitativement nous avons un développement asymptotique complet

$$u_n \underset{n \to +\infty}{\approx} \sum_{k=0}^{+\infty} c_k(n)\phi^{n/2^k},$$

où $(c_k(n))_n$ est une suite qui admet la période 2^k.

Exemple 109 : Nous avons rencontré au chapitre 3 page 43 la notion d'autocorrélation définie par Guibas et Odlizko. La série génératrice du nombre de mots de longueur n dont l'autocorrélation s'écrit $10 \cdots 0\gamma$ vérifie l'équation de Mahler

$$z^c(1 - qz)f(z) + [z^c + (1 - qz)P_\gamma(z)]f(z^2) = 2k(\gamma)z^{2c}[z^c + (1 - qz)P_\gamma(z)],$$

dans laquelle $k(\gamma)$ est le nombre de mots d'autocorrélation γ et

$$P_\gamma(z) = \sum_{0\le k<c} \gamma_k z^k$$

si $\gamma = \gamma_0\gamma_1\cdots\gamma_{c-1}$. Cette équation tombe dans le cas interne car l'unique racine non nulle de $z^c(1-qz)$ est $1/q < 1$ et nous attendons un développement asymptotique suivant les $q^{n/2^k}$. Effectivement Guibas et Odlyzko donnent [41, p. 33] un premier terme en q^n et affirment que l'on peut poursuivre le développement aussi loin que l'on veut. Ils donnent par ailleurs des valeurs numériques pour le coefficient de q^n dans quelques cas.

Cependant les pôles qui apparaissent dans le développement obtenu par itération peuvent être tout à fait illusoires et la difficulté est de savoir s'ils sont effectivement présents. Il faut remarquer d'ailleurs que la considération de la seule équation est insuffisante et qu'il est nécessaire de préciser par une autre voie la solution que l'on étudie.

Exemple 110 : La fraction rationnelle $F(z) = 1/(1-16z)$ satisfait l'équation de Mahler un peu stupide

$$(1-3\,z)(1-16\,z)F(z) + z\,(1-16\,z)(1-16\,z^2)F(z^2) - z\,(1-16\,z)(1-16\,z^4)F(z^4) = 1-3\,z.$$

Les pôles sont à rechercher parmi les racines carrées itérées des racines de $c_0(z) = (1-3z)(1-16z)$. Evidemment $\pm 1/4$, $\pm 1/2$, $\pm i/2$, *etc* ne sont pas pôles comme on s'en aperçoit rapidement en itérant :

$$F(z) = \frac{1}{1-16\,z} - \frac{z\left(1-16\,z^2\right)}{1-3\,z}\left(\frac{1}{1-16\,z^2} - \frac{z^2\left(1-16\,z^4\right)F(z^4)}{1-3\,z^2} + \frac{z^2\left(1-16\,z^8\right)F(z^8)}{1-3\,z^2}\right)$$

$$+\frac{z\left(1-16\,z^4\right)}{1-3\,z}\left(\frac{1}{1-16\,z^4} - \frac{z^4\left(1-16\,z^8\right)F(z^8)}{1-3\,z^4} + \frac{z^4\left(1-16\,z^{16}\right)F(z^{16})}{1-3\,z^4}\right).$$

Il n'est pas encore évident que $1/3$ et ses racines carrées itérées ne sont pas pôles. En reprenant les idées utilisées au chapitre 3 dans la recherche des solutions rationnelles, nous considérons le coefficient $c_2(z) = z(1-16z)(1-16z^4)$ et ceci élimine le pôle $1/3$ et ses racines carrées successives, car les pôles ne peuvent être que des racines carrées itérées des racines de $c_2(z)$.

Exemple 111 : Les deux opérateurs $(1-2\,z)-(1-2\,z^2)M$ et $(1-3\,z)-(1-3\,z^2)M$ s'annulent respectivement sur les deux fractions $1/(1-2\,z)$ et $1/(1-3\,z)$. Leur ppcm

$$z\,(1+z)(1-2\,z)(1-3\,z) - (1+z+z^2)(1-2\,z^2)(1-3\,z^2)M + (1-2\,z^4)(1-3\,z^4)M^2$$

s'annule donc sur les deux. En appliquant les remarques que nous avons faites sur les éventuels singularités polaires des solutions, nous constatons que les seuls pôles possibles sont $1/2$ et $1/3$, mais seule la considération des conditions initiales dans la récurrence associée permet de trancher et de dire quel pôle est effectivement présent dans la solution $a/(1-2\,z) + b/(1-3\,z)$.

7.4 Cas modulaire

Le cas modulaire porte sur des produits infinis

$$\prod_{k\ge 0} \frac{1}{\phi(z^{B^k})},$$

dans lequel le polynôme $\phi(z)$ n'a comme racine que des nombres de module 1. Cependant nous avons vu au chapitre 6 qu'un tel produit est B-régulier, si les racines de $\phi(z)$ sont toutes des

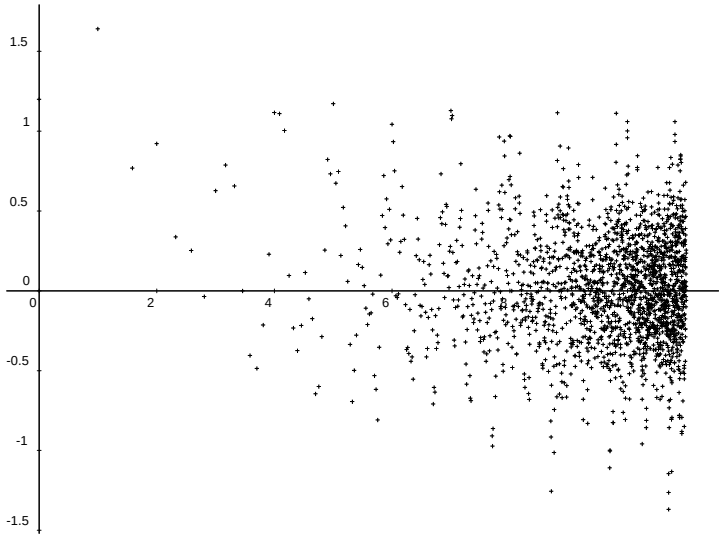

FIG. 7.3
Le comportement de la suite des coefficients du produit $\prod_{k\geq 0} \frac{1}{1-6/5\, z^{2^k}+z^{2.2^k}}$ laisse perplexe le petit asymptoticien.

racines de l'unité dont l'ordre, au sens de la théorie des groupes, n'est pas premier avec B. Nous éliminons donc de telles racines et il reste deux types de racines ; d'une part les racines de l'unité dont l'ordre est premier avec B, d'autre part les nombres de module 1, qui ne sont pas des racines de l'unité. Autrement dit le cas complémentaire se scinde en deux sous-cas, disons *commensurable* et *incommensurable* par référence aux arguments des racines de $\phi(z)$.

Un exemple typique du cas commensurable est la fonction génératrice du nombre de partitions B-aires d'un entier

$$\prod_{k\geq 0} \frac{1}{1-z^{B^k}} = \sum_{n\geq 0} p_B(n)\, z^n.$$

Elle a déjà donné lieu à de nombreuses publications comme [52], dans laquelle Mahler montre, entre autres choses, que

$$p_B(Bn) \underset{n\to+\infty}{=} \frac{B^{-\ell\,(\ell-1)/2} n^\ell}{\ell!}\, e^{O(1)}$$

si ℓ est l'entier défini par

$$B^{\ell-1}\ell \leq n < B^\ell(\ell+1).$$

En particulier, il en tire l'équivalent

$$\ln p_B(n) \underset{n\to+\infty}{\sim} \frac{\ln^2 n}{2\,\ln B}.$$

De Bruijn est revenu sur cette question dans [23] en étudiant le $O(1)$ dans le développement

$$\ln p_B(Bn) \underset{n\to+\infty}{=} \frac{1}{2\,\ln B}\left(\ln\frac{n}{\ln n}\right)^2 + \left(\frac{1}{2}+\frac{1}{\ln B}+\frac{\ln\ln B}{\ln B}\right)\ln n - \left(1+\frac{\ln\ln B}{\ln B}\right)\ln\ln n + O(1),$$

dû à Mahler. Il a montré que ce $O(1)$ s'explicite en

$$F\left(\frac{\ln n - \ln\ln n}{\ln B}\right) + o(1),$$

où F est une fonction 1-périodique et même qu'il s'exprime par un développement asymptotique complet. Nous obtiendrons au chapitre 8 un résultat de même nature pour le produit

$$\prod_{k\geq 0} \frac{1}{\Phi_a(z^B)},$$

où $\Phi_a(z)$ est le polynôme cyclotomique d'indice a, dans l'hypothèse où a est premier avec B. Ceci généralise l'exemple des partitions B-aires, qui correspond à $a = 1$.

Notre traitement du cas incommensurable sera particulièrement bref et nous ne citerons qu'un exemple. Le nombre $(3 + 4i)/5$ est de module 1 sans être une racine de l'unité. Son polynôme minimal, $p(z) = 1 - 6/5\, z + z^2$, fournit le produit infini

$$\prod_{k\geq 0} \frac{1}{1 - 6/5\, z^{2^k} + z^{2.2^k}} = 1 + \frac{6}{5}\, z + \frac{41}{25}\, z^2 + \frac{96}{125}\, z^3 + \frac{576}{625}\, z^4 + \cdots$$

et les coefficients de celui-ci vérifient la récurrence

$$u_n = \frac{6}{5} u_{n-1} - u_{n-2} + u_{n/2}$$

avec $u_0 = 1$, $u_1 = 6/5$. Cependant nous ne savons pas actuellement traiter cet exemple autrement que par une violente majoration en $\exp(\ln^2 n)$ qui ne semble pas correspondre au bon ordre de grandeur et il n'est ici que pour mémoire (cf. figure 7.3).

7.5 Cas externe

Il reste enfin le cas d'un produit infini associé à un polynôme dont toutes les racines ont un module strictement plus grand que 1. Un exemple typique en est

$$\prod_{k\geq 1} \frac{1}{1 - \rho\, z^{2^k}}$$

avec $\rho < 1$. Le graphe de la suite $(u(n))$ des coefficients (cf. figure 7.4, où $\rho = 1/2$) fait apparaître des phénomènes périodiques comme pour les suites B-régulières. En particulier il est tentant de comparer les valeurs de la suite pour n et $n + 2^{\lambda(n)+k}$, où, rappelons le, $\lambda(n)$ est le nombre de bits de n. Le comportement de la suite

$$q_{n,k} = \frac{u(n + 2^{\lambda(n)+k})}{u(n)},$$

fait sentir une fonction périodique et surtout est relativement indépendant de k. Il semble qu'on passe de la suite $(q_{n,k})$ à la suite $(q_{n,\ell})$ par une simple transformation affine Ainsi le n-ième terme de la suite vaut approximativement une composée de fonctions affines, dépendant de l'entier n,

$$a_{\ell_1} \circ a_{\ell_2} \circ \cdots \circ a_{\ell_k} \circ F(w(n)),$$

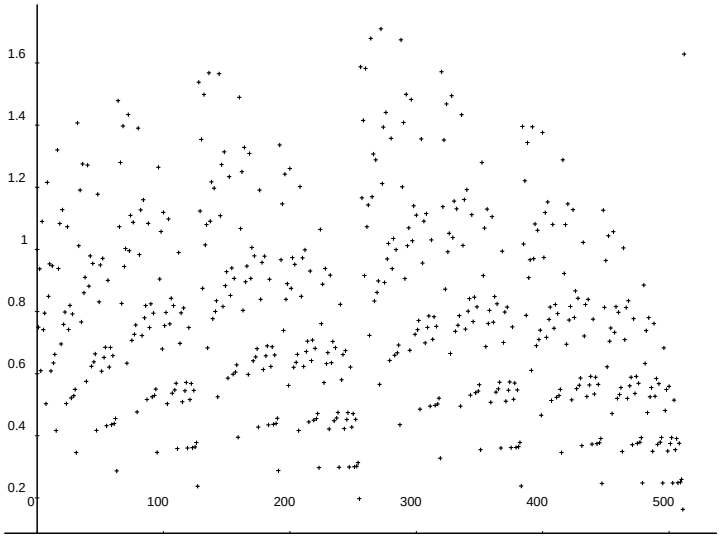

FIG. 7.4
Les coefficients $u(n)$ du produit $\displaystyle\prod_{k\geq 1}\frac{1}{1-z^{2^k}/2}$ présente un comportement périodique en $\lg n$, assez similaire à celui des suites 2-régulières.

si l'écriture binaire de n se décompose en k blocs $10\cdots 0$, le i-ème bloc comportant ℓ_i zéros, et $w(n)$ est la suite 2-régulière qui donne la longueur du bloc maximal de 1, côté poids faibles, dans l'écriture binaire de n.

Nous ne sommes actuellement pas capable d'expliquer la dépendance périodique en $\ln n$; de plus les variations de la fonction ne sont pas assez violentes pour permettre l'utilisation d'une méthode de col. Par contre une récurrence élémentaire fournit une majoration qualitative du coefficient d'indice n.

Proposition 57. *Les coefficients du développement en série d'un produit infini*

$$f(z)=\prod_{k\geq 0}\frac{1}{\phi(z^{B^k})},$$

associé à un polynôme $\phi(z)$ dont toutes les racines ont un module strictement plus grand que 1, ont un comportement en n^α.

Si $\phi(z)$ est de degré d est si ses racines ont toutes un module supérieur à $1/\rho$, avec $\rho<1$, alors

$$f_n \underset{n\to+\infty}{=} O\left(n^{d\log_B(1/(1-\rho))}\right).$$

DÉMONSTRATION. Il suffit de considérer le cas d'une racine et en passant aux modules de considérer la suite (v_n) définie par $v_0>0$ et

$$v_n=\rho v_{n-1}+v_{n/B}.$$

Une simple récurrence montre que l'on a $v_n\leq C\,n^\alpha$ dès que

$$\frac{1}{B^\alpha}\leq 1-\rho,$$

d'où le résultat. □

Chapitre 8

Variations cyclotomiques

Le but de ce chapitre est d'illustrer le cas modulaire et spécialement le cas modulaire commensurable défini au chapitre 7, en déterminant le comportement asymptotique des coefficients du développement en série de certains produits infinis. L'exemple basique en est

$$\prod_{k=0}^{+\infty} \frac{1}{1+z^{2^k}+z^{2^{k+1}}}.$$

Nous considérerons plus généralement le produit infini lié au polynôme cyclotomique $\Phi_a(z)$,

$$f_{a,B}(z) = \prod_{k=0}^{+\infty} \frac{1}{\Phi_a(z^{B^k})},$$

dans l'hypothèse où les entiers a et B sont premiers entre eux. Le cas de base correspond donc à $a = 3$ et $B = 2$. L'énoncé visé est le théorème suivant, dont la démonstration va s'étaler sur les sections 2 à 4. Il donne un développement asymptotique du coefficient de z^n dans $f_{a,B}(z)$, qui met bien en valeur le phénomène attendu de périodicité modulo a, mais aussi une dépendance périodique plus cachée en $\log n$. Nous restons volontairement imprécis pour ne pas noyer le résultat sous la technique. Les quantités utiles seront définies dans la suite.

Théorème 34. *Soient a et B deux entiers premiers entre eux, le nombre a étant libre de carré. Le coefficient de z^n dans le développement en série de*

$$f_{a,B}(z) = \prod_{k=0}^{+\infty} \frac{1}{\Phi_a(z^{B^k})}$$

admet le développement asymptotique complet

$$[z^n] \prod_{k=0}^{+\infty} \frac{1}{\Phi_a(z^{B^k})} \underset{n\to+\infty}{\approx} \exp\left[\frac{\ln^2\rho}{2\,\ln B} + (1+\kappa)\ln\rho + n\rho + \frac{1}{2}\ln n\rho\right] \sum_{k=0}^{+\infty} \frac{1}{(n\rho)^{\frac{k}{2}}} \varpi_k\left(\frac{\ln\rho}{\varphi(a)\,\ln B}\right),$$

dans lequel les fonctions $\varpi_k(v)$ sont analytiques 1-périodiques et le nombre ρ vérifie

$$\ln\rho \underset{n\to+\infty}{=} -\ln n + \ln\ln n - \ln\ln 2 + o(1).$$

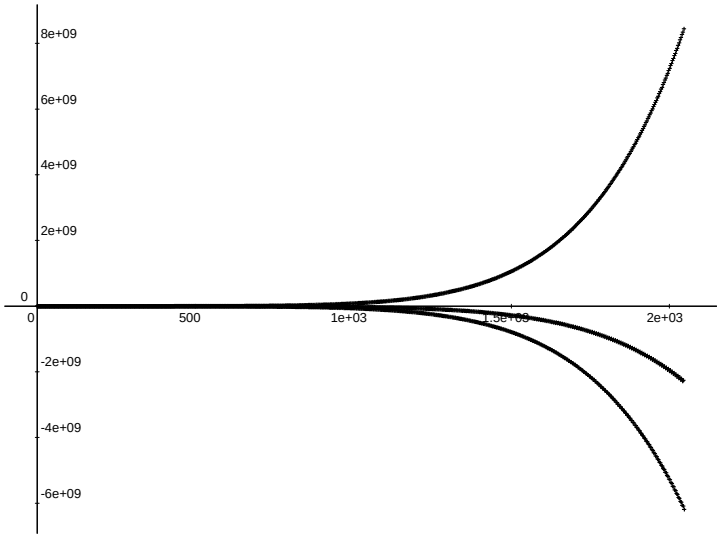

FIG. 8.1
La suite des coefficients de $f_{3,2}(z)$ présente clairement une périodicité modulo 3.

Précisons un peu les choses. Tout d'abord il n'est pas utile de considérer tous les a premiers avec B. A l'entier a est associé son radical $\sqrt{a}$, c'est-à-dire sa partie libre de carré, et les polynômes cyclotomiques $\Phi_a(z)$ et $\Phi_{\sqrt{a}}(z)$ sont reliés par (cf. page 13)

$$\Phi_a(z) = \Phi_{\sqrt{a}}(z^{a/\sqrt{a}}).$$

Il en résulte que

$$f_{a,B}(z) = f_{\sqrt{a},B}(z^{a/\sqrt{a}})$$

et il suffit d'étudier $f_{\sqrt{a},B}(z)$. Nous supposerons donc désormais que a est libre de carré, comme dans l'énoncé.

Le nombre κ vaut

$$\kappa = -\frac{1}{2} + \frac{\ln a}{\ln B}$$

et ρ est l'unique solution strictement positive de l'équation

$$\frac{\ln \rho}{\ln B} + n\rho + \kappa = 0.$$

Il satisfait à l'égalité asymptotique

$$n\rho \ln B \underset{n\to+\infty}{=} \ln n - \ln\ln n + O(1)$$

et le coefficient de z^n dans $f(z)$ se comporte essentiellement comme $\exp(\ln^2 n/2 \ln B)$ puisque $\ln \rho$ est de l'ordre de $-\ln n$.

Pour fixer les idées nous donnons tout de suite le premier terme du développement asymptotique dans le cas $a = 3$, $B = 2$.

Exemple 112 : En posant

$$v = \frac{\ln \rho}{2\,\ln 2},$$

le coefficient de z^n dans le produit infini $f_{3,2}(z)$ satisfait à l'équivalence

$$[z^n] \prod_{k\geq 0} \frac{1}{1+z^{2^k}+z^{2.2^k}} \underset{n\to+\infty}{\sim}$$

$$\exp\left[2\,v^2\,\ln 2 + v(-2+\ln 3) - \frac{1}{2}\ln 2n\pi + C + P(v)\right] \times 2\cos\left(\frac{2n\pi}{3}+\frac{\pi}{12}+P^*(v)\right),$$

où la constante C est

$$C = -\frac{1}{12\,\ln 2}\left(-3\,\ln^2 3 + 3\ln 2\,\ln 3 - \ln^2 2 - 6\,\ln 2 + 12\,\ln 3 + 6\,\gamma^2 - \pi^2 + 12\,\gamma_1\right)$$

et les fonctions 1-périodiques $P(v)$ et $P^*(v)$ sont définies par leur série de Fourier

$$P(v) = \frac{1}{2\,\ln 2}\sum_{k\neq 0}\Gamma(s_k)\zeta(1+s_k)\left(3^{-s_k}+1\right)\exp(4ki\pi v),$$

$$P^*(v) = \frac{1}{2\,\ln 2}\sum_{k}\Gamma(r_k)3^{-1/2-r_k}\left[\zeta(1+r_k,1/3)-\zeta(1+r_k,2/3)\right]\exp((4k+2)i\pi v)$$

avec

$$s_k = 2ik\pi/\ln 2, \quad r_k = (2k+1)i\pi/\ln 2.$$

Rappelons que $\zeta(s,h)$ est la fonction ζ d'Hurwitz [71, p. 265] et que γ_1 est la constante d'Euler d'ordre 1 [1, formule 23.2.5 p. 807],

$$\gamma_1 = \lim_{N\to+\infty}\sum_{k=1}^{N}\frac{\ln k}{k} - \frac{1}{2}\ln^2 N.$$

Il importe de remarquer que les deux fonctions périodiques $P(v)$ et $P^*(v)$ ont une amplitude très faible à cause de la décroissance très violente de la fonction Γ sur l'axe imaginaire dès que l'on s'éloigne de 0.

8.1 Synopsis de la preuve

Désormais nous notons $f(z)$ pour $f_{a,B}(z)$. Le coefficient d'indice n de $f(z)$ est extrait par la formule de Cauchy

$$[z^n]f(z) = \frac{1}{2i\pi}\int_C \frac{f(z)}{z^{n+1}}\,dz,$$

où C est un lacet entourant l'origine. Le lacet utilisé est un cercle centré à l'origine et collé le long du cercle unité. Pour évaluer cette intégrale, nous appliquons la méthode du col, ce qui est justifié par les variations assez violentes de la fonction f au voisinage du cercle unité. On peut le constater sur la figure 8.2, où nous avons représenté en échelle logarithmique les variations du module de $f_{3,2}(z)$ sur le contour d'intégration que nous utiliserons. Bien que le cercle unité soit frontière naturelle, il est clair que certains points ont une importance prépondérante. D'abord les points j et j^2 dominent tous les autres et ceci est naturel car ils sont racines de tous les $\Phi_3(z^{2^k})$. Ensuite viennent $-j$ et $-j^2$, qui sont racines de $\Phi_3(z^{2^k})$ à partir de $k=1$, puis leur racines carrées qui sont racines de $\Phi_3(z^{2^k})$ à partir de $k=2$, *etc.* Plus nous itérons l'extraction des racines carrées et moins les points ont de poids dans l'intégrale.

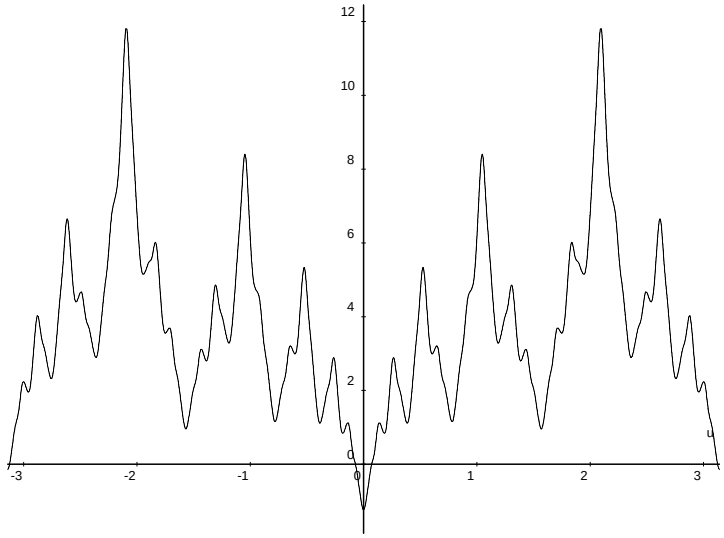

FIG. 8.2
Le comportement de $\ln|f_{3,2}(z)|$ sur le contour d'intégration montre une prédominance des racines cubiques primitives de l'unité et de leurs racines carrées itérées.

Pour mettre en évidence ce comportement de $f(z)$, nous procédons dans un premier temps à une étude locale au voisinage de certaines racines de l'unité, ω, en utilisant la transformation de Mellin et le calcul des résidus. L'expression usuelle des polynômes cyclotomiques à l'aide de la fonction de Möbius $\mu(n)$,

$$\Phi_a(z) = \prod_{d|a} \left(1 - z^d\right)^{\mu(a/d)},$$

amène à considérer d'abord la série génératrice des partitions B-aires,

$$f_{1,B}(z) = \prod_{k\geq 0} \frac{1}{1 - z^{B^k}}.$$

L'étude locale de $f_{1,B}(z)$ au voisinage de ω passe par la fonction

$$\Lambda_\omega(t) = \ln f_{1,B}(\omega e^{-t}) = \sum_{k=0}^{+\infty} \ln\left(1 - \omega^{B^k} e^{-B^k t}\right)^{-1}.$$

La transformée de Mellin de cette dernière fonction est

$$\Lambda^*_\omega(s) = \Gamma(s) \sum_{k=0}^{+\infty} B^{-ks} \sum_{n=1}^{+\infty} \frac{\omega^{B^k n}}{n^{s+1}}.$$

Si ω est une racine aB^ℓ-ième de l'unité, la suite des ω^{B^k} est périodique à partir d'un certain rang, ce qui permet d'étudier les singularités de $\Lambda^*_\omega(s)$. En particulier 0 est pôle d'ordre 2 ou 3 de $t^{-s}\Lambda^*_\omega(s)$. Plus précisément il est pôle d'ordre 3 si et seulement si ω^{B^ℓ} vaut 1 et le résidu en 0 est alors

$$\text{Rés}[t^{-s}\Lambda^*_\omega(s), s=0] = \frac{\ln^2 t}{2\ln B} + \left(\ell - \frac{1}{2}\right)\ln t + \frac{\ln B}{12} + \ell(\ell-1)\frac{\ln B}{2} - \frac{\gamma^2 - \frac{\pi^2}{6} + 2\gamma_1}{2\ln B} + \sigma_\omega(1).$$

La transformation de Mellin inverse donne

$$\Lambda_\omega(t) = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} t^{-s} \Lambda_\omega^*(s)\, ds$$

et en poussant la droite d'intégration vers la gauche, on montre que $\Lambda_\omega(t)$ est égale à la somme des résidus de $t^{-s}\Lambda_\omega^*(s)$ en ses différents pôles. Il suffit alors de recombiner le résultat obtenu avec la fonction de Möbius pour obtenir un développement local de $\ln f(\omega e^{-t})$. Le point remarquable est que $\ln f(\omega e^{-t})$ a un comportement en $\ln^2 t$ au voisinage des racines primitives a-ièmes de l'unité et de leurs racines B-ièmes itérées, alors qu'il n'apparaît qu'un $\ln t$ pour les racines a-ièmes de l'unité non primitives et leurs racines B-ièmes itérées. Cette dichotomie amène à parler de racines majeures et de racines mineures.

Dans un deuxième temps, le cercle d'intégration, qui a pour rayon $e^{-\rho}$, est brisé en petits arcs sur lesquels on peut appliquer les développements précédemment obtenus et qui vont donc se classer en arcs majeurs et mineurs. Les petits arcs apparaissent en recouvrant le cercle d'intégration de la formule de Cauchy par de petits onglets dont le demi-angle d'ouverture est θ_0 et dont les sommets sont les racines aB^ℓ-ième de l'unité pour ℓ entre 0 et L avec

$$L = -\frac{\ln \rho}{\ln B} - \frac{\ln a}{\ln B} + \frac{\ln (2\pi\, \cos\theta_0)}{\ln B} + \delta.$$

La valeur de ρ est déterminée en appliquant la méthode du col aux arcs majeurs qui font face aux racines primitives a-ième de l'unité, ce qui donne l'équation de col

$$\frac{\ln \rho}{\ln B} + n\rho + \kappa = 0.$$

Cette méthode appliquée aux arcs majeurs et une majoration plus grossière pour les arcs mineurs permet d'évaluer chacune des intégrales sur ces petits arcs et même de donner un développement asymptotique complet pour les premières. Les arcs majeurs fournissent des termes en $\exp(\ln^2 n)$ et les arcs mineurs apportent des $\exp(\ln n)$.

Dans un troisième temps la collecte des différentes contributions montre que seules les racines primitives a-ièmes importent vraiment. Le rapport entre la contribution d'un arc associé à une racine aB^ℓ-ième de l'unité et la contribution d'un arc associé à une racine primitive a-ième s'exprime comme l'exponentielle d'un trinôme du second degré en ℓ. *Grosso modo* ce trinôme est nul en $\ell = 0$, minimal et négatif en $\ell = L/2$ et quasi nul en $\ell = L$. En ajustant le demi-angle d'ouverture des onglets θ_0, on peut diminuer la valeur de L de quelques unités, ce qui garantit que le trinôme reste bien négatif dans tout l'intervalle entre 0 et L et en fait part vers $-\infty$. Ainsi la contribution d'une racine aB^ℓ-ième de l'unité est-elle négligeable devant celles des racines primitives a-ièmes de l'unité et les contributions de celles-ci donnent la développement asymptotique cherché.

8.2 Etude locale

Le but de cette section est d'étudier le comportement de $f(z)$ au voisinage d'une racine aB^ℓ-ième de l'unité. Il y a essentiellement deux comportements locaux.

Définition 47. *Une racine aB^ℓ-ième de l'unité, ω, est majeure si $\alpha = \omega^{B^\ell}$ est une racine primitive a-ième de l'unité. Sinon elle est dite mineure.*

La racine de l'unité α est primitive m-ième et ω est une racine majeure si $m = a$ et mineure si m est un diviseur strict de a. Remarquons que la racine α dépend de la valeur de ℓ utilisée, mais son ordre, m, est indépendant de ℓ, car a et B sont premiers entre eux. Par exemple $\omega = \exp(2i\pi/6)$ est une racine sixième de l'unité, mais aussi une racine douzième ou vingt-quatrième ; cependant ω^2, ω^4 comme ω^8 sont des racines primitives cubiques de l'unité. Pour ce qui est de ℓ, nous prendrons toujours la valeur la plus petite possible, de façon qu'il soit bien défini.

Proposition 58. *Soit ω une racine aB^ℓ-ième de l'unité et $\alpha = \omega^{B^\ell}$ la racine a-ième de l'unité associée, qui est une racine primitive m-ième de l'unité. Si ω est majeure la fonction*

$$F_\omega(t) = \ln f_{a,B}(\omega\, e^{-t})$$

s'exprime sous la forme

$$F_\omega(t) = \frac{\ln^2 t}{2\,\ln B} + \left(\ell + \kappa - \frac{\lambda_\alpha}{\ln B}\right)\,\ln t + A_\omega + P_\omega\left(\frac{\ln t}{\varphi(a)\,\ln B}\right) + Q_\omega(t)$$

et si ω est mineure par

$$F_\omega(t) = -\frac{\lambda_\alpha}{\ln B}\,\ln t + A_\omega + P_\omega\left(\frac{\ln t}{\varphi(m)\,\ln B}\right) + Q_\omega(t).$$

Ces développements sont valables pour

$$|t| < \frac{2\pi}{B^\ell m}, \quad \mathfrak{Re}(t) > 0.$$

Voyons maintenant comment parvenir à ce résultat qui sera affiné dans les lemmes 16 et 17, pages 190 et 192 respectivement. Le polynôme cyclotomique $\Phi_a(z)$ s'écrit

$$\Phi_a(z) = \prod_{d|a}(1 - z^d)^{\mu(a/d)} = \prod_{d|a}\Phi_1(z^d)^{\mu(a/d)},$$

où μ est la fonction de Möbius. Nous commençons donc par étudier

$$f_{1,B}(z) = \prod_{k=0}^{+\infty}\frac{1}{1 - z^{B^k}}$$

au voisinage d'une racine de l'unité, ω, en nous inspirant de De Bruijn [23], c'est-à-dire par la transformation de Mellin. Nous obtenons ainsi un développement local de $\Lambda_\omega(t) = \ln f_{1,B}(\omega e^{-t})$, puis de $F_\omega(t) = \ln f_{a,B}(\omega e^{-t})$ par combinaison linéaire.

8.2.1 Transformation de Mellin

A une racine aB^ℓ-ième de l'unité, ω, est associée une racine a-ième de l'unité $\alpha = \omega^{B^\ell}$, dont l'ordre est noté m. Le nombre ω est une racine majeure si $m = a$ et une racine mineure si m est un diviseur strict de a.

Pour étudier le comportement de $f_{1,B}(z)$ au voisinage de ω, nous posons $z = \omega e^{-t}$, ce qui produit la fonction $\Lambda_\omega(t)$ définie pour $\mathfrak{Re}(t) > 0$,

$$\Lambda_\omega(t) = \ln f_{1,B}(\omega e^{-t}) = \sum_{k=0}^{+\infty}\ln\left(1 - \omega^{B^k} e^{-B^k t}\right)^{-1}.$$

La transformée de Mellin de cette dernière fonction est

$$\Lambda_\omega^*(s) = \Gamma(s) \sum_{k=0}^{+\infty} B^{-ks} \sum_{n=1}^{+\infty} \frac{\omega^{B^k n}}{n^{s+1}}.$$

Elle est clairement définie pour $\mathfrak{Re}(s) > 0$.

La transformation de Mellin inverse [58, p. 219] fournit, avec $c > 0$, l'égalité

$$\Lambda_\omega(t) = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} t^{-s} \Lambda_\omega^*(s)\, ds, \tag{8.1}$$

car l'intégrale

$$\int_{c-i\infty}^{c+i\infty} \left| t^{-s}\Gamma(s) \sum_{k=0}^{+\infty} B^{-ks} \sum_{n=1}^{+\infty} \frac{\omega^{B^k n}}{n^{s+1}} \right| ds$$

converge uniformément pour $c > 0$ et si $\mathfrak{Re}(t) > 0$

$$e^{-t} = \frac{1}{2i\pi} \int_{c-i\infty}^{c+i\infty} \Gamma(s) t^{-s}\, ds.$$

Cette expression intégrale de $\Lambda_\omega(t)$ va permettre d'en donner un développement local au voisinage de $t = 0$, par la détermination des singularités de $\Lambda^*(s)$. Pour cela il faut d'abord transformer l'écriture de $\Lambda_\omega^*(s)$. La suite $\left(\omega^{B^k}\right)$ est périodique à partir du rang ℓ (rappelons que ℓ est toujours pris le plus petit possible) avec une période qui divise $\varphi(m)$, l'indicateur d'Euler de m. Ceci introduit une scission de la somme en une partie initiale et une partie finale qui se récrit en tenant compte de la périodicité :

$$\Lambda_\omega^*(s) = \Gamma(s) \left[\sum_{k=0}^{\ell-1} B^{-ks} \sum_{n=1}^{+\infty} \frac{\omega^{B^k n}}{n^{s+1}} + \sum_{0 \le r < \varphi(m)} \frac{B^{-(r+\ell)s}}{1 - B^{-s\varphi(m)}} \sum_{n=1}^{+\infty} \frac{\omega^{B^{(r+\ell)} n}}{n^{s+1}} \right].$$

La fonction ζ d'Hurwitz,

$$\zeta(s,h) = \sum_{n=0}^{+\infty} \frac{1}{(n+h)^s},$$

apparaît alors naturellement comme conséquence de l'égalité

$$\sum_{n=1}^{+\infty} \frac{\beta^n}{n^s} = \frac{1}{t^s} \sum_{j=1}^{t} \beta^j \zeta(s, j/t),$$

où β est une racine de l'unité d'ordre t [8, p. 249]. Ceci donne la formule

$$\Lambda_\omega^*(s) = \frac{\Gamma(s)}{B^{\ell s} m^s} \left[\sigma_\omega(s+1) + \frac{1}{m} \frac{1}{1 - B^{-s\varphi(m)}} \sum_{0 \le r < \varphi(m)} B^{-rs} L_{\alpha^{B^r}}(s+1) \right], \tag{8.2}$$

si nous posons, pour abréger,

$$\sigma_\omega(s) = \sum_{0 \le k < \ell} \frac{1}{B^{\ell-k} m} \sum_{j=1}^{B^{\ell-k} a} \omega^{B^k j} \zeta\left(s, \frac{j}{B^{\ell-k} m}\right) \tag{8.3}$$

et

$$L_\beta(s) = \sum_{j=1}^{t} \beta^j \zeta(s, \frac{j}{t}). \tag{8.4}$$

Dans cette dernière égalité, β est une racine de l'unité primitive d'ordre t, de façon à donner une définition intrinsèque. Il faut noter que $\sigma_\omega(s)$ provient de la partie non périodique de la série de Dirichlet, alors que les $L_{\alpha^{B^r}}(s)$ proviennent de la partie périodique.

EXEMPLE 113 : Prenons $B = 2$ et $\ell = 0$, ce qui fait que $\omega = \alpha$.

Si $\alpha = 1$, nous obtenons

$$\Lambda_1^*(s) = \frac{\Gamma(s)}{1 - 2^{-s}} \zeta(s+1)$$

et, si $\alpha = j$ ou j^2,

$$\Lambda_\alpha^*(s) = \frac{\Gamma(s)}{1 - 2^{-2s}} \left[\sum_{n \geq 1} \frac{\alpha^n}{n^{s+1}} + 2^{-s} \sum_{n \geq 1} \frac{\alpha^{2n}}{n^{s+1}}. \right] = \frac{\Gamma(s)}{1 - 2^{-2s}} \frac{1}{3^{s+1}} \left[L_\alpha(s+1) + \frac{1}{2^s} L_{\alpha^2}(s+1) \right].$$

EXEMPLE 114 : Avec $a = 1$, $B = 2$, $\omega = -1$ et $\alpha = 1$, le calcul donne

$$\Lambda_{-1}^*(s) = \Gamma(s) \left[\sum_{n \geq 1} \frac{(-1)^n}{n^{s+1}} + \sum_{k \geq 1} 2^{-ks} \sum_{n \geq 1} \frac{1}{n^{s+1}}, \right]$$

$$\Lambda_{-1}^*(s) = \Gamma(s) \left[2^{-s} - 1 + \frac{2^{-s}}{1 - 2^{-s}} \right] \zeta(s+1).$$

EXEMPLE 115 : Dans le cas $B = 4$ et $\ell = 0$, nous obtenons, pour $\alpha = 1$,

$$\Lambda_1^*(s) = \frac{\Gamma(s)}{1 - 4^{-s}} \zeta(s+1)$$

et pour $\alpha = j$ ou j^2

$$\Lambda_\alpha^*(s) = \frac{\Gamma(s)}{1 - 4^{-s}} \sum_{n \geq 1} \frac{\alpha^n}{n^{s+1}} = \frac{\Gamma(s)}{1 - 4^{-s}} \frac{1}{3^{s+1}} L_\alpha(s+1).$$

Bien que $\varphi(3) = 2$, nous ne scindons pas la somme en deux car $4 \equiv 1 \bmod 3$ et $\alpha^4 = \alpha$.

8.2.2 Singularités de Λ_ω^*

La formule (8.2) montre que la transformée de Mellin de $\Lambda_\omega(t)$ se prolonge en une fonction méromorphe dans le plan complexe et l'étude des singularités de $\Lambda_\omega^*(s)$ permet d'appliquer le théorème des résidus à l'intégrale qui provient de la transformation de Mellin inverse.

Lemme 11. *La fonction $\Lambda_\omega^*(s)$ se prolonge en une fonction méromorphe dans le plan complexe. La fonction $t^{-s}\,\Lambda_\omega^*(s)$ admet pour pôles les entiers négatifs et les $\chi_{m,k} = 2ik\pi/[\varphi(m)\,\ln B]$, si $\alpha = \omega^{B^\ell}$ est une racine primitive m-ième. Ces pôles sont simples, sauf 0, qui est triple si $\alpha = 1$ et double si $\alpha \neq 1$.*

Rappelons que ℓ prend la valeur minimale telle que α soit une racine a-ième de l'unité, que m est un diviseur de a et que $\varphi(m)$ est l'indicateur d'Euler de m.

DÉMONSTRATION. La fonction d'Hurwitz est méromorphe dans $\mathbb{C}$ avec comme seule singularité un pôle simple en 1 de résidu 1 :

$$\zeta(s+1,h) \underset{s\to 0}{=} \frac{1}{s} - \psi(h) + \gamma_1(h)s + o(s). \tag{8.5}$$

Ici ψ désigne la dérivée logarithmique de la fonction Γ d'Euler et on peut considérer que $\gamma_1(h)$ est définie par cette égalité. Pour $\beta = 1$ la fonction $L_\beta(s)$ est une fonction méromorphe dans le plan complexe avec un pôle simple en 1 de résidu 1 et pour β racine de l'unité différente de 1 et primitive d'ordre t la fonction $L_\beta(s)$ est entière. Dans ce dernier cas nous avons d'ailleurs

$$L_\beta(1) = -\sum_{j=1}^{t} \beta^j \psi\left(\frac{j}{t}\right).$$

L'égalité

$$\sigma_\omega(s) = \sum_{0\le k<\ell} \frac{1}{B^{\ell-k}m} L_{\omega^{B^k}}(s)$$

montre que $\sigma_\omega(s)$ est une fonction entière pour tous les ω car ou bien la somme est vide ou bien aucun des ω^{B^k} $(0 \le k < \ell)$ ne vaut 1. D'autre part l'intégrale eulérienne de seconde espèce, $\Gamma(s)$, admet des pôles simples aux entiers négatifs [71, §12.1 p. 236] et la fonction $(1 - B^{-s\varphi(m)})^{-1}$ a pour pôles les $\chi_{m,k} = \dfrac{2ik\pi}{\varphi(m)\ln B}$ $(k \in \mathbb{Z})$. Ainsi l'intégrande de (8.1), $t^{-s}\Lambda^*_\omega(s)$, est elle une fonction méromorphe avec des pôles simples sauf 0 qui est triple ou double suivant que $\alpha = 1$ ou $\alpha \neq 1$. □

Lemme 12. *Les résidus de $t^{-s}\Lambda^*_\omega(s)$ sont de la forme suivante ;*

— *en 0, si $\alpha = 1$*

$$\text{Rés}[t^{-s}\Lambda^*_\omega(s), s=0] = \frac{\ln^2 t}{2\ln B} + \left(\ell - \frac{1}{2}\right)\ln t + \frac{\ln B}{12} + \ell(\ell-1)\frac{\ln B}{2} - \frac{\gamma^2 - \frac{\pi^2}{6} + 2\gamma_1}{2\ln B} + \sigma_\omega(1),$$

et si $\alpha \neq 1$ le résidu est du premier degré en $\ln t$ et en ℓ ;

— *en $\chi_{m,k} = 2ik\pi/[\varphi(m)\ln B]$ $(k \neq 0)$, le résidu est produit de $\left(B^\ell m t\right)^{-\chi_{m,k}}$ par une fonction de α ;*

— *en $-n$, le résidu est en $(B^\ell m t)^n$.*

DÉMONSTRATION. Si $\alpha = 1$, le résidu de

$$t^{-s}\Lambda^*_\omega(s) = \Gamma(s)(B^\ell t)^{-s}\left[\sigma_\omega(s+1) + \frac{\zeta(s+1)}{1-B^{-s}}\right]$$

vaut

$$\text{Rés}[t^{-s}\Lambda^*_\omega(s), s=0] = \frac{\ln^2 t}{2\ln B} + \left(\ell - \frac{1}{2}\right)\ln t + \frac{\ln B}{12} + \ell(\ell-1)\frac{\ln B}{2} - \frac{\gamma^2 - \frac{\pi^2}{6} + 2\gamma_1}{2\ln B} + \sigma_\omega(1),$$

ce qui redonne bien le résultat dû à De Bruijn [23] pour $l = 0$, c'est-à-dire $\omega = 1$.

Ensuite quand l'ordre de α est différent de 1, $t^{-s}\Lambda^*_\omega(s)$ est donné par

$$t^{-s}\Lambda^*_\omega(s) = \Gamma(s)(B^\ell t)^{-s} m^{-s-1}\left[\sigma_\omega(s+1) + \frac{1}{1-B^{-s\varphi(m)}} \sum_{0\le r<\varphi(m)} B^{-rs} L_{\alpha^{B^r}}(s+1)\right],$$

et son résidu en 0 vaut

$$\text{Rés}\left[t^{-s}\Lambda^*_\omega(s), s=0\right] = -\frac{1}{m\,\varphi(m)\ln B}\ln t \sum_{0\le r<\varphi} B^{-r} L_{\alpha^{B^r}}(1)$$

$$+\frac{1}{m\,\varphi(m)\,\ln B}\sum_{0\le r<\varphi} B^{-r}L'_{\alpha^{B^r}}(1)$$

$$+\frac{1}{m}\left[\sum_{0\le r<\varphi(m)} B^{-r}L_{\alpha^{B^r}}(1)\right]\left[\frac{1}{2}-\frac{\gamma}{\varphi(m)\,\ln B}-\frac{\ln(B^\ell m)}{\varphi(m)\,\ln B}\right]+\sigma_\omega(1).$$

Cette ignoble expression n'a guère d'importance en elle même. Le point remarquable est qu'elle ne comporte pas de $\ln^2 t$.

Avec $\chi_{m,k}=2ik\pi/[\varphi(m)\,\ln B]$ et $k\neq 0$, le résidu est

$$\text{Rés}\left[t^{-s}\Lambda^*_\omega(s), s=\chi_{m,k}\right]=\frac{1}{m\,\varphi(m)\,\ln B}\Gamma(\chi_{m,k})\left(B^\ell mt\right)^{-\chi_{m,k}}\sum_{0\le r<\varphi(m)} B^{-r(1+\chi_{m,k})}L_{\alpha^{B^r}}(1+\chi_{m,k}).$$

Enfin, pour n entier strictement positif,

$$\text{Rés}\left[t^{-s}\Lambda^*_\omega(s), s=-n\right]=\frac{(-t)^n}{n!}(B^\ell m)^n\left[\sigma_\omega(1-n)+\frac{1}{1-B^{n\varphi(m)}}\sum_{0\le r<\varphi(m)} B^{rn}L_{\alpha^{B^r}}(1-n)\right].$$

□

Reprenons les calculs précédents dans des cas simples. Il suffit de considérer le cas $\ell=0$ car pour $\ell>0$ seuls les résultats qualitatifs seront utiles.

Exemple 116 : Prenons ce qu'il y a de plus simple : $a=3$, $B=2$. Le point de départ est l'égalité

$$\Lambda^*_\alpha(s)=\frac{\Gamma(s)}{1-2^{-s\varphi(m)}}\sum_{0\le r<\varphi(m)} 2^{-rs}\sum_{n=1}^{+\infty}\frac{\alpha^{2^r n}}{n^{s+1}}.$$

Etudions le cas $\alpha=1$. Tout d'abord

$$\text{Rés}[t^{-s}\Lambda^*(s), s=0]=\frac{\ln^2 t}{2\,\ln 2}-\frac{1}{2}\ln t+\frac{\ln 2}{12}-\frac{\gamma^2-\frac{\pi^2}{6}+2\gamma_1}{2\,\ln 2},$$

résultat déjà fourni par De Bruijn.

Si $n>0$,

$$\text{Rés}\left[t^{-s}\Lambda^*(s), s=-n\right]=\frac{(-t)^n}{n!}\frac{\zeta(1-n)}{1-2^n}=-\frac{(-t)^n}{n!}\frac{B_n(1)}{n}\frac{1}{1-2^n}$$

c'est-à-dire

$$\text{Rés}\left[t^{-s}\Lambda^*(s), s=-n\right]=\frac{(-1)^{n+1}t^n}{n.n!}\frac{B_n}{1-2^n}.$$

Nous avons utilisé la formule [71, §13.14 p. 267]

$$\zeta(-n,h)=-\frac{\mathrm{B}_{n+1}(h)}{n+1},\quad n\ge 0,\ 0<h\le 1.$$

Si $k\neq 0$ et $\chi_k=2ik\pi/\ln 2$,

$$\text{Rés}\left[t^{-s}\Lambda^*(s), s=\chi_k\right]=\frac{1}{\ln 2}\Gamma(\chi_k)t^{-\chi_k}\zeta(1+\chi_k).$$

Passons au cas $\alpha=\exp(\pm 2i\pi/3)$. Nous venons de

$$\frac{\Lambda^*_\alpha(s)}{\Gamma(s)}=\sum_{k\ge 0}2^{-ks}\sum_{n\ge 1}\frac{\alpha^{2^k n}}{n^{s+1}}$$

$$= \frac{1}{1-2^{-2s}} \left[\sum_{n\geq 1} \frac{\alpha^n}{n^{s+1}} + 2^{-s} \sum_{n\geq 1} \frac{\alpha^{2n}}{n^{s+1}}. \right]$$

Le terme entre crochets devient en introduisant les fonctions d'Hurwitz

$$\frac{1}{3^{s+1}} \left(\alpha\zeta(s+1,1/3) + \alpha^2\zeta(s+1,2/3) + \zeta(s+1) \right)$$

$$+\frac{2}{6^{s+1}} \left(\alpha^2\zeta(s+1,1/3) + \alpha\zeta(s+1,2/3) + \zeta(s+1) \right)$$

et les deux fonctions entre parenthèses sont entières. Ce sont $L_\alpha(s+1)$ et $L_{\alpha^2}(s+1)$. De l'égalité asymptotique

$$\zeta(s+1,h) \underset{s\to 0}{=} \frac{1}{s} - \psi(h) + \gamma_1(h)s + o(s),$$

il résulte que

$$L_\alpha(s+1) = -[\alpha\psi(1/3) + \alpha^2\psi(2/3) + \psi(1)] + [\alpha\gamma_1(1/3) + \alpha^2\gamma_1(2/3) + \gamma_1(1)]s + o(s).$$

Nous en tirons

$$L_\alpha(s+1) + \frac{1}{2^s} L_{\alpha^2}(s+1) \underset{s\to 0}{=} -3\,\ln 3 + \left[-3\,\ln 3 \left(\gamma + \frac{\ln 3}{2} \right) + \frac{3}{2} \ln 2\,\ln 3 + i\frac{\pi}{2}\ln 2 \right] s + o(s).$$

Pour le terme constant, ceci provient de l'égalité

$$\psi(1/3) + \psi(2/3) - 2\psi(1) = -3\,\ln 3$$

obtenue grâce à $\psi(1/3) + \psi(2/3) + \psi(1) = -3(\ln 3 + \gamma)$. Cette dernière est un cas particulier de

$$\sum_{j=1}^{N} \psi\left(\frac{j}{N}\right) = -N(\ln N + \gamma),$$

qui est conséquence du théorème de multiplication de Gauss Legendre [71, §12.15 p. 240]. Pour le coefficient de s, nous obtenons d'abord l'expression

$$2\gamma_1(1) - \gamma_1(1/3) - \gamma_1(2/3) + \frac{3}{2}\ln 2\,\ln 3 + i\frac{\pi}{2}\,\ln 2,$$

ce qui nous amène à introduire

$$\tau(s) = 2\zeta(s) - \zeta(s,1/3) - \zeta(s,2/3)$$

car celle-ci a pour développement

$$\tau(s+1) \underset{s\to 0}{=} -[2\psi(1) - \psi(1/3) - \psi(2/3)] + [2\gamma_1(1) - \gamma_1(1/3) - \gamma_1(2/3)]\,s + o(s).$$

Cependant

$$\tau(s) = 2\zeta(s) - \zeta(s,1/3) - \zeta(s,2/3)$$

et

$$3^s\zeta(s) = \zeta(s) + \zeta(s,1/3) + \zeta(s,2/3),$$

d'où en additionnant

$$\tau(s) = 3(1-3^{s-1})\zeta(s)$$

puis

$$\tau(s+1) \underset{s\to 0}{=} -3\,\ln 3 - 3\,\ln 3 \left[\gamma + \frac{\ln 3}{2} \right] s + o(s)$$

et finalement l'expression de $L_\alpha(s+1)+1/2^s\,L_{\alpha^2}(s+1)$. Ceci fournit le résidu cherché

$$12\,\ln 2\,\text{Rés}\left[t^{-s}\Lambda^*(s),s=0\right]=6\,\ln 3\,\ln t+3\,\ln^2 3-3\,\ln 2\,\ln 3+i\pi\ln 2.$$

Passons aux pôles imaginaires purs $\chi_k=\chi_{3,k}=ik\pi/\ln 2$. Le résidu vaut

$$\text{Rés}\left[t^{-s}\Lambda^*_\alpha(s),s=\chi_k\right]=\frac{1}{2\,\ln 2}\Gamma(\chi_k)t^{-\chi_k}\left[\sum_{n\geq 1}\frac{\alpha^n}{n^{1+\chi_k}}+2^{-\chi_k}\sum_{n\geq 1}\frac{\alpha^{2n}}{n^{1+\chi_k}}\right].$$

On peut être plus précis en distinguant les indices pairs et impairs. Si l'indice est pair et $s_k=\chi_{2k}$, comme $2^{-\chi_{2k}}=1$ nous avons

$$\sum_{n\geq 1}\frac{\alpha^n}{n^{1+\chi_{2k}}}+2^{-\chi_{2k}}\sum_{n\geq 1}\frac{\alpha^{2n}}{n^{1+\chi_{2k}}}=\sum_{n\geq 1}\frac{\alpha^n+\alpha^{2n}}{n^{1+s_k}}$$

et la fonction τ utilisée plus haut réapparait. La somme précédente est la valeur en $s=s_k$ de

$$\frac{\tau(s+1)}{3^{s+1}}=\frac{3(1-3^s)}{3^{s+1}}\zeta(s+1)=(3^{-s}-1)\zeta(s+1)$$

donc

$$\text{Rés}\left[t^{-s}\Lambda^*_\alpha(s),s=s_k\right]=\frac{1}{2\,\ln 2}\Gamma(s_k)t^{-s_k}(3^{-s_k}-1)\zeta(s_k+1).$$

Si l'indice est impair nous devons prendre la valeur en $r_k=\chi_{2k+1}$ de

$$\sum_{n\geq 1}\frac{\alpha^n-\alpha^{2n}}{n^{1+s}}=\frac{\epsilon i\sqrt{3}}{3^{s+1}}\left[\zeta(s+1,1/3)-\zeta(s+1,2/3)\right]$$

avec $\epsilon=\text{sgn}\,\mathfrak{Im}(\alpha)$.

Pour les pôles entiers négatifs, nous trouvons

$$\text{Rés}\left[t^{-s}\Lambda^*_\alpha(s),s=-n\right]=\frac{(-t)^n3^{n+1}}{1-2^{2n}}\left[(\alpha+2^{n-1}\alpha^2)B_n(1/3)+(\alpha^2+2^{n-1}\alpha)B_n(2/3)+(1+2^{n-1})B_n\right].$$

mais cette formule ne va pas servir. Seul son contenu qualitatif est utile.

Exemple 117 : Recommençons avec $a=3$, $B=4$ et $\ell=0$.

Pour $\alpha=1$, la transformée de Mellin vaut

$$\Lambda^*_1(s)=\frac{\Gamma(s)}{1-4^{-s}}\zeta(s+1)$$

et le résidu en l'origine est donc

$$\text{Rés}\left[t^{-s}\Lambda^*_1(s),s=0\right]=\frac{\ln^2 t}{2\,\ln 4}-\frac{\ln t}{\ln 4}+\frac{\ln^2 4-12\gamma_1(1)-6\gamma^2+\pi^2}{12\,\ln 4};$$

de même pour $\chi_k=\chi_{1,k}=2ik\pi/\ln 4$

$$\text{Rés}\left[t^{-s}\Lambda^*_1(s),s=\chi_k\right]=\frac{1}{\ln 4}\Gamma(\chi_k)\zeta(1+\chi_k)\exp(-\chi_k\ln t)$$

et pour $-n$

$$\text{Rés}\left[t^{-s}\Lambda^*_1(s),s=-n\right]=\frac{(-1)^n\mathrm{B}_n(1)}{n.n!(4^n-1)}t^n.$$

Pour $\alpha=j$ ou j^2, l'égalité

$$\Lambda^*_\alpha(s)=\frac{\Gamma(s)}{1-4^{-s}}\sum_{n\geq 1}\frac{\alpha^n}{n^{s+1}}=\frac{\Gamma(s)}{1-4^{-s}}\frac{1}{3^{s+1}}L_\alpha(s+1)$$

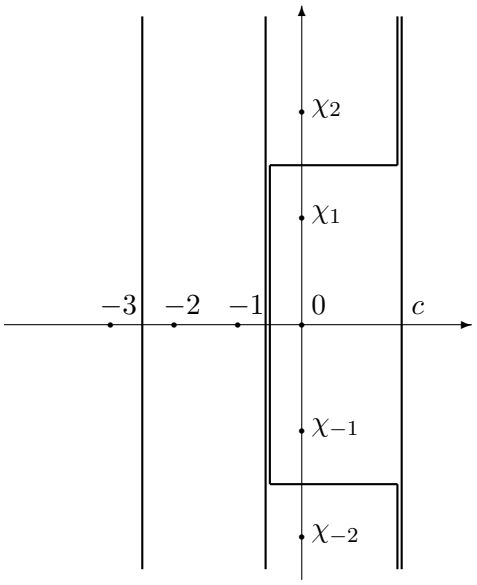

FIG. 8.3
En poussant vers la gauche la droite d'intégration, nous récoltons les résidus de $t^{-s}\Lambda^*(s)$ et le développement de $\Lambda(t)$.

fournit pour le pôle 0

$$\text{Rés}\left[t^{-s}\Lambda^*_\alpha(s), s=0\right] = -\frac{L_\alpha(1)}{3\,\ln 4}\ln t + \frac{L_\alpha(1)}{3\,\ln 4}\left(\frac{1}{2}\ln 4 - \frac{1}{3}\ln 3 - \gamma\right) + \frac{L'_\alpha(1)}{3\,\ln 4},$$

pour les $\chi_k = \chi_{3,k} = ik\pi/\ln 4$

$$\text{Rés}\left[t^{-s}\Lambda^*_\alpha(s), s=\chi_k\right] = \frac{\Gamma(\chi_k)L_\alpha(1+\chi_k)}{\ln 4\; 3^{1+\chi_k}}\exp\left(-\chi_k \ln t\right)$$

avec, rappelons le,

$$L_\alpha(s) = \alpha\zeta(s,1/3) + \alpha^2\zeta(s,2/3) + \zeta(s)$$

et enfin pour le pôle $-n$

$$\text{Rés}\left[t^{-s}\Lambda^*_\alpha(s), s=-n\right] = \frac{(-1)^n 3^{n-1}}{n.n!(4^n-1)}t^n\left[\alpha \mathrm{B}_n(1/3) + \alpha^2\mathrm{B}_n(2/3) + \mathrm{B}_n\right].$$

8.2.3 Développement en série de $\Lambda_\omega(t)$

Nous reprenons la formule

$$\Lambda_\omega(t) = \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} t^{-s}\Lambda^*_\omega(s)\,ds$$

en modifiant le chemin d'intégration, plus précisément en poussant la droite d'intégration $\mathfrak{Re}(s) = c$ vers la gauche.

Lemme 13. *La fonction $\Lambda_\omega(t)$ est égale à la somme des résidus de l'intégrande $t^{-s}\Lambda^*_\omega(s)$, si t vérifie*

$$|t| < \frac{2\pi}{B^\ell m}, \quad \mathfrak{Re}(t) > 0.$$

DÉMONSTRATION. Tout d'abord (cf. figure 8.3) la droite d'équation $\mathfrak{Re}(s) = c$ est remplacée par la ligne brisée infinie qui va de $c - i\,\infty$ à $c + i\,\infty$ en passant par les points $c - \chi_{N+1/2}$, $-1/2 - \chi_{N+1/2}$, $-1/2 + \chi_{N+1/2}$, $c + \chi_{N+1/2}$ où $\chi_{N+1/2} = 2i\pi(N+1/2)/[\varphi(m)\,\ln B]$ et N est un entier. Ceci donne une nouvelle intégrale qui diffère de la précédente par la somme des résidus des pôles qui sont à l'intérieur du rectangle de sommets $c - \chi_{N+1/2}$, $c + \chi_{N+1/2}$, $-1/2 + \chi_{N+1/2}$, $-1/2 - \chi_{N+1/2}$. En passant à la limite sur N, on obtient

$$\Lambda_\omega(t) = \int_{-1/2-i\infty}^{1/2+i\infty} t^{-s}\Lambda_\omega^*(s)\,ds$$

$$+ \text{Rés}\left[t^{-s}\Lambda_\alpha^*(s), s=0\right] + \sum_{k\neq 0} \text{Rés}\left[t^{-s}\Lambda_\alpha^*(s), s=\chi_{m,k}\right]$$

car les intégrales sur les segments horizontaux

$$\int_{c-\chi_{N+1/2}}^{-1/2-\chi_{N+1/2}} t^{-s}\Lambda_\omega^*(s)\,ds, \quad \int_{-1/2+\chi_{N+1/2}}^{c+\chi_{N+1/2}} t^{-s}\Lambda_\omega^*(s)\,ds$$

tendent vers 0 quand N tend vers l'infini si $\mathfrak{Re}(t) > 0$. Reprenons en effet l'expression de $\Lambda_\omega^*(s)$:

$$\Lambda_\omega^*(s) = \Gamma(s)\sum_{k=0}^{\ell-1} B^{-ks}\sum_{n=1}^{+\infty}\frac{\omega^{B^k n}}{n^{s+1}} + \frac{1}{1-B^{-s\varphi(m)}}\Gamma(s)\sum_{0\le r<\varphi(m)} B^{-(r+\ell)s}\sum_{n=1}^{+\infty}\frac{\omega^{B^{(r+\ell)}n}}{n^{s+1}}.$$

Le premier terme

$$\Gamma(s)\sum_{k=0}^{\ell-1} B^{-ks}\sum_{n=1}^{+\infty}\frac{\omega^{B^k n}}{n^{s+1}}$$

est la transformée de Mellin de

$$\sum_{k=0}^{\ell-1}\ln\left(1-\omega^{B^k}e^{-B^k t}\right)^{-1}$$

qui est analytique dans le demi-plan $\mathfrak{Re}(s) > 0$, donc [28, p. 115] ce premier terme est un

$$O\left(\exp\left[-\left(\frac{\pi}{2}-\epsilon\right)|y|\right]\right)$$

pour tout $\epsilon > 0$ (avec $y = \mathfrak{Im}(s)$). De la même façon

$$\Gamma(s)\sum_{0\le r<\varphi(m)} B^{-(r+\ell)s}\sum_{n=1}^{+\infty}\frac{\omega^{B^{(r+\ell)}n}}{n^{s+1}}$$

est la transformée de

$$\sum_{k=\ell}^{\ell+\varphi(m)-1}\ln\left(1-\omega^{B^k}e^{-B^k t}\right)^{-1}$$

et nous obtenons une majoration du même type. Quant à

$$\frac{1}{1-B^{-s\varphi(m)}}$$

il est majoré par 1, parce que le segments horizontaux passent à mi-chemin entre les pôles. D'autre part le module de $|t^{-s}|$ est

$$\exp\left(-\mathfrak{Re}(s)\ln|t| + y\ \text{Arg}\,t\right)$$

d'où un majorant en

$$\left[-|y|\left(\frac{\pi}{2}-\epsilon\right) + y\ \text{Arg}\,t\right] O\left(\frac{\sqrt{|t|}}{\ln|t|}\right)$$

ainsi que le résultat annoncé. En prime l'intégrale tend uniformément vers 0 si l'on impose

$$|\mathrm{Arg}\, t| \leq \frac{\pi}{2} - \delta.$$

Ensuite l'intégrale sur la droite $\mathfrak{Re}(s) = -1/2$ est remplacée par l'intégrale sur la droite $\mathfrak{Re}(s) = -N-1/2$ en collectant au passage les résidus. De plus l'intégrale sur cette dernière droite tend vers 0 quand N tend vers l'infini si

$$\left|B^\ell m t\right| < 2\pi.$$

En effet la fonction $\Lambda^*_\omega(s)$ est essentiellement une combinaison linéaire de fonctions $\Gamma(s)\,\zeta(s+1,h)$. Or

$$\frac{2}{(2\pi)^s}\Gamma(s)\,\zeta(s,h) = \frac{1}{\cos \pi s/2}\sum_{n\geq 1}\frac{\cos 2n\pi h}{n^{1-s}} + \frac{1}{\sin \pi s/2}\sum_{n\geq 1}\frac{\sin 2n\pi h}{n^{1-s}}$$

en supposant $\mathfrak{Re}(s) < 0$ et $s \notin \mathbf{Z}$ [69, pp. 36–37]. Il en résulte qu'avec $s = -N - 1/2 + iy$ et en utilisant

$$\Gamma(s)\,\zeta(s+1,h) = \frac{1}{s}\Gamma(s+1)\,\zeta(s+1,h)$$

nous obtenons la majoration

$$|\Gamma(s)\,\zeta(s+1,h)| < \frac{1}{\sqrt{(N+1/2)^2+y^2}}\frac{(2\pi)^{-N+1/2}}{2}e^{-\frac{\pi}{2}|y|}\zeta(N+1/2).$$

Il suffit de savoir que

$$|\Gamma(s)\,\zeta(s+1,h)| < \frac{C}{\sqrt{N^2+y^2}}\frac{e^{-\frac{\pi}{2}|y|}}{(2\pi)^N}, \tag{8.6}$$

où C est une constante absolue. Nous trouvons ainsi

$$\left|\frac{\Gamma(s)\sigma_\omega(s+1)t^{-s}}{B^{\ell s}m^{s+1}}\right| \leq C_1\left(\frac{|t|B^\ell m}{2\pi}\right)^{N+1/2}\frac{e^{-\frac{\pi}{2}|y|}}{\sqrt{N^2+y^2}}$$

et

$$\left|\frac{\Gamma(s)\,t^{-s}}{B^{\ell s}m^{s+1}}\frac{1}{1-B^{-s\varphi(m)}}\sum_{0\leq r<\varphi(m)}B^{-rs}L_{\alpha^{B^r}}(s+1)\right| \leq \frac{C_2}{B^{N+1/2}-1}\left(\frac{|t|B^\ell m}{2\pi}\right)^{N+1/2}\frac{e^{-\frac{\pi}{2}|y|}}{\sqrt{N^2+y^2}}$$

avec C_1 et C_2 ne dépendant que de B, m et ℓ. Précisons un peu d'où vient la dernière majoration. L'inégalité (8.6) permet de majorer les

$$\Gamma(s)L_{\alpha^{B^r}}(s+1)$$

et et ceci fait apparaître

$$\frac{1}{\left|1-B^{-s\varphi(m)}\right|}\sum_{0\leq r<\varphi(m)}B^{(N+1/2)r}.$$

Il suffit alors d'écrire

$$\frac{1}{1-B^{-s\varphi(m)}} = -\frac{B^{s\varphi(m)}}{1-B^{s\varphi(m)}} = -\sum_{n\geq 1}B^{ns\varphi(m)}$$

et de majorer la série des modules. À nouveau l'intégrale sur la droite verticale est convergente grâce à une décroissance exponentielle qui vient du

$$\frac{e^{-\frac{\pi}{2}|y|}}{\sqrt{N^2+y^2}}.$$

De plus le terme

$$\left(\frac{|t|B^\ell m}{2\pi}\right)^{N+1/2}$$

montre que l'intégrale tend vers 0 quand N tend vers l'infini si

$$|t| < \frac{2\pi}{B^\ell m}$$

comme annoncé. On pourrait aussi dire que la série des résidus en les entiers strictement négatifs est une série entière en t, disons $q_\omega(t)$. Son rayon de convergence au moins égal à $2\pi/B^\ell m$ et la fonction analytique qu'elle définit est nulle en 0.

Ainsi $\Lambda_\omega(t)$ est égale à la somme des résidus précédemment calculés si t est dans un demi-disque

$$\mathfrak{Re}(t) > 0, \quad |t| < \frac{2\pi}{B^\ell a}.$$

Les convergences des séries sont uniformes sous l'hypothèse plus stricte :

$$|\operatorname{Arg} t| \leq \frac{\pi}{2} - \delta, \quad |t| \leq r < \frac{2\pi}{B^\ell a}.$$

□

Nous obtenons pour $\Lambda_\omega(t)$ un développement en série essentiellement constitué de quatre termes, respectivement un terme logarithmique, un terme constant, une série oscillante et une série entière.

Lemme 14. *Soit ω une racine aB^ℓ-ième de l'unité et $\alpha = \omega^{B^\ell}$ la racine a-ième de l'unité associée, qui est une racine primitive m-ième de l'unité. Pour*

$$|t| < \frac{2\pi}{B^\ell m}, \quad \mathfrak{Re}(t) > 0,$$

la fonction $\Lambda_\omega(t)$ se décompose en la somme de quatre termes,

- *un terme logarithmique, qui vaut $\dfrac{\ln^2 t}{2\,\ln B} + \left(\ell - \dfrac{1}{2}\right)\ln t$, si ω est une racine majeure ($m = a$), ou $-\dfrac{\lambda_\alpha}{\ln B}\,\ln t$, si ω est mineure (m est un diviseur strict de a) ;*
- *une constante a_ω de la forme $t(\ell) + \sigma_\omega(1)$, où $t(\ell)$ est un polynôme du premier degré en ℓ si ω est mineure et du second degré, avec coefficient dominant $\ln B\,/2$, si ω est majeure ;*
- *un terme oscillant $p_\omega\left(\dfrac{\ln t}{\varphi(m)\,\ln B}\right)$, où $p_\omega(v)$ est une une fonction 1-périodique, analytique dans la bande $|\mathfrak{Im}(v)| < \dfrac{\pi}{2\,\varphi(m)\,\ln B}$, qui est définie comme somme d'une série de Fourier uniformément convergente dans les bandes $|\mathfrak{Im}(v)| < (1-\epsilon)\,\dfrac{\pi}{2\,\varphi(m)\,\ln B}$;*
- *une fonction $q_\omega(t)$, analytique dans le disque $|t| < 2\pi/mB^\ell$, nulle en 0.*

DÉMONSTRATION. Les $\chi_{m,k}$ apportent une série oscillante

$$\tilde{p}_\omega(t) = \sum_{k\neq 0} c_{\omega,k} \exp\left(2ik\pi \frac{\ln t}{\varphi(m)\,\ln B}\right)$$

avec

$$c_{\omega,k} = \frac{1}{a\varphi(m)\ln B}\Gamma(\chi_{m,k})\left(B^\ell m t\right)^{-\chi_{m,k}} \sum_{0\leq r<\varphi(m)} B^{-r(1+\chi_{m,k})} L_{\alpha^{B^r}}(1+\chi_{m,k})$$

ou encore avec

$$v = \frac{\ln t}{\varphi(m)\,\ln B}$$

$$p_\omega(v) = \sum_{k\neq 0} c_{\omega,k} \exp(2ik\pi v).$$

Comme

$$|\Gamma(\chi_{m,k})| \underset{k\to\pm\infty}{\sim} \sqrt{2\pi} \exp\left[-\frac{\pi^2|k|}{\varphi(m)\,\ln B}\right] \Big/ \sqrt{\frac{2\pi|k|}{\varphi(m)\,\ln B}}$$

et [71, p. 275]

$$\left|\sum_{0\leq r<\varphi(m)} B^{-r(1+\chi_{m,k})} L_{\alpha^{B^r}}(1+\chi_{m,k})\right| \underset{k\to\pm\infty}{=} O(\ln|k|),$$

nous avons

$$c_{\omega,k} \underset{k\to\pm\infty}{=} O\left(\frac{\ln|k|}{|k|^{1/2}} \exp\left[-\frac{\pi^2|k|}{\varphi(m)\,\ln B}\right]\right).$$

Il faut remarquer que cette majoration est indépendante de ℓ, car celui-ci n'intervient que par $B^{-\ell\chi_{m,k}}$, qui est de module 1. Ainsi la série

$$p_\omega(v) = \sum_{k\neq 0} c_{\omega,k} \exp(2ik\pi v).$$

converge dans la bande

$$\mathcal{B}_m \ : \ |\mathfrak{Im}(v)| < \frac{\pi}{2\,\varphi(m)\,\ln B}$$

et définit une fonction analytique admettant la période 1. De plus la convergence est uniforme dans les bandes

$$\mathcal{B}_{m,\epsilon} \ : \ |\mathfrak{Im}(v)| < (1-\epsilon)\frac{\pi}{2\,\varphi(m)\,\ln B}$$

et $p_\omega(v)$ est uniformément bornée dans les $\mathcal{B}_{m,\epsilon}$ avec une borne indépendante de ℓ.

Le pôle 0 fournit un terme en $\ln t$ dont l'expression dépend de l'ordre de α. Si $\alpha = 1$, un $\ln^2 t$ apparait,

$$d_\omega(t) = \frac{\ln^2 t}{2\,\ln B} + \left(\ell - \frac{1}{2}\right)\ln t.$$

Si $\alpha \neq 1$, il y a seulement un $\ln t$,

$$d_\omega(t) = -\frac{\ln t}{a\varphi(m)\,\ln B} \sum_{0\leq r<\varphi(m)} B^{-r} L_{\alpha^{B^r}}(1).$$

Il reste un terme qui ne dépend pas de t mais seulement de ω (et donc de ℓ et α). Pour $\alpha = 1$ il s'écrit

$$a_\omega = \frac{\ln B}{12} + \ell(\ell-1)\frac{\ln B}{2} - \frac{\gamma^2 - \frac{\pi^2}{6} + 2\gamma_1}{2\,\ln B} + \sigma_\omega(1)$$

et nous remarquons qu'il est du second degré en ℓ. Pour $\alpha \neq 1$ il est de la forme

$$a_\omega = b_\alpha(\ell) + \sigma_\omega(1),$$

où b_α est un binôme du premier degré en ℓ dont les coefficients ne dépendent que de α. □

8.2.4 Développement en série de $F_\omega(t)$

Revenons à l'étude de

$$f_{a,B}(z) = \prod_{k=0}^{+\infty} \frac{1}{\Phi_a(z^{B^k})}.$$

En posant

$$F_\omega(t) = \ln f_{a,B}(\omega e^{-t}),$$

nous avons

$$F_\omega(t) = \sum_{d|a} \mu(a/d)\Lambda_{\omega^d}(dt)$$

et si ω est une racine aB^ℓ-ième de l'unité, les développements obtenus précédemment s'appliquent. La distinction introduite entre les racines majeures et les racines mineures est justifiée par le lemme suivant.

Lemme 15. *Soit ω une racine aB^ℓ-ième de l'unité. Le développement de $F_\omega(t)$ comporte un terme en $\ln^2 t$ si et seulement si ω est une racine majeure.*

Démonstration. Si ω est une racine aB^ℓ-ième de l'unité, son ordre s'écrit mb, où m divise a et b divise B^ℓ. Si d divise a, alors ω^d est d'ordre

$$\frac{mb}{\operatorname{pgcd}(d, mb)} = \frac{mb}{\operatorname{pgcd}(d, m)}.$$

La racine ω^d apporte un $\ln^2 t$ uniquement dans le cas où le α associé vaut 1 ; il ne peut donc apparaître un $\ln^2 t$ dans le développement de $F_\omega(t)$ que si $\operatorname{pgcd}(d, m) = m$, ce qui impose que m divise d.

Prenons donc un ω d'ordre mb avec $m \mid d$ et $b \mid B^\ell$. Le coefficient de $\ln^2 t$ dans $F_\omega(t)$ est

$$\sum_{m|d|a} \mu\left(a/d\right)$$

où la somme porte sur les d qui sont multiples de m et divisent a, c'est-à-dire en posant $a = km$ et $d = \ell m$

$$\sum_{\ell|k} \mu\left(k/\ell\right).$$

Ceci vaut 0, sauf si $k = 1$, grâce aux propriétés de la fonction de Möbius. Ainsi il n'apparaît un $\ln^2 t$ que si $m = a$, *id est* ω est une racine d'ordre ab, c'est-à-dire une racine B^ℓ-ième d'une racine primitive d'ordre a. □

En additionnant les différentes contributions pondérées par la fonction de Möbius, on obtient une écriture de la forme annoncée dans la proposition 58 page 178. Commençons par étudier les racines majeures, en rappelant que les fonctions σ_ω et L_α ont été définies par les égalités 8.3 et 8.4 page 180.

Lemme 16. *Si ω est une racine majeure, $F_\omega(t)$ admet le développement*

$$F_\omega(t) = \frac{\ln^2 t}{2\,\ln B} + (\ell + \kappa - \frac{\lambda_\alpha}{\ln B})\ln t + A_\omega + P_\omega\left(\frac{\ln t}{\varphi(a)\,\ln B}\right) + Q_\omega(t),$$

pour les t vérifiant

$$|t| < \frac{2\pi}{B^\ell a}, \quad \mathfrak{Re}(t) > 0.$$

De plus il y a convergence uniforme de la série de Fourier P_ω et de la série entière Q_ω, sous les conditions

$$|t| \le (1-\epsilon_1)\frac{2\pi}{B^\ell a}, \quad |\operatorname{Arg} t| \le (1-\epsilon_2)\frac{\pi}{2}.$$

Les nombres κ et λ_α sont définis par

$$\kappa = -\frac{1}{2} + \frac{\ln a}{\ln B},$$

$$\lambda_\alpha = \sum_{d|a, d\neq 1} \frac{\mu(d)}{d\,\varphi(d)} \sum_{0\leq r<\varphi(d)} B^{-r} L_{\alpha^{B^r a/d}}(1).$$

Le terme constant A_ω s'écrit

$$A_\omega = T_\alpha(\ell) + \Sigma_\omega.$$

Le terme $T_\alpha(\ell)$ est un binôme du second degré en ℓ, dont les coefficients ne dépendent que de α et dont le coefficient dominant est $\ln B\,/2$. Enfin

$$\Sigma_\omega = \sum_{d|a} \mu(a/d)\sigma_{\omega^d}(1).$$

Démonstration. Explicitons les différents termes, en employant les mêmes notations que dans le lemme 14 page 188. Nous posons

$$Q_\omega(t) = \sum_{d|a} \mu(a/d) q_{\omega^d}(dt)$$

et il suffit de savoir que le rayon de convergence de cette série entière vaut au moins $2\pi/B^\ell a$ et que $Q_\omega(0) = 0$.

La partie oscillante vaut

$$\tilde{P}_\omega(t) = \sum_{d|a} \mu(a/d) \tilde{p}_{\omega^d}(dt)$$

et avec

$$v = \frac{\ln t}{\varphi(a)\,\ln B}$$

nous constatons que

$$\tilde{P}_\omega(t) = P_\omega(v),$$

où $P_\omega(v)$ est une fonction qui admet la période 1 et qui est analytique dans la bande

$$|\mathfrak{Im}(v)| < \frac{\pi}{2\,\varphi(a)\,\ln B}.$$

De plus elle est uniformément bornée dans les bandes

$$\mathcal{B}_\epsilon \ : \ |\mathfrak{Im}(v)| < (1-\epsilon)\frac{\pi}{2\,\varphi(a)\,\ln B}$$

avec une borne qui est indépendante de ℓ.

Dans le terme

$$\sum_{d|a} \mu(a/d) d_{\omega^d}(dt),$$

il faut traiter à part le diviseur $d = a$ car l'expression de $d_{\omega^a}(at)$ est différente des autres. Nous avons

$$d_{\omega^a}(at) = \frac{\ln^2 at}{2\,\ln B} + \left(\ell - \frac{1}{2}\right)\ln at,$$

ce qui nous fournit le terme logarithmique

$$\frac{\ln^2 t}{2\,\ln B} + \left(\ell - \frac{1}{2} + \frac{\ln a}{\ln B}\right)\ln t.$$

Les diviseurs stricts de a fournissent le terme logarithmique

$$-\frac{\ln t}{(a/d)\,\varphi(a/d)\,\ln B}\sum_{0\le r<\varphi(a/d)} B^{-r}L_{\alpha^{B^r d}}(1).$$

Ainsi en posant

$$\kappa=-\frac{1}{2}+\frac{\ln a}{\ln B}$$

et

$$\lambda_\alpha=\sum_{d|a,d\neq 1}\frac{\mu(d)}{d\,\varphi(d)}\sum_{0\le r<\varphi(d)} B^{-r}L_{\alpha^{B^r a/d}}(1),$$

le terme logarithmique est

$$D_\omega(t)=\frac{\ln^2 t}{2\,\ln B}+\ln t\left(\ell+\kappa-\frac{\lambda_\alpha}{\ln B}\right).$$

Enfin il y a un terme constant A_ω. Il comporte en particulier une combinaison des a_{ω^d} et il faut encore distinguer le cas $d=a$, qui fournit

$$\frac{\ln B}{12}+\ell(\ell-1)\frac{\ln B}{2}-\frac{\gamma^2-\frac{\pi^2}{6}+2\gamma_1}{2\,\ln B}+\sigma_{\omega^a}(1).$$

Le reste ne donne que des termes du premier degré en ℓ,

$$-\ell\sum_{d|a,d\neq a}\frac{\mu(a/d)}{a/d\,\varphi(a/d)}\sum_{0\le r<\varphi} B^{-r}L_{\alpha^{B^r d}}(1),$$

et A_ω apparaît sous la forme

$$A_\omega=T_\alpha(\ell)+\Sigma_\omega,$$

où T_α est un binôme du second degré en ℓ, dont les coefficients ne dépendent que de α et

$$\Sigma_\omega=\sum_{d|a}\mu(a/d)\sigma_{\omega^d}(1).$$

Nous remarquons que le coefficient de ℓ^2 dans $T_\alpha(\ell)$ est $\dfrac{\ln B}{2}$. □

Passons maintenant aux racines mineures.

Lemme 17. *Si ω est une racine mineure et $\alpha=\omega^{B^\ell}$ est une racine primitive m-ième, la fonction $F_\omega(t)$ admet le développement*

$$F_\omega(t)=-\lambda_\alpha\ln t+A_\omega+P_\omega\left(\frac{\ln t}{\varphi(m)\,\ln B}\right)+Q_\omega(t),$$

pour les t vérifiant

$$|t|<\frac{2\pi}{B^\ell m},\quad \mathfrak{Re}(t)>0,$$

avec des définitions similaires au cas majeur. Précisons que le terme A_ω s'écrit

$$A_\omega=T_\omega(\ell)+\Sigma_\omega$$

où T_ω est seulement du premier degré en ℓ et Σ_ω vaut encore

$$\Sigma_\omega=\sum_{d|a}\mu(a/d)\sigma_{\omega^d}(1).$$

DÉMONSTRATION. Il faut regrouper les contributions des ω^d pondérées par la fonction de Möbius, suivant les diviseurs d de a. La racine de l'unité ω^d est d'ordre un diviseur de B^ℓ si et seulement si m divise d et nous scindons l'ensemble des diviseurs de a en deux suivant que m divise d ou non. La lettre δ désigne le pgcd de m et d.

Dans la somme sur les d multiples de m

$$\sum_{m|\dot{d}\,|a} \mu(a/d)\left[\frac{\ln^2 dt}{2\,\ln B}+\left(\ell-\frac{1}{2}\ln dt\right)\right],$$

les $\ln^2 t$ disparaissent comme annoncé, mais il reste

$$\frac{\ln t}{\ln B}\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln d+\frac{1}{2\,\ln B}\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln^2 d+\left(\ell-\frac{1}{2}\right)\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln d.$$

Quant à la somme sur les d non multiples de m, elle nous fournit

$$-\frac{\ln t}{\ln B}\left[\sum_{m\nmid\dot{d}\,|a}\frac{\mu(a/d)}{m/\delta\;\varphi(m/\delta)}\sum_{0\le r<\varphi(m/\delta)}B^{-r}L_{\alpha^{B^r d}}(1)\right]$$

comme terme logarithmique et

$$-\frac{1}{\ln B}\left[\sum_{m\nmid\dot{d}\,|a}\frac{\mu(a/d)\,\ln d}{m/\delta\;\varphi(m/\delta)}\sum_{0\le r<\varphi(m/\delta)}B^{-r}L_{\alpha^{B^r d}}(1)\right]$$

comme terme constant. La partie logaritmique se résume donc dans le coefficient λ_α, qui vaut

$$\lambda_\alpha=-\frac{1}{\ln B}\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln d+\frac{1}{\ln B}\left[\sum_{m\nmid\dot{d}\,|a}\frac{\mu(a/d)}{m/\delta\;\varphi(m/\delta)}\sum_{0\le r<\varphi(m/\delta)}B^{-r}L_{\alpha^{B^r d}}(1)\right].$$

Comme nous venons de le voir, il y a un terme constant

$$\frac{1}{2\,\ln B}\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln^2 d+\left(\ell-\frac{1}{2}\right)\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln d-\frac{1}{\ln B}\left[\sum_{m\nmid\dot{d}\,|a}\frac{\mu(a/d)\,\ln d}{m/\delta\;\varphi(m/\delta)}\sum_{0\le r<\varphi(m/\delta)}B^{-r}L_{\alpha^{B^r d}}(1)\right]$$

comme résidu du terme logarithmique. Les d multiples de m fournissent

$$\sum_{m|\dot{d}\,|a}\mu(a/d)\sigma_{\omega^d}(1)$$

et les d non multiples de m amènent une horreur sans non. En regroupant ces termes constants, nous obtenons un A_ω qui s'écrit

$$A_\omega=T_\omega(\ell)+\Sigma_\omega.$$

Le T_ω est du premier degré en ℓ, avec un coefficient dominant qui vaut

$$\sum_{m|\dot{d}\,|a}\mu(a/d)\,\ln d+\sum_{m\nmid\dot{d}\,|a}\frac{1}{m/\delta\;\varphi(m/\delta)}\sum_{0\le r<\varphi(m/\delta)}B^{-r}L_{\alpha^{B^r d}}(1)$$

et le Σ_ω s'obtient en regroupant toutes les contributions en σ. Il vaut

$$\Sigma_\omega=\sum_{d|a}\mu(a/d)\sigma_{\omega^d}(1).$$

□

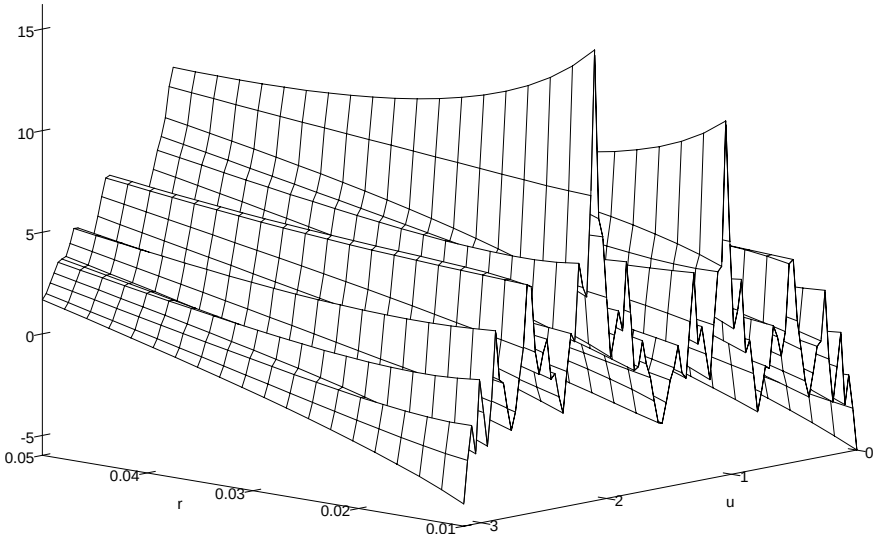

FIG. 8.4
Les variations du module de $F_1(t) + (n+1)t$ pour $a = 3$, $B = 2$ et $n = 100$. L'échelle est logarithmique et t varie dans le rectangle $[0,01,\ 0,05] \times [0, \pi]$. Ici $\rho = 0,03679416640$.

EXEMPLE 118 : Reprenons le cas test, $a = 3$, $B = 2$. Ici $\alpha = \exp(\pm 2i\pi/3)$ ($\ell = 0$) et

$$F_\alpha(t) = \Lambda_1(3t) - \Lambda(t).$$

Pour $|t| < 4\pi/3$ et $|\operatorname{Arg} t| < \pi/2$, nous avons

$$F_\alpha(t) = \frac{\ln^2 t}{2\,\ln 2} - \frac{\ln t}{2}\left(1 - \frac{\ln 3}{\ln 2}\right) + A_\alpha + P_\alpha(v) + Q_\omega(t)$$

avec $v = \ln t/2\,\ln 2$.

La fonction oscillante P_α se décompose en deux. Il y a une première partie relative aux $\chi_{2k} = \chi_{3,2k}$ et indépendante de α :

$$P_0(v) = \frac{1}{2\,\ln 2}\sum_{k\neq 0}\Gamma(\chi_{2k})\zeta(1+\chi_{2k})(3^{-\chi_{2k}}+1)\exp(-4ik\pi v)$$

et une seconde relative aux $\chi_{2k+1} = \chi_{3,2k+1}$ et qui ne dépend de α que par $\epsilon = \operatorname{sgn}\mathfrak{Im}(\alpha)$:

$$P_{\alpha,1}(v) = \frac{-\epsilon}{2\sqrt{3}\,\ln 2}\sum_k \Gamma(\chi_{2k+1})3^{-\chi_{2k+1}}\left[\zeta(1+\chi_{2k+1},1/3) - \zeta(1+\chi_{2k+1},2/3)\right]\exp(-(4k+2)i\pi v).$$

D'autre part

$$A_\alpha = -\frac{1}{12\,\ln 2}\left(-3\,\ln^2 3 + 3\,\ln 2\,\ln 3 - \ln^2 2 + 6\gamma^2 - \pi^2 + 12\gamma_1\right) - \epsilon\frac{i\pi}{12}$$

ce que nous notons $A_\alpha = A - \epsilon i\pi/12$.

8.3 Méthode de col

Le coefficient de z^n dans le développement de Taylor de

$$f(z) = \prod_{k\geq 0}\frac{1}{\Phi_a(z^{B^k})}$$

vaut, d'après la formule de Cauchy,

$$\frac{1}{2i\pi}\int_C \frac{f(z)}{z^{n+1}}\,dz,$$

où C est un lacet entourant l'origine. Les développements obtenus vont guider le choix du contour d'intégration C.

Nous privilégions les racines primitives a-ièmes de l'unité, Ω, qui vont donner la contribution la plus importante dans l'intégrale. Le développement local de la proposition 58 page 178,

$$F_\Omega(t) = \frac{\ln^2 t}{2\,\ln B} + \left(\kappa - \frac{\lambda_\Omega}{\ln B}\right)\ln t + A_\Omega + P_\Omega\left(\frac{\ln t}{\varphi(a)\,\ln B}\right) + Q_\Omega(t),$$

permet d'approcher l'intégrande

$$\frac{f(z)}{z^n} = \Omega^{-n}\exp\left(F_\Omega(t) + nt\right) \qquad (z = \Omega e^{-t})$$

par l'expression

$$\Omega^{-n}\exp\left[\frac{\ln^2 t}{2\,\ln B} + \kappa\,\ln t + nt\right].$$

L'équation de col [24, chap. 5]

$$\frac{\ln\rho}{\ln B} + n\rho + \kappa = 0$$

s'obtient en écrivant que la dérivée de

$$\frac{\ln^2 t}{2\,\ln B} + \kappa\ln t + nt$$

est nulle en $t = \rho$, avec le nombre κ toujours donné par

$$\kappa = -\frac{1}{2} + \frac{\ln a}{\ln B}.$$

Nous choisissons alors comme lacet C un cercle de rayon $e^{-\rho}$. Ce cercle passe approximativement par les cols qui font face aux racines primitives a-ièmes, mais ces cols ne sont pas exactement sur les rayons quand les λ_Ω ne sont pas réels. Cependant la différence sur les arguments est un $O(1/n)$ et ceci ne perturbera pas trop les calculs. Précisons en effet les ordres de grandeur de ρ et $\ln\rho$. En utilisant la fonction W, réciproque de xe^x, le nombre ρ s'exprime par

$$n\rho\,\ln B = W(n\,\ln B\;e^{-\kappa\ln B}).$$

La fonction W admet le développement asymptotique [24, p. 25]

$$W(x) \underset{x\to+\infty}{=} \ln x - \ln\ln x + o(1)$$

d'où les approximations

$$n\rho\,\ln B \underset{n\to+\infty}{=} \ln n - \ln\ln n + \kappa + \ln\ln 2 + o(1)$$

et

$$\ln\rho \underset{n\to+\infty}{=} -\ln n + \ln\ln n - \ln\ln 2 + o(1).$$

Pour faciliter l'expression, nous introduisons la définition suivante.

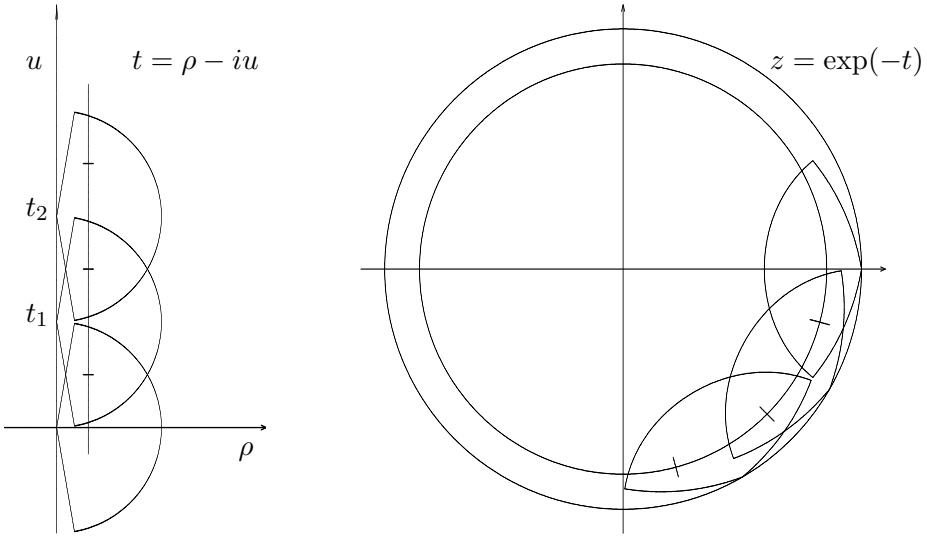

FIG. 8.5
Le contour d'intégration est recouvert par de petits onglets dans lesquels les développements locaux s'appliquent.

Définition 48. *Une fonction est dite exponentiellement petite ou négligeable si elle est négligeable devant le produit de* $\exp(\ln^2 n/2 \ln B)$ *par une quelconque puissance négative de* $\ln n$.

En particulier le produit de $\exp(\ln^2 n/2 \ln B)$ et $1/n$ est exponentiellement petit.

Par le changement de variables $z = \exp(-t)$, l'intégration se fait sur le segment défini par $t = \rho - i\theta$ avec $\theta \in [0, 2\pi]$. Nous recouvrons ce segment par des onglets de sommets les $t_k = \dfrac{2ik\pi}{aB^L}$ avec $0 \leq k < aB^L$ et de demi-angle au sommet θ_0. Evidemment il faut déterminer un L adéquat, ce qui fait l'objet du lemme suivant. L'intégrale éclate en $N = aB^L$ intégrales

$$I_\omega = \frac{\omega^{-n} e^{n\rho}}{2\pi} \int_{-\pi/N}^{\pi/N} f(\omega e^{-\rho} e^{i\theta}) e^{-in\theta}\, d\theta$$

où ω est l'une quelconque des racines N-ièmes de l'unité et pour chacune d'elles les développements vus dans la première partie sont applicables.

Lemme 18. *Si* $\theta_0 \in]0, \pi/2[$ *vérifie*

$$\frac{\sqrt{3}}{2} > B \cos\theta_0$$

et L *est le premier entier tel que*

$$\cos\theta_0 \frac{2\pi}{a\rho} < B^L < \frac{\sqrt{3}}{2} \frac{2\pi}{a\rho},$$

nous avons

$$\frac{1}{2i\pi} \int_C \frac{f(z)}{z^{n+1}}\, dz = \sum_\omega I_\omega,$$

où la somme porte sur les ω, *racines* aB^L*-ièmes de l'unité, et l'égalité*

$$L = -\frac{\ln \rho}{\ln B} - \frac{\ln a}{\ln B} + \frac{\ln(2\pi\, \cos\theta_0)}{\ln B} + \delta$$

avec $0 < \delta \leq 1$.

DÉMONSTRATION. Le fait que la droite d'intégration soit toute entière dans la bande verticale la plus large recouverte par les onglets impose

$$\cos\theta_0 \frac{2\pi}{aB^L} < \rho < \frac{\sqrt{3}}{2}\frac{2\pi}{aB^L}$$

ou encore

$$\cos\theta_0 \frac{2\pi}{a\rho} < B^L < \frac{\sqrt{3}}{2}\frac{2\pi}{a\rho}.$$

Si θ_0 est assez proche de $\pi/2$ pour que

$$\frac{\sqrt{3}}{2} > B\cos\theta_0,$$

il existe une puissance de B qui satisfait à cet encadrement et nous choisissons par exemple la plus petite. L'encadrement fournit tout de suite l'expression de L. □

Le traitement est différent suivant que ω est majeure ou mineure. Dans le premier cas, nous utilisons la méthode de Laplace ; dans le second, un traitement plus grossier suffira.

Proposition 59. *Soient ω une racine aB^L de l'unité et α la racine a-ième de l'unité, qui lui est associée. Si ω est majeure, I_ω admet le développement asymptotique complet,*

$$I_\omega \underset{n\to+\infty}{\approx} \frac{\rho\,\omega^{-n}e^{n\rho}}{\sqrt{2\pi}\sqrt{n\rho}} \exp\left[\frac{\ln^2\rho}{2\,\ln B} + \left(\ell + \kappa - \frac{\lambda_\alpha}{\ln B}\right)\ln\rho + A_\omega\right] \sum_{k=0}^{+\infty} \frac{1}{(n\rho)^{\frac{k}{2}}} \frac{(2k)!}{2^k k!} \chi_{2k,\omega}(v).$$

Dans cette expression, les $\chi_{2k,\omega}(v)$ sont des fonctions analytiques et 1-périodiques, la variable v vaut

$$v = \frac{\ln\rho}{\varphi(a)\,\ln B}.$$

De plus le premier terme de la série est donné par

$$\chi_{0,\omega}(v) = \exp\left[P_\omega\left(\frac{\ln\rho}{\varphi(a)\,\ln B}\right)\right],$$

où $P_\omega(v)$ est défini dans la proposition 58 page 178.

Si ω est mineure, I_ω est un O de

$$\frac{\rho\,\omega^{-n}e^{n\rho}}{2\pi} \exp\left[-\frac{\lambda_\alpha}{\ln B}\ln\rho + A_\omega\right]$$

et la constante impliquée par le O ne dépend que de α.

DÉMONSTRATION. Le remplacement de $f(\omega e^{-\rho}e^{i\theta})$ par son développement, suivi du changement de variables $\theta = \rho u$, donne

$$I_\omega = leader(\omega) J_\omega$$

avec

$$leader(\omega) = \frac{\rho\,\omega^{-n}e^{n\rho}}{2\pi} \exp\left[\frac{\ln^2\rho}{2\,\ln B} + \left(\ell + \kappa - \frac{\lambda_\alpha}{\ln B}\right)\ln\rho + A_\omega\right]$$

et

$$J_\omega = \int_{-\pi/N\rho}^{\pi/N\rho} \exp\left[\frac{\ln^2(1-iu)}{2\,\ln B} + \left(\ell - n\rho - \frac{\lambda_\alpha}{\ln B}\right)\ln(1-iu) - in\rho u + \tilde{P}_\omega(\rho(1-iu)) + Q_\omega(\rho(1-iu))\right] du.$$

Le coefficient de $\ln(1-iu)$ a été simplifié en tenant compte de l'équation vérifiée par ρ.

Nous introduisons ϵ_1 et ϵ_2 tels que

$$\epsilon_{1,2} \underset{n\to+\infty}{\sim} \frac{1}{\ln^r n}$$

avec

$$\frac{1}{3} < r < \frac{1}{2}.$$

Le choix de ϵ_1 et ϵ_2 sera précisé un peu plus loin. La contribution essentielle provient de

$$K_\omega = \int_{-\epsilon_1}^{\epsilon_2} \exp\left[\frac{\ln^2(1-iu)}{2\,\ln B} + \left(\ell - n\rho - \frac{\lambda_\alpha}{\ln B}\right)\ln(1-iu) - in\rho u + \tilde{P}_\omega(\rho(1-iu))\right] du.$$

Nous notons

$$v = \frac{\ln\rho}{\varphi(a)\,\ln B}.$$

La fonction

$$\nu \ : u \longmapsto \frac{\ln^2(1-iu)}{2\,\ln B} + \left(\ell - \frac{\lambda_\alpha}{\ln B}\right)\ln(1-iu) + P_\omega\left(v + \frac{\ln(1-iu)}{\varphi(a)\,\ln B}\right)$$

est analytique dans le disque unité : $|u|<1$. De plus comme fonction de v elle admet la période 1. L'égalité

$$\frac{w^2}{2} = \ln(1-iu) + iu$$

définit u comme fonction analytique de w au voisinage de 0, une fois levée l'ambiguïté de la racine carrée :

$$w = u + \frac{2}{3}iu^2 - \frac{1}{2}u^3 - \frac{2}{5}iu^4 + \frac{1}{3}u^5 + \frac{2}{7}iu^6 + \cdots,$$

$$u = w - \frac{i}{3}w^2 - \frac{1}{36}w^3 - \frac{i}{720}w^4 + \frac{1}{4320}w^5 + \cdots.$$

Ceci est valable dans un disque centré en $u=0$ et pour n un peu grand tout le segment d'intégration est dans ce disque. Nous procédons au changement de variables qui fait passer de u à w et nous développons l'intégrande en série entière, ce qui donne

$$K_\omega = \int_\gamma \exp\left(-n\rho\frac{w^2}{2}\right)\sum_{n=0}^{+\infty}\chi_{n,\omega}(v)w^n\,dw.$$

Les $\chi_{n,\omega}$ sont périodiques de période 1 et satisfont à une inégalité de la forme

$$|\chi_{n,\omega}(v)| \le c^{n+1}.$$

De plus γ est l'arc image du segment $[-\epsilon_1,\epsilon_2]$ dans le changement de variables. Il est tangent à l'axe réel en 0 et d'allure ordinaire. Si $-\eta_1$ et η_2 sont ses deux extrémités, nous choisissons ϵ_1 et ϵ_2 pour que

$$\mathfrak{Re}(\eta_1) = \mathfrak{Re}(\eta_2) = \epsilon \underset{n\to+\infty}{\sim} \frac{1}{\ln^r n}.$$

Comme l'intégrande est analytique, nous remplaçons l'arc γ par les trois segments $[-\eta_1,-\epsilon]$, $[-\epsilon,\epsilon]$, $[\epsilon,\eta_2]$. L'application de la méthode de Laplace à l'intégrale sur $[-\epsilon,\epsilon]$ fournit le développement asymptotique

$$\sum_{k=0}^{+\infty}\frac{\sqrt{2\pi}}{(n\rho)^{\frac{k+1}{2}}}\frac{(2k)!}{2^k k!}\chi_{2k,\omega}(v)$$

et en particulier l'équivalent

$$\sqrt{\frac{2\pi}{n\rho}}\chi_{0,\omega}(v) = \sqrt{\frac{2\pi}{n\rho}}\exp\left[P_\omega\left(\frac{\ln\rho}{\varphi(a)\,\ln B}\right)\right].$$

Les intégrales $\int_{-\eta_1}^{-\epsilon}$ et $\int_{\epsilon}^{\eta_2}$ sont des $O\left(\exp\left[-n\rho\frac{\epsilon^2}{2}\right]\epsilon^2\right)$ et sont exponentiellement négligeables. Il reste les queues $\int_{-\pi/N\rho}^{-\epsilon_1}$ et $\int_{\epsilon_2}^{\pi/N\rho}$. Nous majorons brutalement par un

$$C\int_{\epsilon_i}^{1}\exp\left[-\frac{n\rho}{2}\ln(1+u^2)\right]\,du \le C\exp\left[-\frac{n\rho}{2}\ln(1+\epsilon_i^2)\right]$$

et ceci est exponentiellement petit.

Il faut encore justifier le fait d'avoir évacué le Q_ω. Cette fonction Q_ω est analytique au voisinage de l'origine et nulle en 0. Ceci permet de majorer le module de $Q_\omega(\rho-i\theta)$ par une constante fois ρ et d'encadrer l'expression par un $(1+O(\rho))$ fois la même expression débarrassée de Q_ω. Comme ρ est exponentiellement petit, nous pouvons négliger cette correction.

Finalement nous avons obtenu, si ω est majeure

$$I_\omega \underset{n\to+\infty}{\approx} \frac{\rho\,\omega^{-n}e^{n\rho}}{\sqrt{2\pi}\sqrt{n\rho}}\exp\left[\frac{\ln^2\rho}{2\,\ln B}+\left(\ell+\kappa-\frac{\lambda_\alpha}{\ln B}\right)\ln\rho+A_\omega\right]\sum_{k=0}^{+\infty}\frac{1}{(n\rho)^{\frac{k}{2}}}\frac{(2k)!}{2^k k!}\chi_{2k,\omega}(v).$$

Il reste les racines mineures. Par les mêmes changements de variables que dans le cas précédent, nous arrivons à l'égalité

$$I_\omega = leader(\omega)J_\omega$$

avec

$$leader(\omega)=\frac{\rho\,\omega^{-n}e^{n\rho}}{2\pi}\exp\left[-\frac{\lambda_\alpha}{\ln B}\ln\rho+A_\omega\right]$$

et

$$J_\omega=\int_{-\pi/N\rho}^{\pi/N\rho}\exp\left[-\frac{\lambda_\alpha}{\ln B}\ln(1-iu)+\tilde{P}_\omega(\rho(1-iu))+Q_\omega(\rho(1-iu))\right]\,du.$$

Comme l'intervalle d'intégration est borné et les fonctions sont bornées sur cette intervalle, il n'est pas difficile de constater que J_ω est borné par une constante qui ne dépend que de α. □

8.4 Collecte

Nous avons obtenu pour chacune des racines aB^L-ième de l'unité, ω, un développement asymptotique de I_ω. Il faut maintenant sommer ces différentes contributions. Les plus importantes sont celles qui proviennent des racines primitives a-ième de l'unité. D'après la proposition 59 page 197, l'apport d'une telle racine Ω est évalué par le premier terme du développement asymptotique,

$$I_\Omega \underset{n\to+\infty}{\sim} \frac{\Omega^{-n}}{\sqrt{2\pi}}\exp\left[\frac{\ln^2\rho}{2\,\ln B}+\left(1+\kappa-\frac{\lambda_\Omega}{\ln B}\right)\ln\rho+n\rho+\frac{1}{2}\ln n\rho+A_\Omega+P_\Omega\left(\frac{\ln\rho}{\varphi(a)\,\ln B}\right)\right].$$

Notre joker consiste à adapter l'angle d'ouverture θ_0 des onglets, que nous avons utilisé dans la méthode du col, aux propriétés arithmétiques de a et B.

Pour comparer les différents I_ω, il faut évaluer d'abord les sommes

$$\Sigma_\omega=\sum_{d|a}\mu(a/d)\sigma_{\omega^d}(1).$$

Rappelons que $\sigma_\omega(s)$ a été défini page 179 par

$$\sigma_\omega(s)=\sum_{0\le k<\ell}\frac{1}{B^{\ell-k}m}\sum_{j=1}^{B^{\ell-k}a}\omega^{B^k j}\zeta\left(s,\frac{j}{B^{\ell-k}m}\right).$$

L'approximation utilise les sommes

$$S_{N,\omega} = \sum_{j=1}^{N} \omega^j \psi\left(\frac{j}{N}\right)$$

où ω est une racine N-ième de l'unité et ψ est la dérivée logarithmique de la fonction Γ. Il est bien connu [71, p. 240] que

$$S_{N,1} = -N(\ln N + \gamma)$$

et nous voulons un résultat similaire pour les $\omega \neq 1$.

Lemme 19. *Soit $\omega = \exp(2i\pi\nu/N)$ une racine N-ième de l'unité différente de 1. Alors pour N grand, nous avons*

$$\mathfrak{Re} \sum_{j=1}^{N} \omega^j \psi\left(\frac{j}{N}\right) = N \ln\left|2 \sin\frac{\pi\nu}{N}\right| + O(N),$$

et la constante impliquée par le O est indépendante de ν.

Démonstration. Le point de départ est [71, p. 241]

$$\psi(z) = -\frac{1}{z} - \gamma + \theta(z)$$

avec

$$\theta(z) = \sum_{m=1}^{+\infty} \left(\frac{1}{m} - \frac{1}{m+z}\right) = z \sum_{m=1}^{+\infty} \frac{1}{m(m+z)}.$$

La somme

$$\sum_{j=1}^{N} \frac{\omega^j}{j} = \ln(1-\omega)^{-1} - \sum_{j=N+1}^{+\infty} \frac{\omega^j}{j}$$

est d'abord évaluée en sommant par parties,

$$\sum_{j=1}^{N} \frac{\omega^j}{j} = \ln(1-\omega)^{-1} - \sum_{j=N+1}^{+\infty} \sigma_j \left(\frac{1}{j} - \frac{1}{j+1}\right)$$

avec

$$\sigma_j = \sum_{i=1}^{j} \omega^i.$$

Le fait que σ_j soit borné par $2/|\omega - 1|$ donne

$$\sum_{j=1}^{N} \frac{\omega^j}{j} = -\ln\left|2 \sin\frac{\pi\nu}{N}\right| + i\frac{\pi\nu}{N} + \frac{1}{\sin \pi\nu/N}\, O\left(\frac{1}{N}\right).$$

Ensuite la formule d'Euler-Maclaurin permet de transformer

$$\sum_{j=1}^{N} \omega^j \theta(j/N) = \sum_{j=1}^{N} \exp\left(2i\pi\nu\frac{j}{N}\right) \theta\left(\frac{j}{N}\right)$$

en

$$\sum_{j=1}^{N} \omega^j \theta(j/N) = N \int_0^1 e^{2i\pi\nu t} \theta(t)\, dt + \frac{1}{2} + O\left(\frac{1}{N}\right).$$

Finalement

$$\sum_{j=1}^{N}\omega^j\psi\left(\frac{j}{N}\right)=N\ln\left|2\sin\frac{\pi\nu}{N}\right|-i\pi\nu+\frac{1}{\sin\pi\nu/N}O(1)+N\int_0^1 e^{2i\pi\nu t}\theta(t)\,dt+\frac{1}{2}+O\left(\frac{1}{N}\right).$$

Nous remarquons que les O ne dépendent pas de ν et une majoration brutale fournit

$$\sum_{j=1}^{N}\omega^j\psi\left(\frac{j}{N}\right)=N\ln\left|2\sin\frac{\pi\nu}{N}\right|+O(N).$$

Encore une fois la constante du O ne dépend pas de ν. □

Lemme 20. *Soit ω une racine aB^ℓ-ième de l'unité, où comme d'habitude ℓ a la valeur minimale, alors*

$$\Sigma_\omega=\sum_{d|a}\mu(a/d)\sigma_{\omega^d}(1)$$

est compris entre un $O(\ell)$ et $\ell^2\,\dfrac{\ln B}{2}+O(\ell)$. De plus les constantes qui interviennent dans les O sont indépendantes de ω et ℓ.

Démonstration. En explicitant les $\sigma_{\omega^d}(1)$, nous obtenons l'expression

$$-\Sigma_\omega=\sum_{0\le k<\ell}\sum_{d|a}\mu(a/d)\frac{1}{B^{\ell-k}a/d}\sum_{j=1}^{B^{\ell-k}a/d}\omega^{B^kjd}\psi\left(\frac{j}{B^{\ell-k}a/d}\right).$$

La somme, correspondant à $k=0$, vaut

$$\sum_{d|a}\mu(a/d)\frac{1}{B^{\ell-k}a/d}\sum_{j=1}^{B^{\ell-k}a/d}\omega^{B^kjd}\psi\left(\frac{j}{B^{\ell-k}a/d}\right).$$

Le lemme précédent appliqué avec $N=aB^\ell$ et $\omega=\exp\left(2i\pi\nu/aB^\ell\right)$, où l'entier ν est premier avec B, fait apparaître deux termes. Le terme complémentaire $O(N)$ fournit seulement un $O(1)$, puisque nous divisons par N. Quant à l'autre terme, il vaut

$$\sum_{d|a}\mu(a/d)\,\ln\left|2\,\sin\frac{\pi\nu}{B^\ell a/d}\right|$$

et nous reconnaissons dans cette expression $\ln|\Phi_a(\omega)|$. Ceci peut surprendre un instant mais est tout à fait normal : l'aller retour par la transformation de Mellin redonne ces termes intacts, même s'ils ont été un instant noyés dans les calculs. Evidemment le module de $\Phi_a(z)$ est majoré sur le cercle unité et le problème est de donner une minoration valable en les racines aB^ℓ de l'unité qui ne sont pas des racines primitives a-ièmes de l'unité. Nous introduisons la fonction π-périodique

$$g_a(t)=\sum_{d|a}\mu(a/d)\,\ln|\sin(dt)|\,.$$

Elle est monotone par morceaux car sa dérivée est une fraction rationnelle en $\operatorname{cotg} t$. Elle est bornée supérieurement comme l'est la fonction $\ln|\Phi_a(z)|$ sur le cercle unité, mais elle n'est pas bornée inférieurement car elle a pour limite $-\infty$ en les $p\pi/a$, où p est premier avec a, et un comportement en $\ln|\sin(at)|$ au voisinage de ces points (cf. figure 8.6).

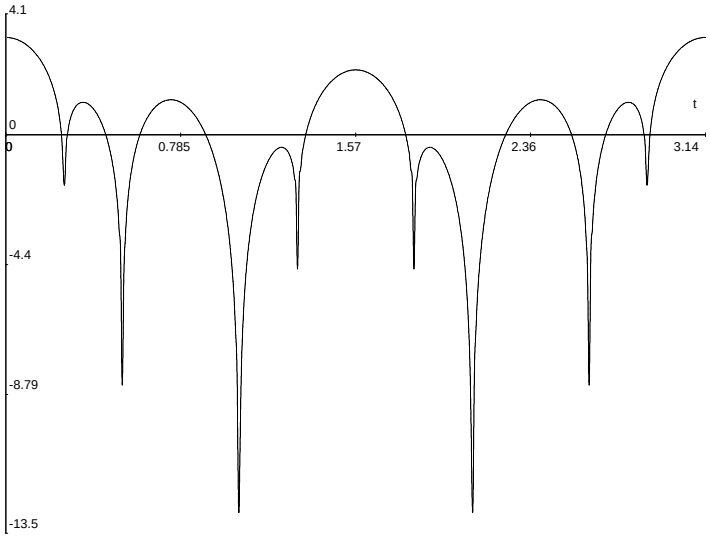

FIG. 8.6
La fonction $\sum_{0\le k<\ell} \ln\left|\Phi_a(z^{B^k})\right|$ est bornée supérieurement sur le cercle unité et a pour limite $-\infty$ en les racines de l'unité d'argument $p\pi/aB^j$, où p est premier avec a et $0 \le j < \ell$. On le constate ici pour $a = 3$, $B = 2$ et $\ell = 3$.

Ainsi le terme $-\Sigma_\omega$ vaut à un $O(\ell)$ près

$$\sum_{0\le k<\ell} \ln\left|\Phi_a(\omega^{B^k})\right| = \sum_{0\le k<\ell} g_a(B^k t),$$

avec $t = \pi\nu/aB^\ell$. Cette dernière fonction est π-périodique, bornée supérieurement par un $O(\ell)$ et a pour limite $-\infty$ en les $p\pi/aB^j$, où p est premier avec a et $0 \le j < \ell$. Les plus petites valeurs que peut donner ω correspondent donc aux points

$$\frac{\pi\nu}{aB^\ell} = \frac{p\pi}{aB^j} \pm \frac{\pi}{aB^\ell}$$

et en reportant nous obtenons à un $O(\ell)$ près la valeur

$$\sum_{j\le k<\ell} \ln\left|\sin\frac{\pi}{B^{\ell-k}}\right| = -j^2\frac{\ln B}{2} + O(\ell).$$

Dans le cas le pire le terme Σ_ω vaut donc

$$\Sigma_\omega = \ell^2\frac{\ln B}{2} + O(\ell).$$

Il faut remarquer que tous les O utilisent des constantes indépendantes de ω. □

Nous arrivons enfin à l'apothéose.

Proposition 60. *A un terme exponentiellement petit près, le coefficient de z^n dans*

$$f(z) = \prod_{k\ge 0} \frac{1}{\Phi_a(z^{B^k})}$$

est la somme des I_Ω, où Ω décrit l'ensemble des racines primitives a-ièmes de l'unité.

DÉMONSTRATION. Si ω est une racine majeure qui n'est pas une racine primitive a-ième de l'unité, nous comparons I_ω et I_α où, comme d'habitude, $\alpha = \omega^{B^\ell}$ est primitive a-ième. Le rapport vaut

$$\frac{I_\omega}{I_\alpha} \underset{n\to+\infty}{\sim} \left(\frac{\omega}{\alpha}\right)^{-n} \exp\left[\ell \ln\rho + A_\omega - A_\alpha + P_\omega(v) - P_\alpha(v)\right]$$

en notant $v = \dfrac{\ln\rho}{\varphi(a)\ln B}$. Comme $P_\omega(v)$ est bornée indépendamment de ℓ, on peut négliger les P. D'autre part la différence $A_\omega - A_\alpha$ vaut

$$A_\omega - A_\alpha = \ell \ln a + \ell(\ell-1)\frac{\ln B}{2} - \ell\lambda_\alpha + \Sigma_\omega.$$

Dans le cas le pire, nous avons $\Sigma_\omega = \ell^2\dfrac{\ln B}{2}$ et le nombres de racines à prendre en compte est moindre que B^ℓ. En faisant preuve d'un pessimisme excessif, le terme dans l'exponentielle est donc un binôme du second degré,

$$\ell^2\frac{\ln B}{2} + \ell \ln\rho + \ell \ln a + \ell(\ell-1)\frac{\ln B}{2} - \ell\lambda_\alpha + O(\ell) + \ell \ln B,$$

qui s'écrit encore

$$\ell^2 \ln B + \ell\left(\ln\rho + \ln a + \frac{\ln B}{2} - \lambda_\alpha\right) + O(\ell).$$

Il faut étudier ce binôme sur l'intervalle $[1, L]$. En 1, il vaut environ $\ln\rho$. Ensuite sa partie réelle décroît et atteint son minimum vers $-\ln\rho\,/2$, puis croît jusqu'à L, où elle vaut

$$L\left(L\ln B + \ln\rho + \ln a + \frac{\ln B}{2} - \lambda_\alpha + O(1)\right),$$

c'est-à-dire

$$L\left(\ln(2\pi\cos\theta_0) + \delta + \frac{\ln B}{2} - \lambda_\alpha + O(1)\right)$$

avec

$$L = -\frac{\ln\rho}{\ln B} - \frac{\ln a}{\ln B} + \frac{\ln(2\pi\cos\theta_0)}{\ln B} + \delta.$$

Nous prenons θ_0 assez proche de $\pi/2$ pour assurer que le terme compris dans la parenthèse a une partie réelle strictement négative et ceci garantit que notre binôme tend vers $-\infty$ pour $\ell = L$ et *a fortiori* pour tous les ℓ de l'intervalle $[1, L]$.

Si ω est une racine mineure, nous comparons I_ω avec I_Ω, où Ω est une racine primitive d'ordre a. Le rapport est

$$\frac{I_\omega}{I_\Omega} \underset{n\to+\infty}{=} O(1)\exp\left[-\frac{\ln^2\rho}{2\ln B} + O(\ln\rho) + A_\omega - A_\Omega\right].$$

Le A_ω comporte un terme du premier degré en ℓ et Σ_ω qui est au pire un $\ell^2 \ln B\,/2$, d'où un quotient qui s'écrit

$$O(1)\exp\left[\ell^2\frac{\ln B}{2} + O(\ell) - \frac{\ln^2\rho}{2\ln B} + O(\ln\rho)\right].$$

Il apparait encore un trinôme, qui en 0 vaut $-\ln^2\rho/2\ln B$ et a donc une partie réelle fortement négative, alors que son coefficient dominant est positif. Sur l'intervalle $[1, L]$, la partie réelle atteint donc sa plus grande valeur en L et cette valeur est

$$L^2\frac{\ln B}{2} - \frac{\ln^2\rho}{2\ln B} + O(L) + O(\ln\rho),$$

c'est-à-dire

$$\frac{\ln B}{2}\left(L - \frac{\ln\rho}{2\ln B}\right)\left(L + \frac{\ln\rho}{2\ln B}\right) + O(\ln\rho).$$

En exprimant L, cela vaut

$$\frac{1}{2}\left(L-\frac{\ln\rho}{2\,\ln B}\right)(-\ln a+\ln\cos\theta_0+\delta)+O(\ln\rho)$$

ou encore

$$-\frac{3}{4}\,\frac{\ln\rho}{\ln B}\,(\ln\cos\theta_0+O(1))\,.$$

A nouveau si nous choisissons θ_0 suffisamment proche de $\pi/2$, le terme entre parenthèses a une partie réelle strictement négative et nous avons une valeur qui tend vers $-\infty$. □

La proposition précédente donne le théorème 34 qui fait l'objet de ce chapitre. En effet les seuls termes utiles sont les I_Ω avec Ω racine primitive d'ordre a, puisqu'un terme exponentiellement petit est négligeable devant tous les termes des développements que nous avons obtenus. En additionnant les I_Ω, nous obtenons

$$[z^n]\prod_{k=0}^{+\infty}\frac{1}{\Phi_a(z^{B^k})}\underset{n\to+\infty}{\approx}\sum_{\Omega}\frac{\Omega^{-n}}{\sqrt{2\pi}}\exp\left[\frac{\ln^2\rho}{2\,\ln B}+\left(\kappa-\frac{\lambda_\Omega}{\ln B}\right)\ln\rho+n\rho+\frac{1}{2}\ln n\rho+A_\Omega\right]$$

$$\times\sum_{k=0}^{+\infty}\frac{1}{(n\rho)^{\frac{k}{2}}}\frac{(2k)!}{2^k k!}\chi_{2k,\Omega}(v).$$

avec $v=\dfrac{\ln\rho}{\varphi(a)\,\ln B}$. En regroupant les contributions des différents Ω, ceci s'écrit encore

$$[z^n]\prod_{k=0}^{+\infty}\frac{1}{\Phi_a(z^{B^k})}\underset{n\to+\infty}{\approx}\exp\left[\frac{\ln^2\rho}{2\,\ln B}+(1+\kappa)\ln\rho+n\rho+\frac{1}{2}\ln n\rho\right]\sum_{k=0}^{+\infty}\frac{1}{(n\rho)^{\frac{k}{2}}}\varpi_k(v)$$

avec en particulier

$$\varpi_0(v)=\sum_{\Omega}\Omega^{-n}\exp\left[-\varphi(a)\lambda_\Omega v+A_\Omega+P_\Omega(v)\right].$$

C'est cette dernière formule que nous avons utilisée pour donner un équivalent dans le cas $a=3$, $B=2$.

Atlas

Au plaisir des yeux

Nous avons rencontré de nombreuses suites mahlériennes, dont certaines ont été illustrées dans le cours du texte. Nous rassemblons dans ce chapitre quelques exemples, classiques ou inédits suivant les cas. Leur intérêt est d'abord de nous étonner par leur aspect inhabituel et ensuite de faire naître des questions naturelles.

Pour ne pas alourdir l'expression nous n'avons pas toujours explicitement décrit les suites dont nous traçons les graphes. Cependant les titres de ceux-ci font facilement voir de quoi il s'agit car nous avons respecté la terminologie suivante. Le suffixe `normal` indique que l'on a normalisé la suite, généralement en la divisant par son comportement dominant. Le préfixe `sum` signifie que l'on a sommé une fois et *a contrario* le préfixe `diff` correspond à la suite des différences.

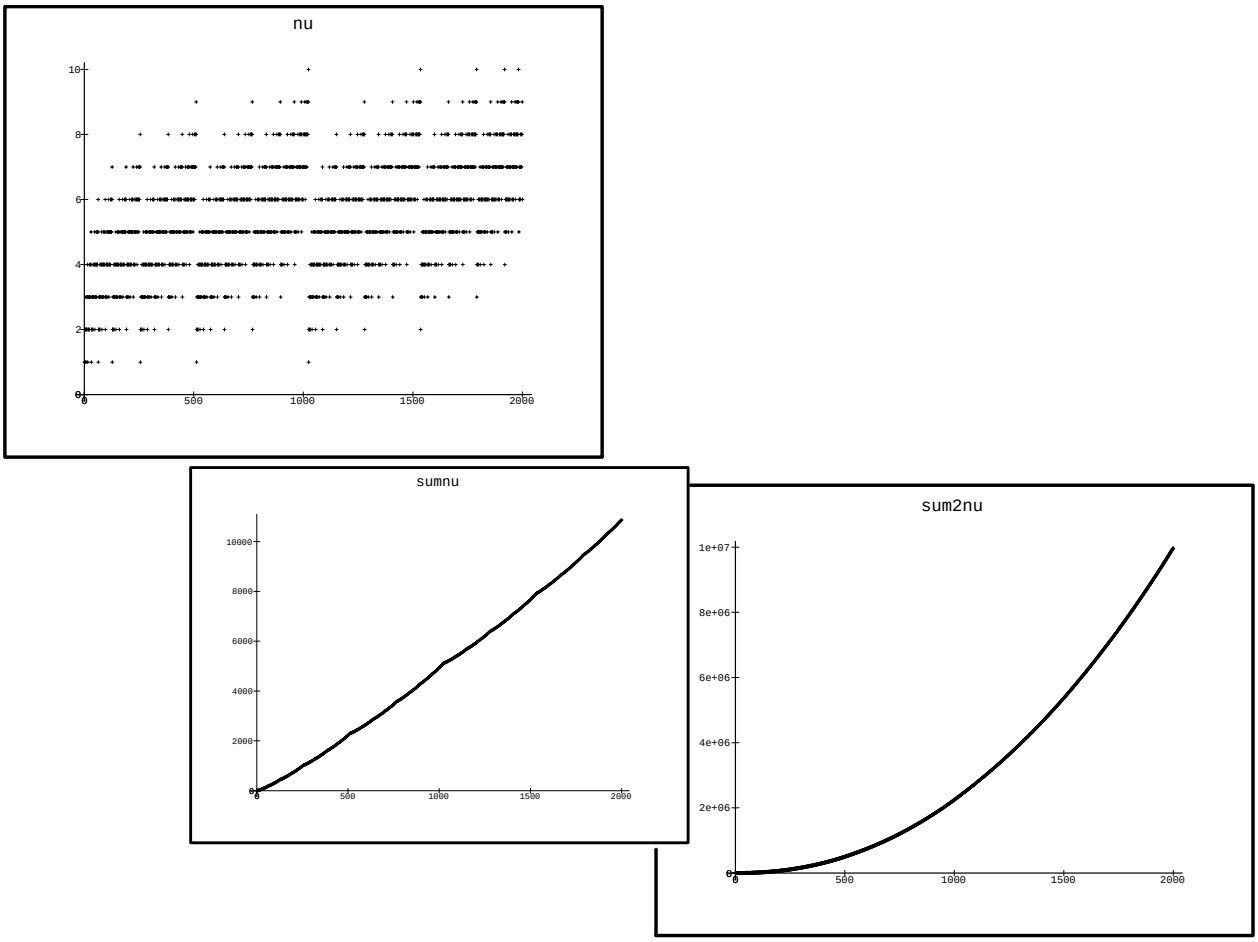

FIG. 8.7
La suite $\nu(n)$.

La suite $\nu(n)$ du nombre de 1 dans l'écriture binaire d'un entier (cf. figure `nu`) est le prototype des suites B-régulières. L'application de l'opérateur de sommation régularise la suite et fait apparaître son comportement en $n \ln n$ (cf. `sumnu`). Plus on applique cet opérateur et plus la suite obtenue est lisse (`sum2nu`). Le graphique `sumnormal` de la figure 8.8 montre la fonction périodique F associée à $\nu(n)$ par l'estimation de Delange,

$$\frac{1}{N}\sum_{n=0}^{N-1}\nu(n) = \frac{1}{2}\,\ln_2 N + F\left(\ln_2 N\right).$$

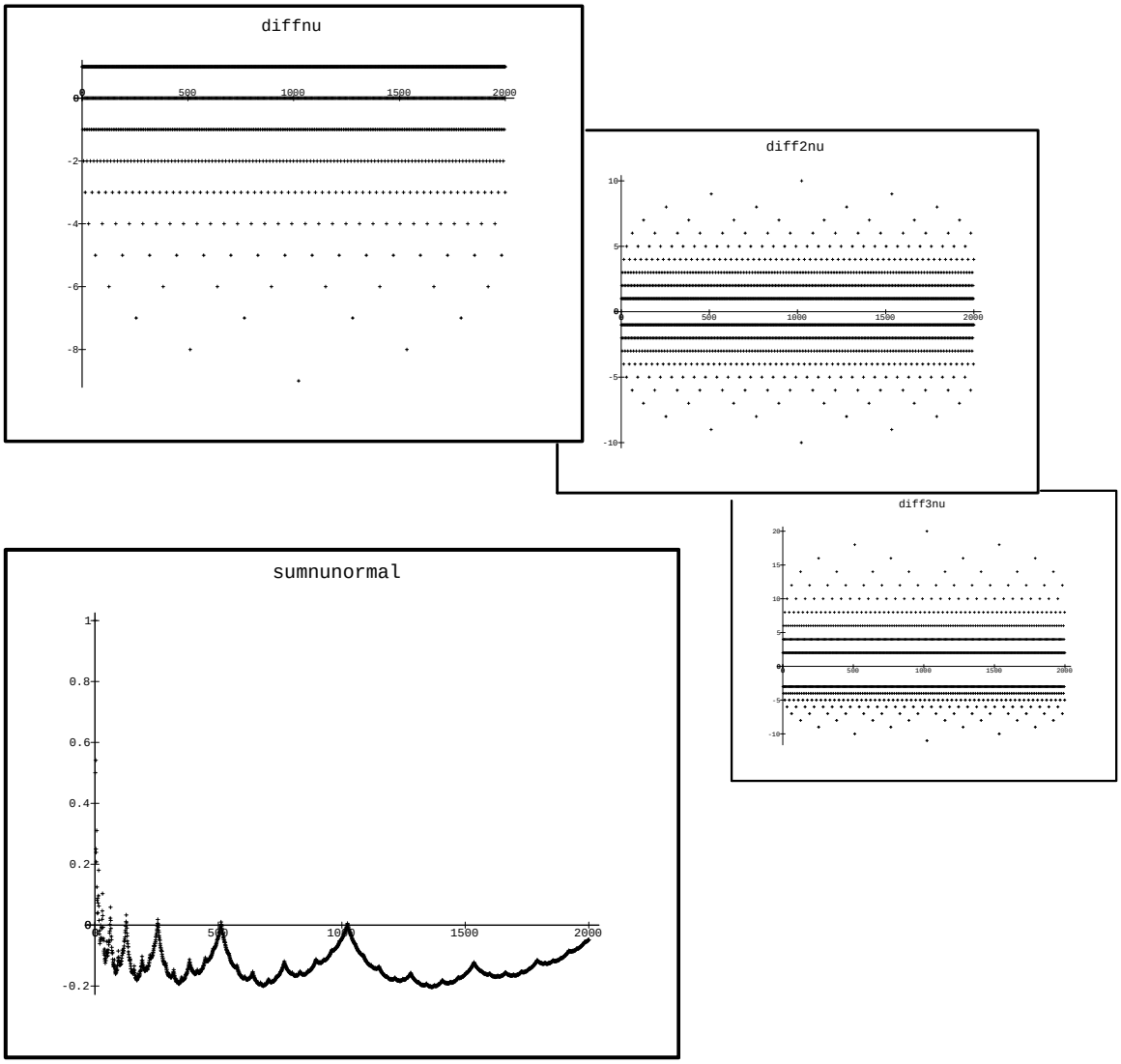

FIG. 8.8
Son comportement normalisé et ses différences.

Les différences de la suite $\nu(n)$ (graphique `diffnu`) sont directement liées à la valuation dyadique puisque

$$\Delta\nu(2\,n) = 1, \quad \Delta\nu(2\,n-1) = -v_2(n).$$

On pourrait penser qu'en itérant l'opérateur de différence sur une suite régulière, on finit par obtenir une suite automatique. Il n'en est rien et les différences k-ièmes de la suite $\nu(n)$ ont un comportement en $2^k \ln n$ (`diff2nu, diff3nu`).

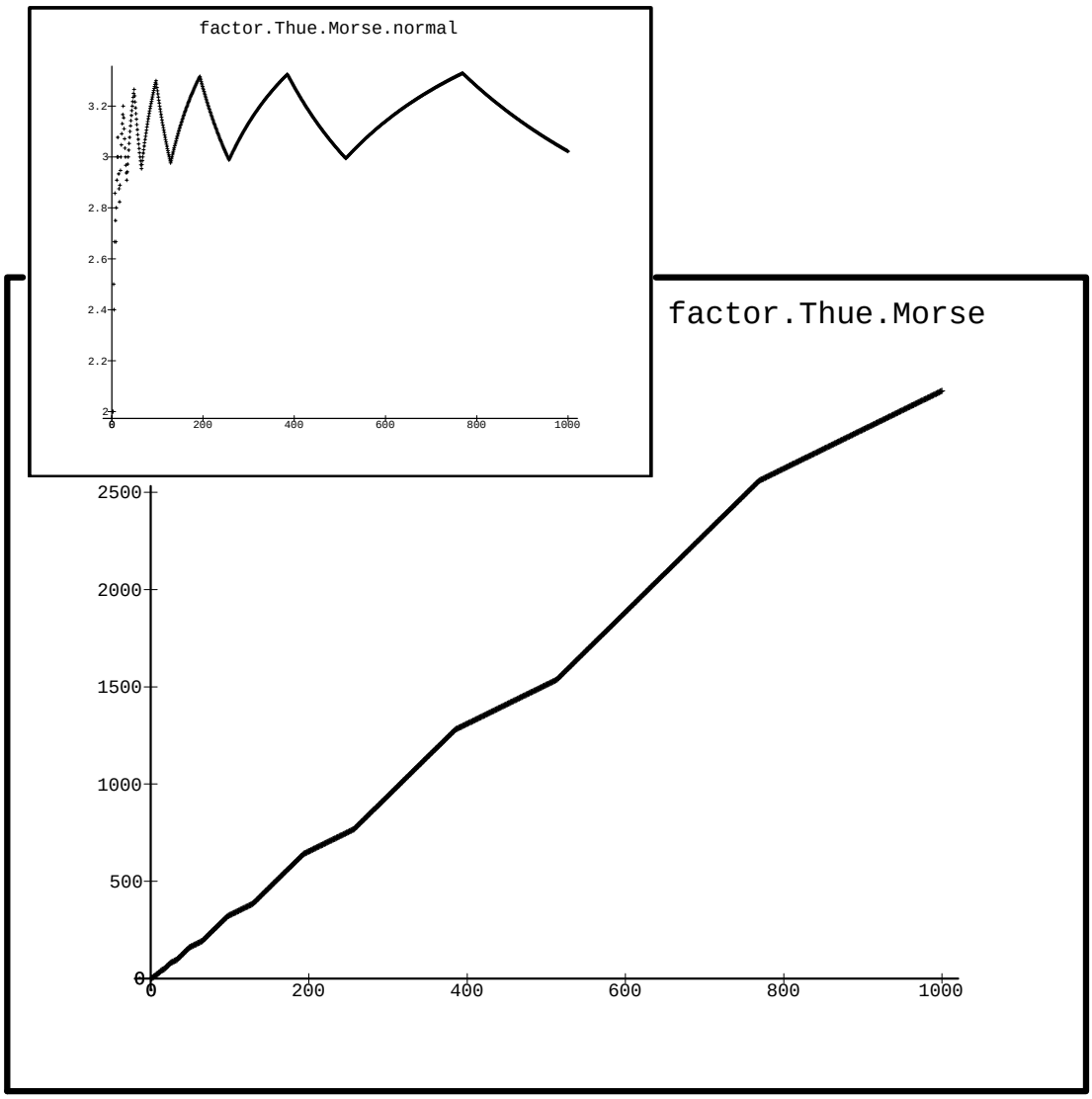

FIG. 8.9
Un avatar de la suite de Thue-Morse.

La suite de Thue-Morse, qui donne la parité du nombre de 1 dans la représentation binaire d'un entier, est le prototype des suites automatiques. Elle a donné lieu à de nombreuses études et généralisations. On voit ici le graphe de la suite $F(n)$ du nombre de facteurs, c'est-à-dire de motifs, de cette suite. Il est réunion de segments de pente alternativement 2 et 4 d'après l'expression explicite [25, p. 340],

$$F(n) = \begin{cases} 2n - 2 + 2^{\lambda(n)} & \text{si } n > 3.2^{\lambda(n)-2} + 1, \\ 4n - 4 - 2^{\lambda(n)-1} & \text{sinon.} \end{cases}$$

La périodicité s'impose naturellement dans ce cas et le dessin annexe, où l'on a divisé la suite par son comportement dominant n, la met bien en valeur.

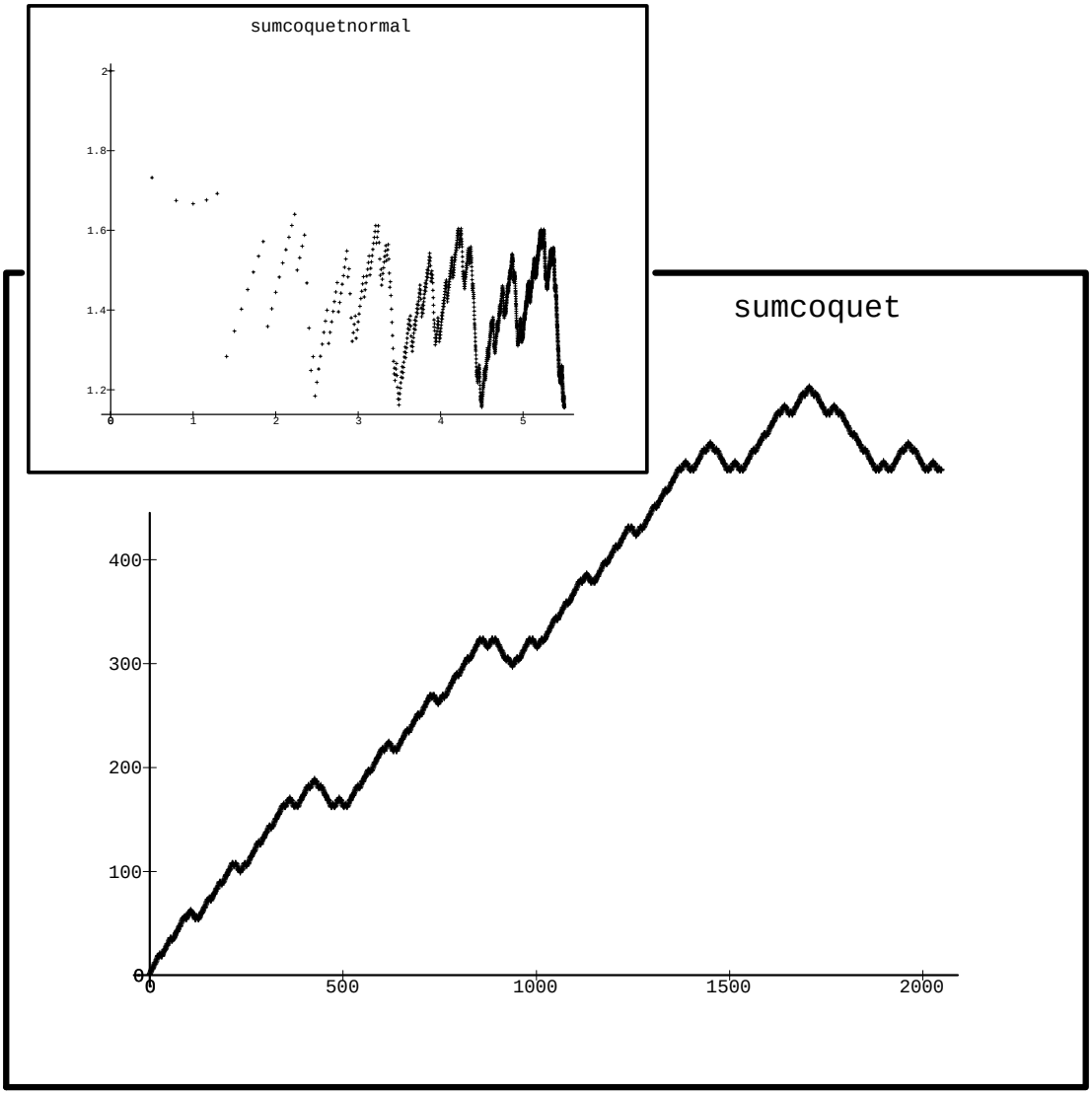

FIG. 8.10
La suite de Newman-Coquet.

La suite de Coquet associe à un entier n, la parité $(-1)^{\nu(n)}$ du nombre de 1 dans la représentation binaire de n. C'est donc une variante de la suite de la suite de Thue- Morse et elle a attiré l'attention parce que les 1 y dominent, alors qu'en moyenne ils apparaissent autant que les -1. On le constate dans son début, où l'on n'a gardé que les signes,

$$+ + + + + + + - + + + + + + - + + + + + + + + - + + .$$

Cette impression renforcée par la figure `sumcoquet` est confirmée par l'analyse puisque

$$\sum_{k<n}(-1)^{\nu(k)} = n^{\ln_4 3}\psi(\ln_4 n) + O(1),$$

où ψ est continue 1-périodique [34], comme on le voit dans la figure `sumcoquet normal`.

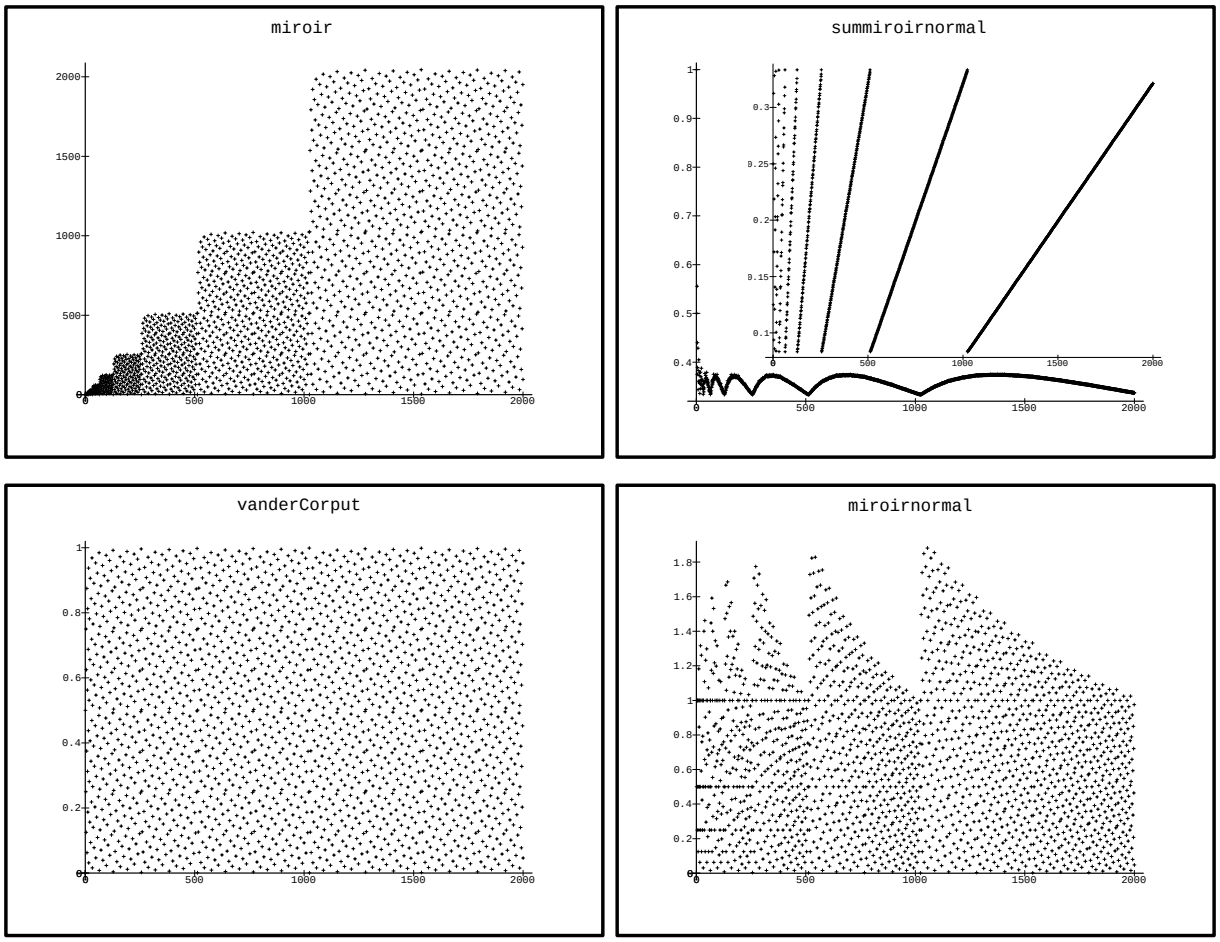

FIG. 8.11
Miroir et suite de Van der Corput.

Le miroir et la suite de Van der Corput sont deux visions du même objet. Pour le premier on associe à l'entier n la valeur de son écriture binaire retournée. Pour la seconde on fait glisser cette écriture inversée derrière la virgule. Autrement dit on divise par $2^{\lambda(n)}$ qui est le comportement dominant du miroir. On pourrait aussi bien utiliser n comme comportement dominant, mais comme on le voit sur la figure `miroirnormal` ceci structure artificiellement le graphe par des branches d'hyperboles liées au quotient $2^{\lambda(n)}/n$ et non au miroir lui-même. D'autre part la fonction sommatoire du miroir a un comportement dominant en n^2 (le rayon spectral est 4 avec une multiplicité égale à 1) et en divisant par cette quantité, la fonction périodique attendue apparaît. Cependant on peut ici aussi utiliser $4^{\lambda(n)}$ comme comportement dominant et la fonction périodique a alors une apparence plus simple car son graphe est réunion de segments (cf. `summiroirnormal`). Ceci pose un problème usuel dans l'asymptotique des suites mahlériennes : vaut-il mieux utiliser les fonctions classiques comme n ou les fonctions liées à l'écriture en base B comme $\lambda(n)$?

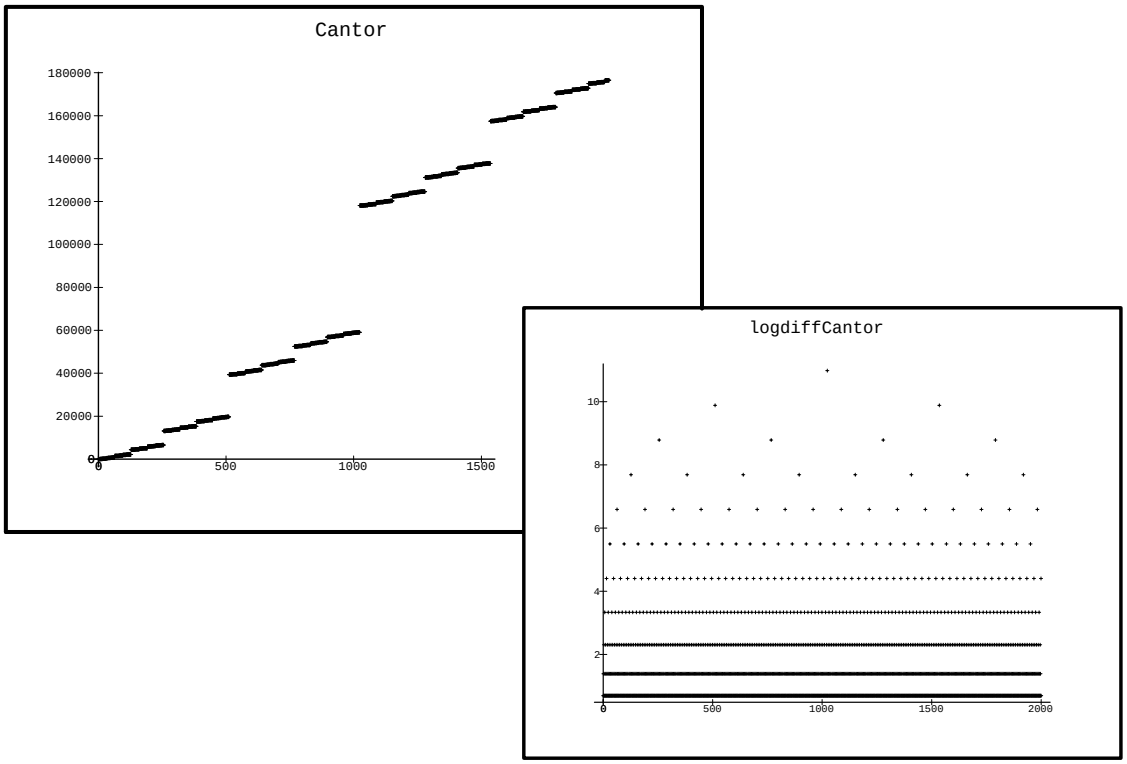

FIG. 8.12
La suite de Cantor.

La suite définie par ses deux premiers termes 0 et 1, le fait d'être strictement croissante et de ne pas contenir de progression arithmétique,

$$0,\ 1,\ 3,\ 4,\ 9,\ 10,\ 12,\ 13,\ 27,\ 28,\ 30,\ 31,\ 36,\ 37,\ 39,\ 40,\ 81,\ 82,\ 84,\ 85,\ 90,$$

est 2-régulière. Il est naturel de se demander si les sauts d'un terme au suivant

$$1,\ 2,\ 1,\ 5,\ 1,\ 2,\ 1,\ 14,\ 1,\ 2,\ 1,\ 5,\ 1,\ 2,\ 1,\ 41,\ 1,\ 2,\ 1,\ 5,\ 1,$$

restent bornés. Mais en multipliant la suite par 2, on obtient l'ensemble des entiers dont l'écriture en base 3 ne comporte pas le chiffre 1, ce qui fait sentir, par comparaison avec l'ensemble de Cantor, que les sauts ont une taille arbitrairement grande. D'ailleurs la série génératrice des différences a pour expression explicite

$$\delta(z) = \sum_{k\geq 0} \frac{3^k\, z^{2^k}}{1+z^{2^k}}$$

et les différences ont un comportement en $n^{\ln_2 3}$.

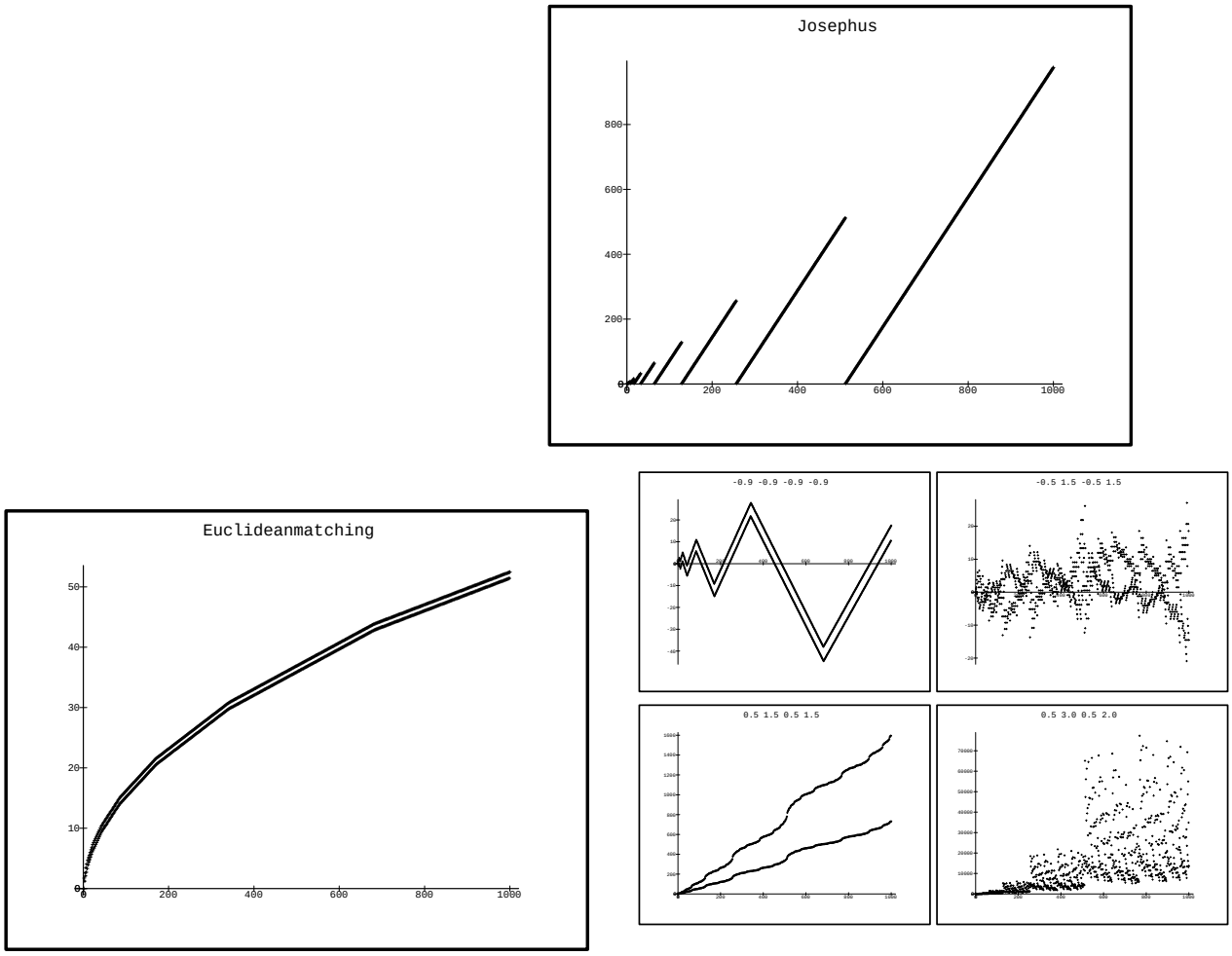

FIG. 8.13
Suites B-régulières affines par morceaux.

À l'occasion on rencontre des suites B-régulières, que l'on peut qualifier d'affines par morceaux. On a figuré ici la suite de Josephus et la suite de Reingold et Supowit apparue dans l'étude de l'appariement euclidien. Pour fabriquer de telles suites, il suffit d'utiliser la série caractéristique d'un langage rationnel de densité nulle, que l'on somme deux fois. Pour varier un peu, on remplace cette série caractéristique par son produit de Hadamard avec une série B-régulière arbitraire.

Ce phénomène semble toutefois assez superficiel. En effet si l'on généralise la récurrence de Reingold et Supowit sous la forme

$$\begin{aligned} u_{4n} &= a_0(u_{2n+1} + u_{2n-1}) + 1, & u_{4n+2} &= a_2(u_{2n+1} + u_{2n+1}) + 1, \\ u_{4n+1} &= a_1(u_{2n+1} + u_{2n}), & u_{4n+3} &= a_3(u_{2n+2} + u_{2n+1}), \end{aligned}$$

avec $u_0 = u_1 = 0$, $u_2 = 1$ et $u_3 = a_3$, on voit que quand tous les a_r sont égaux à un réel a, on a encore une suite affine par morceaux avec un comportement en $n^{1+\ln_2 a}$. Si a_0 et a_2 d'une part et a_1 et a_3 d'autre part sont égaux, les parties paires et impaires ont souvent des comportements similaires, que l'on pourrait qualifier de continus. Par contre dans le cas général on assiste à un éclatement complet.

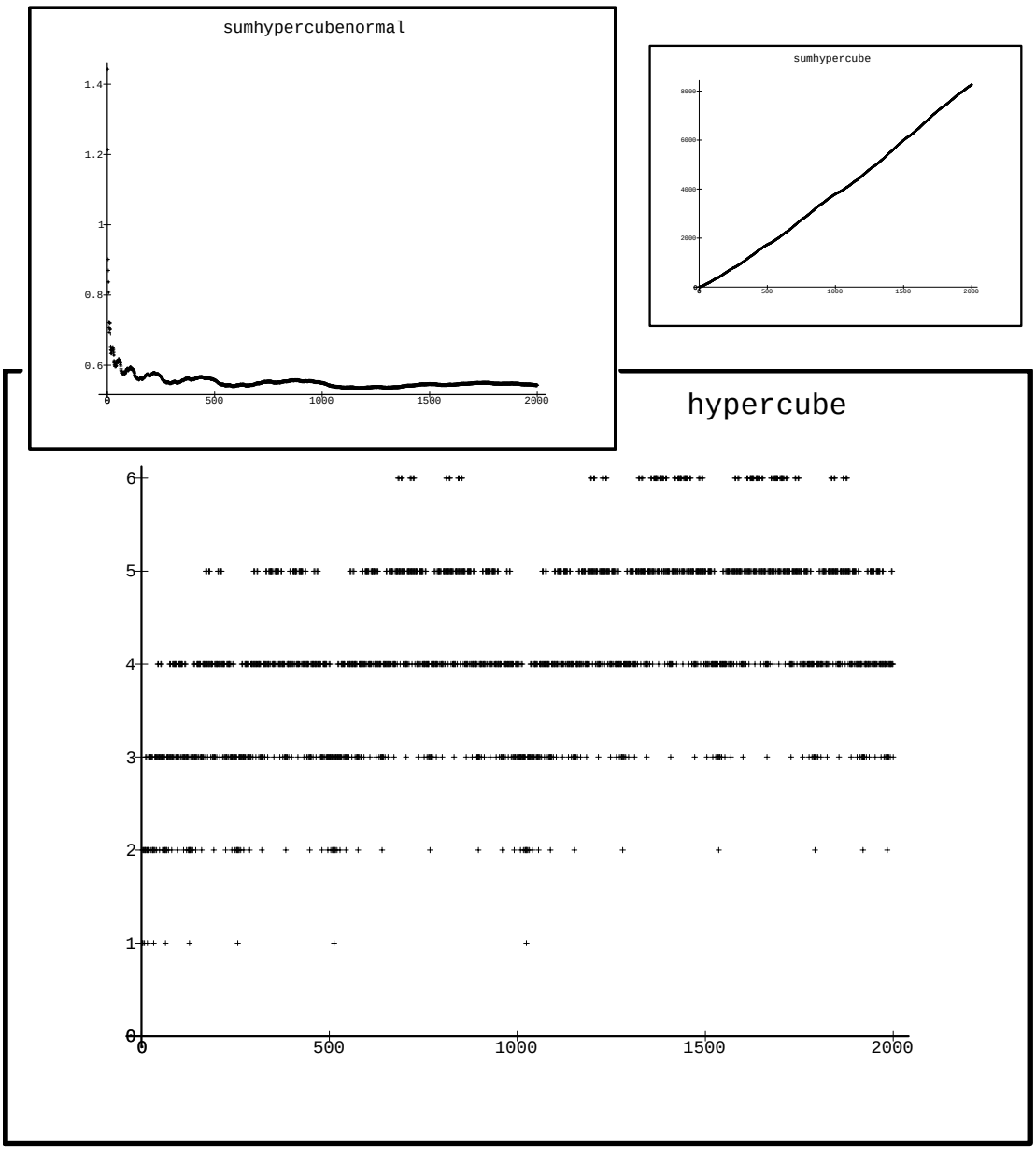

FIG. 8.14
Promenade sur un hypercube.

La recherche du plus court chemin entre deux points d'un hypercube fait considérer la suite (w_n) définie par $w_0 = 0$, $w_n = 1$ si $n = 2^k$ et $w_n = 1 + \min(w_{n-2^k}, w_{2^{k+1}-n})$ si $2^k < n < 2^{k+1}$. La fonction sommatoire de (w_n) est 2-régulière de rang 7 avec un rayon spectral $\rho = 2$ et une multiplicité $\tau = 2$. Nous attendons un comportement dominant en $n \ln n$ et en divisant par ce terme nous obtenons une suite périodique en $\ln n$.

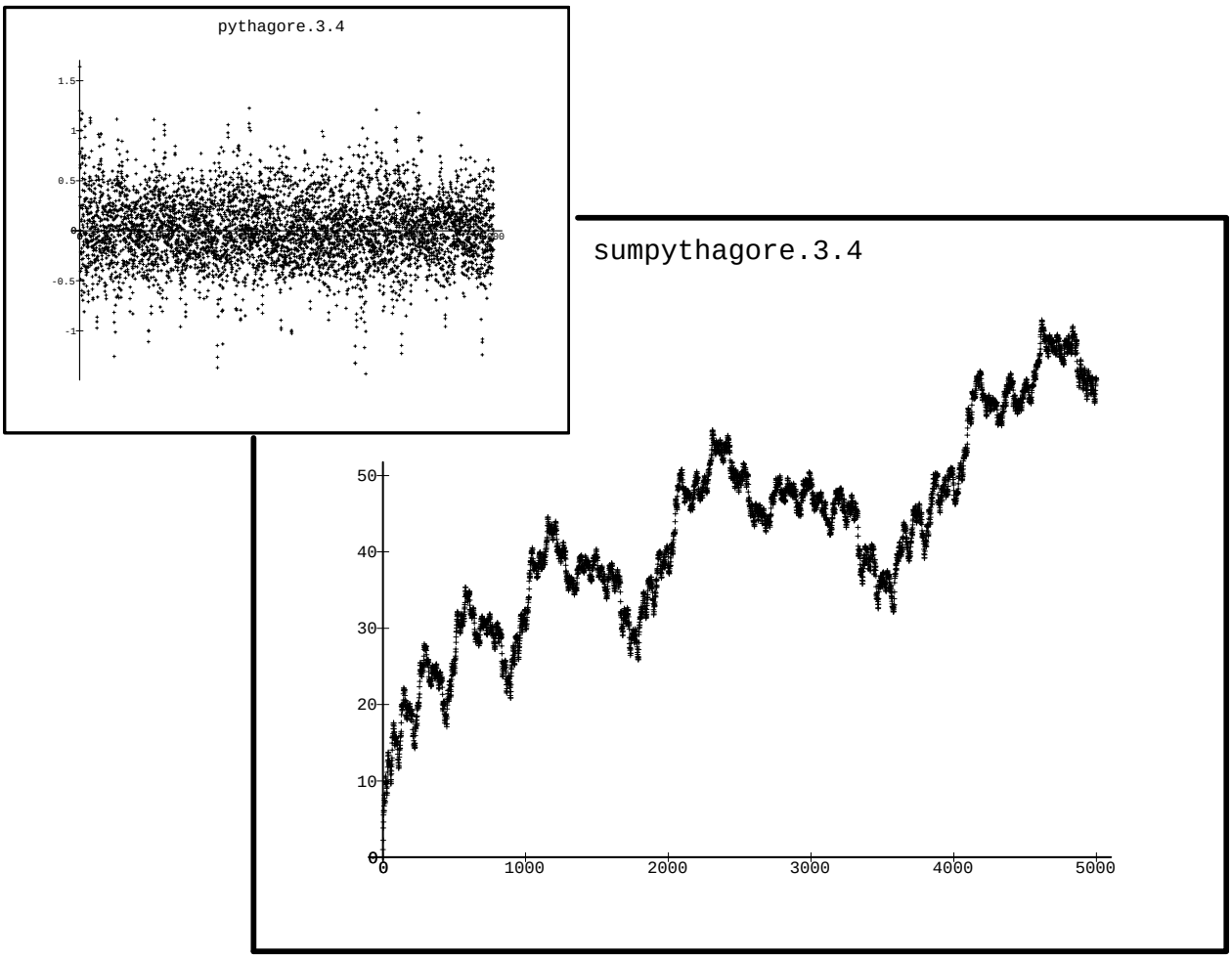

FIG. 8.15
De Pythagore à Mahler (premier tableau).

Les produits infinis mahlériens définis par des polynômes dont les racines sont de module 1 sans être des racines de l'unité n'ont pas encore été étudiés. On obtient des exemples simples en associant à un triplet pythagoricien (a, b, c) le polynôme $p(z)$ dont les racines sont les deux nombres $(a \pm ib)/c$ et le produit

$$\prod_{k\geq 0} \frac{1}{p(z^{2^k})} = \prod_{k\geq 0} \frac{1}{1 - 2\, z^{2^k} \cos\vartheta + z^{2.2^k}},$$

où $\cos\vartheta = a/c$. On a pris ici le triplet de base $a = 3$, $b = 4$, $c = 5$. La suite obtenue a des variations violentes mais la fonction sommatoire de celle-ci est déjà plus lisse et fait voir la périodicité attendue en $\ln n$.

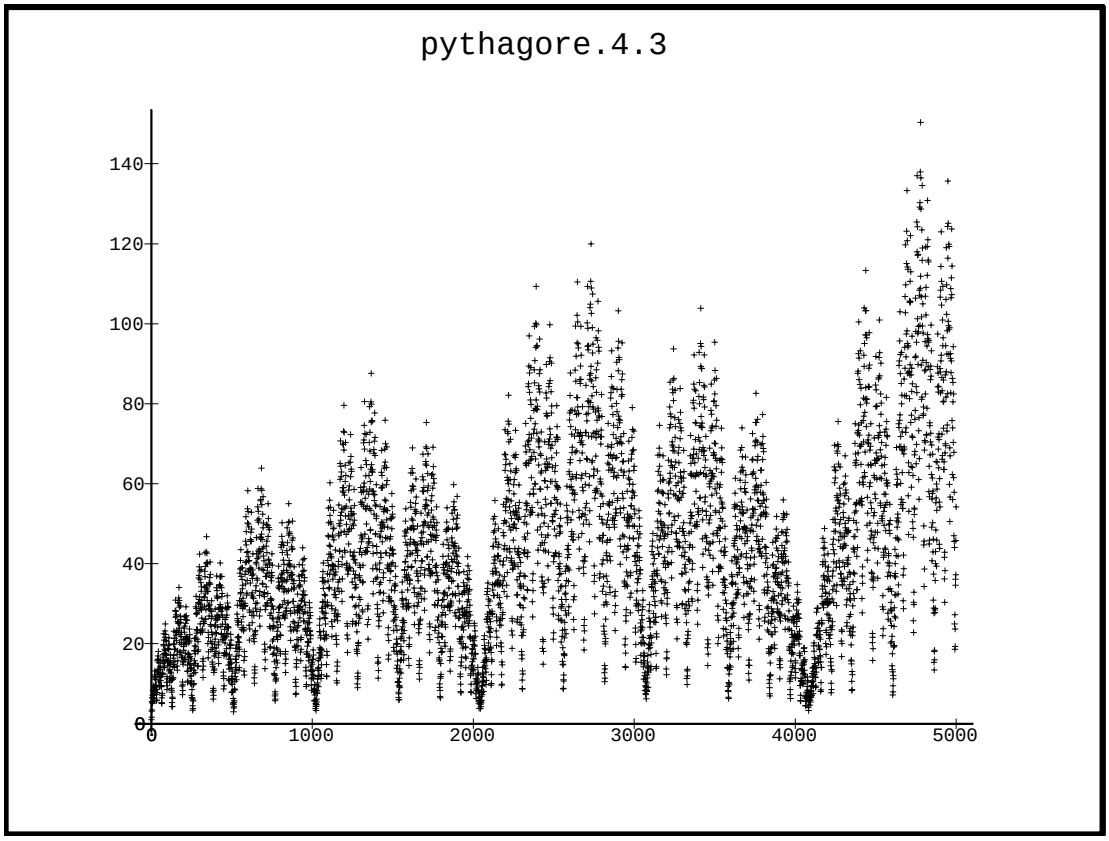

FIG. 8.16
De Pythagore à Mahler (deuxième tableau).

L'exemple précédent, modifié par l'échange de a et b, présente un aspect tout différent. La périodicité en $\ln n$ apparaît sans qu'il soit besoin de sommer, mais les variations sont encore plus prononcées.

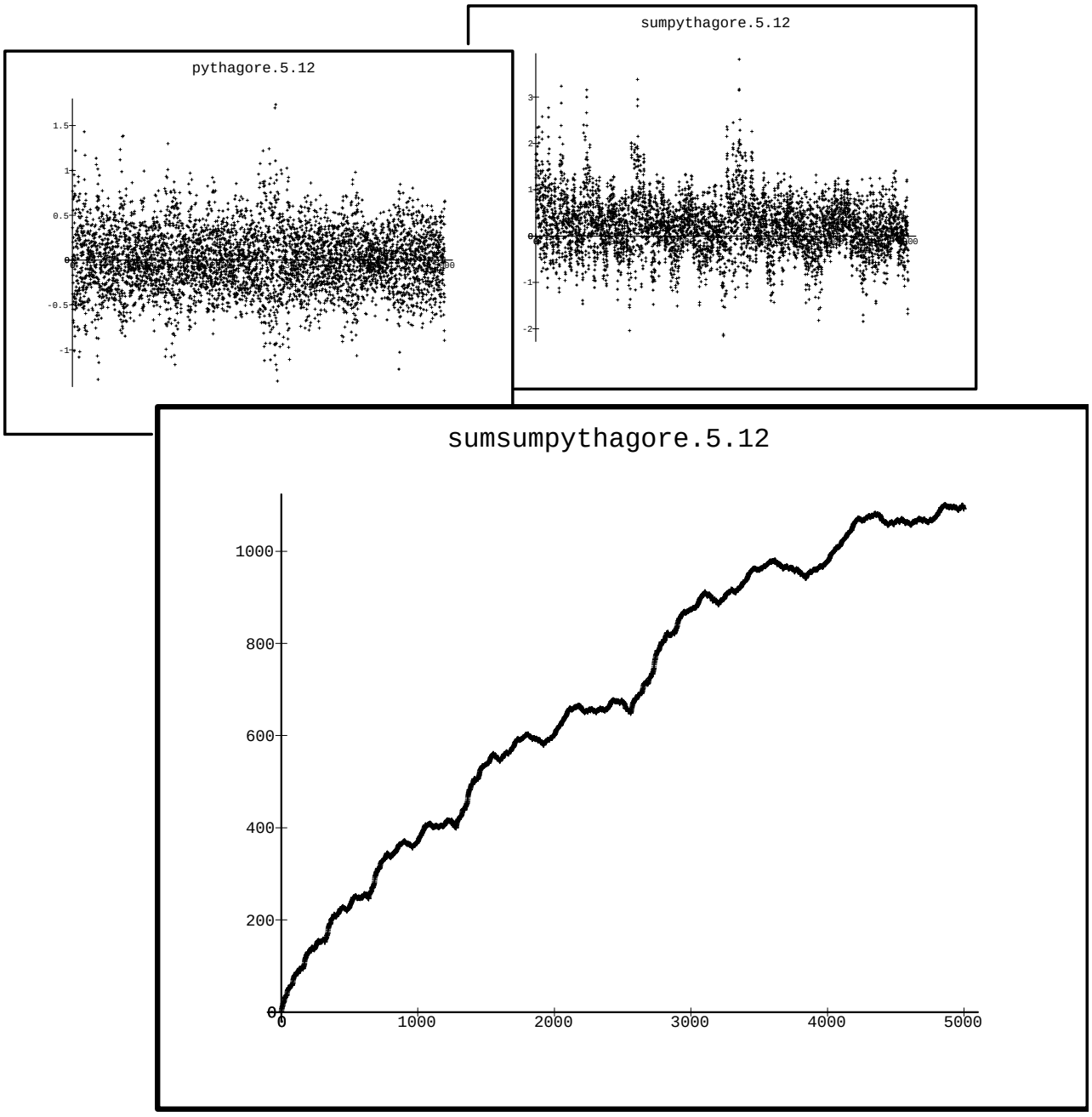

FIG. 8.17
De Pythagore à Mahler (troisième tableau).

Le triplet $a = 5$, $b = 12$, $c = 13$ amène un comportement particulièrement chaotique puisque deux sommations sont nécessaires pour obtenir un graphique disons continu.

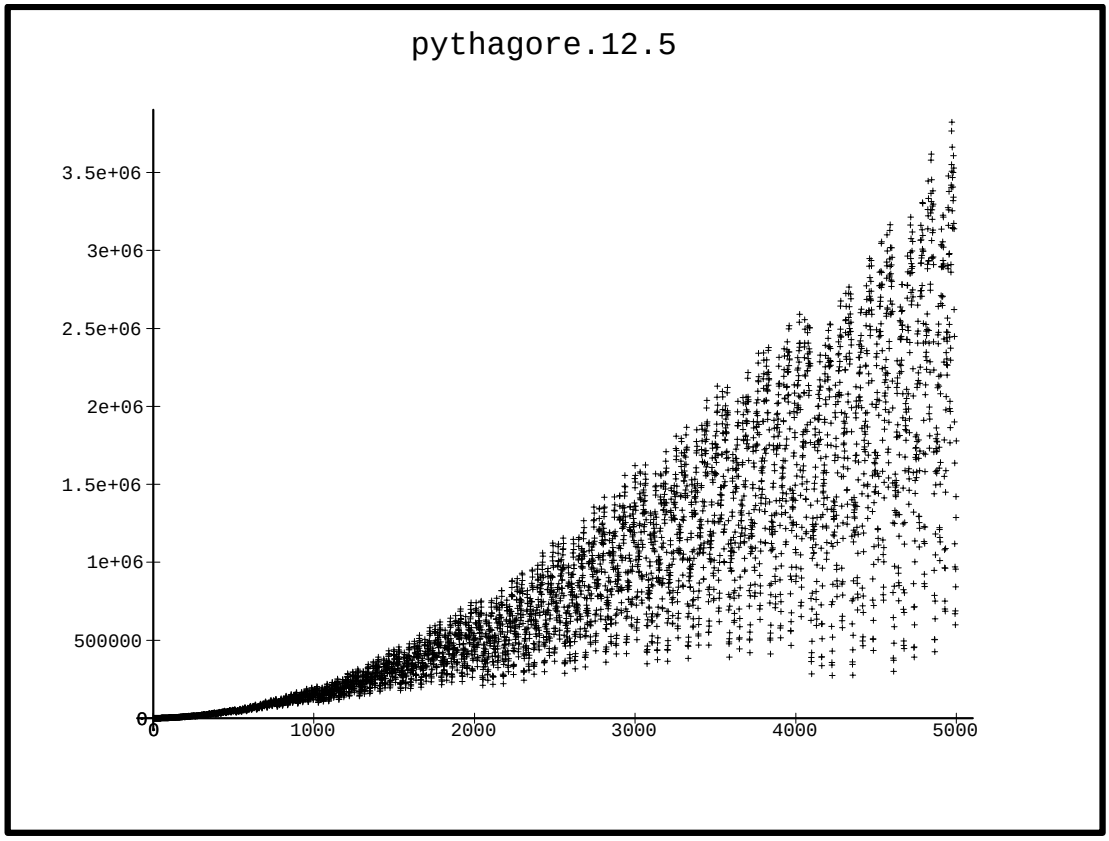

FIG. 8.18
De Pythagore à Mahler (dernier tableau).

Ici le triplet utilisé est $a = 12$, $b = 5$, $c = 13$. Nous obtenons une croissance violente de type exponentiel et par ailleurs un aspect assez lisse. Le point frappant de ces exemples est la variété des comportements, borné, logarithmique ou exponentiel, qui sont liés à la nature arithmétique de l'irrationnel ϑ/π.

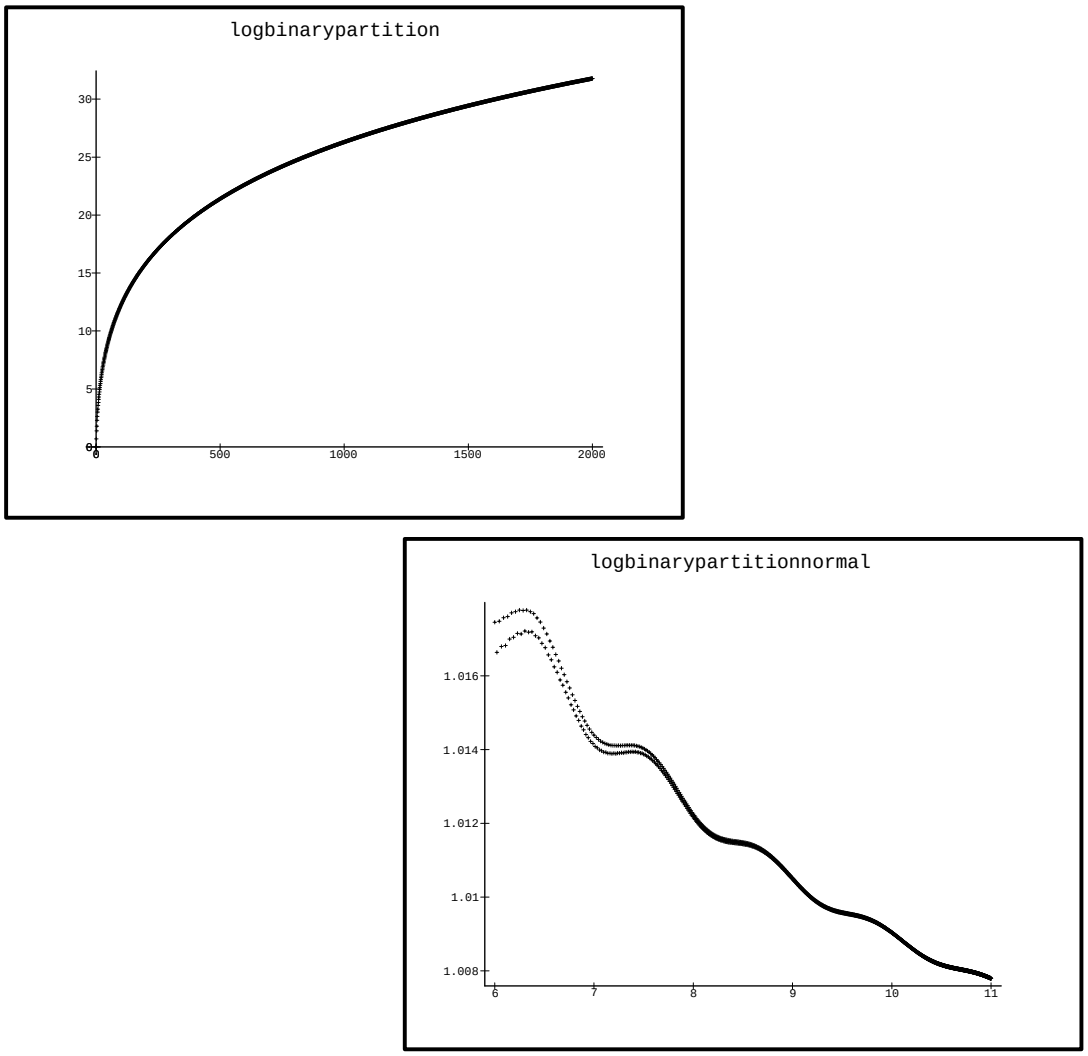

FIG. 8.19
Les partitions binaires.

La suite (b_n) du nombre de partitions binaires d'une entier a un logarithme qui se comporte en $\ln^2 n$ comme on le voit sur la figure `logbinarypartition`. Elle recèle aussi une fonction périodique en $\ln n$, qui est plus difficile à sentir. En effet dans l'échelle du problème les termes négligeables sont en $\ln^2(\ln n)/\ln n$, ce qui reste numériquement assez grand et il ne suffit pas de soustraire le comportement dominant en $\ln^2 n$ et $\ln n$ obtenu par l'analyse pour voir apparaître une fonction périodique, dont l'amplitude est très faible car elle est liée aux valeurs de la fonction Γ sur l'axe imaginaire. Pour contourner cette difficulté, on peut d'abord considérer le rapport b_{2n}/b_n, ce qui fait disparaitre le comportement en $\ln^2 n$ du logarithme de b_n, puis le birapport $\rho_n = b_n b_{4n}/b_{2n}^2$ qui élimine aussi le terme en $\ln n$. Il ne reste plus qu'à jouer sur un décalage de phase en considérant $(\rho_{6n}-1)/(\rho_{4n}-1)$ pour faire enfin sortir un comportement périodique (cf. figure `logbinarypartitionnormal`).

Prolongement

Arrivé au terme de ce travail, nous revenons sur certains points que nous avons laissé dans l'ombre soit pour ne pas alourdir la présentation, soit par force.

Nous avons développé différents algorithmes de calcul, dont certains ont été réalisés dans le langage Maple. Cette tâche doit être poursuivie, en particulier pour tester les propriétés des suites mahlériennes que l'on rencontre dans la littérature. Le travail à effectuer dépasse cependant l'écriture routinière de programmes, car beaucoup de nos raisonnements utilisent des nombres algébriques sur lesquels on doit faire des calculs exacts.

Les équations de Mahler admettent différentes extensions. On peut envisager des séries multivariées avec des opérateurs en nombre égal au nombre de variables ; ou bien rester dans le domaine des séries à une variable mais avec plusieurs opérateurs, ce que nous avons très légérement envisagé dans le chapitre 3. Il est aussi possible de considérer des équations mixtes, à la fois différentielles et mahlériennes.

Il est clair que l'on peut poursuivre l'étude des solutions sous forme close en cherchant par exemple si une équation de Mahler possède des solutions rationnellement dépendantes, ce qui permettrait de lever la difficulté apparue au chapitre 5 dans la recherche de l'équation minimale satisfaite par une série B-régulière.

La traduction des propriétés des séries rationnelles en indéterminées non commutatives, si elle n'est pas complète, ne semble pas présenter de difficultés particulières et il nous semble plus intéressant d'en montrer les applications que de l'approfondir pour l'instant. Le lien entre les séries B-régulières et les séries mahlériennes nous semble plus ardu car il y a peu d'espoir de caractériser les équations mahlériennes dont toutes les solutions sont B-régulières. Il n'est pas impossible que l'équation minimale d'une telle série vérifie systématiquement le critère que nous avons donné.

L'asymptotique est certainement la partie la plus prometteuse. D'abord il reste à traiter deux cas de notre classification et si nous entrevoyons déjà certains comportements, il faudra encore quelques acrobaties pour atteindre des résultats complets. Il est dès maintenant possible de fusionner certains cas étudiés. À terme nous espérons bien pouvoir décrire tous les comportements possibles. Bref nous trépignons d'impatience.

Bibliographie

[1] Abramowitz, M., and Stegun, I. A. *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, vol. 55 of *National Bureau of Standards Applied Mathematics Series*. For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C., 1964.

[2] Allouche, J.-P. Somme des chiffres et transcendance. *Bull. Soc. Math. France 110*, 3 (1982), 279–285.

[3] Allouche, J.-P. Automates finis en théorie des nombres. *Exposition. Math. 5*, 3 (1987), 239–266.

[4] Allouche, J.-P. Sur la transcendance de la série formelle Π. *Sém. Théor. Nombres Bordeaux (2) 2*, 1 (1990), 103–117.

[5] Allouche, J.-P., and Cohen, H. Dirichlet series and curious infinite products. *Bull. London Math. Soc. 17*, 6 (1985), 531–538.

[6] Allouche, J.-P., and Shallit, J. The ring of k-regular sequences. *Theoret. Comput. Sci. 98*, 2 (1992), 163–197.

[7] Andrews, G. E. *The theory of partitions*. Addison-Wesley Publishing Co., Reading, Mass.-London-Amsterdam, 1976. Encyclopedia of Mathematics and its Applications, Vol. 2.

[8] Apostol, T. M. *Introduction to analytic number theory*. Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[9] Beauquier, J., and Thimonier, L. Prefix-free words of length n over m letters : two-sided well-balanced parentheses and palindromes. In *Combinatoire énumérative (Montreal, Que., 1985/Quebec, Que., 1985)*, vol. 1234 of *Lecture Notes in Math.* Springer, Berlin, 1986, pp. 27–33.

[10] Becker, P.-G. k-regular power series and Mahler-type functional equations. *J. Number Theory 49*, 3 (1994), 269–286.

[11] Berlekamp, E. R. *Algebraic coding theory*. McGraw-Hill Book Co., New York, 1968.

[12] Berstel, J. Ensembles reconnaissables de nombres. In *Langages algébriques (Proc. First Meeting, Information Theory, Bonascre, 1973)*. École Nat. Sup. Tech. Avancées, Paris, 1978, pp. 23–84.

[13] Berstel, J., and Reutenauer, C. *Les séries rationnelles et leurs langages*. Études et Recherches en Informatique. [Studies and Research in Computer Science]. Masson, Paris, 1984.

[14] Borevitch, Z. I., and Chafarevitch, I. R. *Théorie des nombres*. Traduit par Myriam et Jean-Luc Verley. Traduction faite d'après l'édition originale russe. Monographies Internationales de Mathématiques Modernes, No. 8. Gauthier-Villars, Paris, 1967.

[15] Bradford, R. J., and Davenport, J. H. Effective tests for cyclotomic polynomials. In *Symbolic and algebraic computation (Rome, 1988)*, vol. 358 of *Lecture Notes in Comput. Sci.* Springer, Berlin, 1989, pp. 244–251.

[16] Brlek, S. Enumeration of factors in the Thue-Morse word. *Discrete Appl. Math. 24*, 1-3 (1989), 83–96. First Montreal Conference on Combinatorics and Computer Science, 1987.

[17] Cartan, H. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*. Avec le concours de Reiji Takahashi. Enseignement des Sciences. Hermann, Paris, 1961.

[18] Christol, G., Kamae, T., Mendès France, M., and Rauzy, G. Suites algébriques, automates et substitutions. *Bull. Soc. Math. France 108*, 4 (1980), 401–419.

[19] Churchhouse, R. F. Congruence properties of the binary partition function. *Proc. Cambridge Philos. Soc. 66* (1969), 371–376.

[20] Cobham, A. On the base-dependence of sets of numbers recognizable by finite automata. *Math. Systems Theory 3* (1969), 186–192.

[21] Comtet, L. *Analyse combinatoire. Tomes I, II*, vol. 5 of *Collection SUP : "Le Mathématicien", 4*. Presses Universitaires de France, Paris, 1970.

[22] Comtet, L. *Advanced combinatorics*, enlarged ed. D. Reidel Publishing Co., Dordrecht, 1974. The art of finite and infinite expansions.

[23] de Bruijn, N. G. On Mahler's partition problem. *Nederl. Akad. Wetensch., Proc. 51* (1948), 659–669 = Indagationes Math. 10, 210–220 (1948).

[24] de Bruijn, N. G. *Asymptotic methods in analysis*, third ed. Dover Publications Inc., New York, 1981.

[25] de Luca, A., and Varricchio, S. Some combinatorial properties of the Thue-Morse sequence and a problem in semigroups. *Theoret. Comput. Sci. 63*, 3 (1989), 333–348.

[26] Dekking, M., Mendès France, M., and van der Poorten, A. Folds. *Math. Intelligencer 4*, 3 (1982), 130–138.

[27] Delange, H. Sur la fonction sommatoire de la fonction"somme des chiffres". *Enseignement Math. (2) 21*, 1 (1975), 31–47.

[28] Doetsch, G. *Theorie und Andwendung der Laplace-Transformation*, vol. XLVII of *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen*. Verlag von Julius Springer, 1937.

[29] Doubilet, P., Rota, G.-C., and Stanley, R. On the foundations of combinatorial theory. VI. The idea of generating function. In *Proceedings of the Sixth Berkeley Symposium on Mathematical Statistics and Probability (Univ. California, Berkeley, Calif., 1970/1971), Vol. II : Probability theory* (Berkeley, Calif., 1972), Univ. California Press, pp. 267–318.

[30] Dumont, J.-M., and Thomas, A. Systèmes de numération et fonctions fractales relatifs aux substitutions. *Theoret. Comput. Sci. 65*, 2 (1989), 153–169.

[31] Eilenberg, S. *Automata, languages, and machines. Vol. A*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York, 1974. Pure and Applied Mathematics, Vol. 58.

[32] Flajolet, P. *Analyse d'algorithmes de manipulation d'arbres et de fichiers*. Doctorat ès sciences, Université de Paris XI at Orsay, 1979.

[33] Flajolet, P., and Golin, M. Mellin transforms and asymptotics. The mergesort recurrence. *Acta Inform. 31*, 7 (1994), 673–696.

[34] Flajolet, P., Grabner, P., Kirschenhofer, P., Prodinger, H., and Tichy, R. F. Mellin transforms and asymptotics : digital sums. *Theoret. Comput. Sci. 123*, 2 (1994), 291–314.

[35] Flajolet, P., and Schott, R. Nonoverlapping partitions, continued fractions, Bessel functions and a divergent series. *European J. Combin. 11*, 5 (1990), 421–432.

[36] Gaudel, M.-C., Soria, M., and Froidevaux, C. *Types de données et algorithmes. Vol. II*, vol. 4 of *Collection Didactique [Didactic Collection]*. Institut National de Recherche en Informatique et en Automatique (INRIA), Rocquencourt, 1987. Recherche, tri, algorithmes sur les graphes. [Searching, sorting and graph algorithms], With an English summary.

[37] Goulden, I. P., and Jackson, D. M. *Combinatorial enumeration*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1983. With a foreword by Gian-Carlo Rota, Wiley-Interscience Series in Discrete Mathematics.

[38] Graham, R. L., Knuth, D. E., and Patashnik, O. *Concrete mathematics*. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1989. A foundation for computer science.

[39] Gramain, F., Mignotte, M., and Waldschmidt, M. Valeurs algébriques de fonctions analytiques. *Acta Arith. 47*, 2 (1986), 97–121.

[40] Greene, D. H., and Knuth, D. E. *Mathematics for the analysis of algorithms*, vol. 1 of *Progress in Computer Science*. Birkhäuser Boston, Mass., 1981.

[41] Guibas, L. J., and Odlyzko, A. M. Periods in strings. *J. Combin. Theory Ser. A 30*, 1 (1981), 19–42.

[42] Henrici, P. *Applied and computational complex analysis. Vol. 2*. Wiley Interscience [John Wiley & Sons], New York, 1977. Special functions—integral transforms—asymptotics—continued fractions.

[43] Hwang, H.-K., and Steyeart, J.-M. On the number of heaps. Research Report LIX/RR/93/01, Ecole Polytechnique–LIX, Jan. 1993.

[44] Ifrah, G. *Histoire universelle des chiffres*. Seghers, 1981.

[45] Jacob, G. Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices. *Theoret. Comput. Sci. 5*, 2 (1977/78), 183–204.

[46] Kubota, K. K. On a transcendance problem of K. Mahler. Rapport IHES, Mar. 1976.

[47] Kuczma, M. *Functional Equations in a Single Variable*, vol. Tom 46 of *Polska Akademia Nauk, Monografie Matematyczne*. PWN Polish Scientific Publishers, 1968.

[48] Kuczma, M., Choczewski, B., and Ger, R. *Iterative Functional Equations*, vol. 32 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1990.

[49] Lipshitz, L. *D*-finite power series. *J. Algebra 122*, 2 (1989), 353–373.

[50] Loxton, J. H., and Van der Poorten, A. J. Transcendence and algebraic independence by a method of Mahler. In *Transcendence theory : advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976)*. Academic Press, London, 1977, pp. 211–226.

[51] Mahler, K. Arithmetische Eigenschaften der Lösungen einer Klasse von Funktionalgleichungen. *Math. Ann. 101*, 1 (1929), 342–366.

[52] Mahler, K. On a special functional equation. *J. London Math. Soc. 15* (1940), 115–123.

[53] Mahler, K. Fifty years as a mathematician. *J. Number Theory 14*, 2 (1982), 121–155.

[54] Mendès France, M., and van der Poorten, A. J. Automata and the arithmetic of formal power series. *Acta Arith. 46*, 3 (1986), 211–214.

[55] Mercouroff, N., and Weitzman, A. Automatic Analysis of the Execution Time of a Class of Parallel Recursive Algorithms, 1991.

[56] Morain, F., and Olivos, J. Speeding up the computations on an elliptic curve using addition-subtraction chains. *RAIRO Inform. Théor. Appl. 24*, 6 (1990), 531–543.

[57] Narkiewicz, W. *Elementary and analytic theory of algebraic numbers*. PWN—Polish Scientific Publishers, Warsaw, 1974. Monografie Matematyczne, Tom 57.

[58] Nielsen, N. *Die Gammafunktion von Niels Nielsen*. Chelsea Publishing Compagny, New York, 1965. Reprinting of Handbuch der Theorie der Gammafunktion (1906) and Theorie der Integrallogaritmus und verwandter Transzendenten (1906).

[59] Odlyzko, A. M., and Wilf, H. S. Functional iteration and the Josephus problem. *Glasgow Math. J. 33*, 2 (1991), 235–240.

[60] Parent, D. P. *Exercices de théorie des nombres*. Gauthier-Villars, Paris, 1978. Avec la collaboration de Daniel Barsky, Françoise Bertrandias, Gilles Christol, Annette Decomps, Hubert Delange, Jean-Marc Deshouillers, Khyra Gérardin, Jean Lagrange, Jean-Louis Nicolas, Martine Pathiaux, Gérard Rauzy and Michel Waldschmidt, Avec une preface de Ch. Pisot et un avant-propos de Jean-Louis Nicolas.

[61] Régnier, M. Enumeration of bordered words. The language of the laughing cow. *RAIRO Inform. Théor. Appl. 26*, 4 (1992), 303–317.

[62] Reutenauer, C. Séries rationnelles et algèbres syntactiques. Master's thesis, Université Pierre et Marie Curie (Paris VI), 1980.

[63] Salomaa, A., and Soittola, M. *Automata-theoretic aspects of formal power series*. Springer-Verlag, New York, 1978. Texts and Monographs in Computer Science.

[64] Sedgewick, R. *Algorithms*. Addison-Wesley Series in Computer Science. Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983.

[65] Stanley, R. P. Differentiably finite power series. *European J. Combin. 1*, 2 (1980), 175–188.

[66] Stolarsky, K. B. Power and exponential sums of digital sums related to binomial coefficient parity. *SIAM J. Appl. Math. 32*, 4 (1977), 717–730.

[67] Supowit, K. J., and Reingold, E. M. Divide and conquer heuristics for minimum weighted Euclidean matching. *SIAM J. Comput. 12*, 1 (1983), 118–143.

[68] Tenenbaum, G. *Introduction à la théorie analytique et probabiliste des nombres*, second ed., vol. 1 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, 1995.

[69] Titchmarsh, E. C. *The theory of the Riemann zeta-function*, second ed. The Clarendon Press Oxford University Press, New York, 1986. Edited and with a preface by D. R. Heath-Brown.

[70] Warner, S. *Modern algebra. Vols. I, II*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1965.

[71] Whittaker, E. T., and Watson, G. N. *A course of modern analysis. An introduction to the general theory of infinite processes and of analytic functions : with an account of the principal transcendental functions*. Fourth edition. Reprinted. Cambridge University Press, New York, 1962.

[72] Zeilberger, D. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math. 32*, 3 (1990), 321–368.

Index

abscisse de convergence absolue, 160
algèbre $\mathbb{A}[[z, M]]$, 109
algèbre $\mathbb{K}(z)[M]$, 21
algorithme
    `équation_de_mahler`, 105
    `forme_quasi_normale`, 54
    `solution_produit`, 57
    `solution_rationnelle`, 50
Allouche J.-P., 65, 75, 86, 88, 94, 103, 163
alphabet, 67
annulateur d'une série, 83
antihomomorphisme, 114
appariement euclidien, 127
appariemment euclidien, 210
autocorrélation d'un mot, 43, 92, 165

base de numération, 11, 67
Baum-Sweet (suite de –), 122
Bell (nombres de –), 123
Berlekamp E., 16
Berstel J., 95

Cantor (suite de –), 75, 104, 120, 125, 209
cas ordinaire, marginal, hypermarginal, 155
Cauchy (produit de –)
    –, 11
    sections d'un –, 20, 88
    stabilité par le –, 31, 87, 91, 126
chiffre, 67, 78, 86, 113, 114
Christol G., 123
Churchhouse R., 138
Cobham A., 94
code suffixe, 84
Cohen H., 163
corrélation de deux mots, 43
cycle (distance à un –), 12
cyclique (élément –), 12
cyclotomique (polynôme –), 13

De Bruijn N., 167, 174
De Luca A., 160
degré d'un opérateur, 22
densité d'un langage, 92
dérivation (stabilité par la –), 31, 88
descendant d'un polynôme, 15, 55
distance à un cycle, 12
division à droite, 70

écriture d'un entier
    –, 67
    nombre de 1 dans l'–, 79, 150, 204–205
égalité (théorème d'–), 41, 85, 101
Eisenstein (critère d'–), 41, 89
entier critique, 37, 40
équation de Mahler
    –, 30
    – minimale, 30
    – générale, 39
équation de point fixe, 40, 45, 113, 148
équation fonctionnelle infinie, 163
Euler L., 59
extension d'une suite aux rationnels, 30

Fatou (lemme de –), 98
Fibonacci (variante de la suite de –), 136, 164
fils d'un polynôme
    –, 15, 55
    – cyclotomique, 14
Flajolet Ph., 123, 150, 160
fonction exponentiellement petite, 191
forme quasi-normale, 54
Fredholm (série de –), 68

graeffe (application –), 14
Graham R., 73
Gray (code de –), 141, 150
Greene D., 88
Guibas L., 43, 92, 165

Hadamard (produit d'–)

–, 11, 88
stabilité par le –, 32, 87, 91
Hankel (matrice de –), 76
Hurwitz (fonction d'–), 174, 176
Hwang H.-K., 69
hypermarginal (cas –), 155

idéal de $\mathbb{K}(z)[M]$, 23

Jacob G., 95, 98
Jacobi (fraction continuée de –), 123
Josephus (problème de –), 73, 75, 210

Kamae T., 123
Kleene-Schützenberger (théorème de –), 68
Knuth D., 73, 88
Kronecker L. (lemme de –), 15
Kuczma M., 58

libre de carré (entier –), 13
longueur, 68, 151

Mahler K., 9, 167
marginal (cas –), 155
Mendès France M., 123
miroir, 72, 91, 116, 208
mot à bord, 43
motif (occurrences d'un –), 150

Newman-Coquet (suite de –), 207

Odlyzko A., 43, 76, 92, 165
opérateur
– B-propre, 115
– de condensation, 91
– de Mahler, 12, 21
– de multiplication, 21
– de section, 19, 70, 71, 77, 83
– de décalage, 20
– quasi-inversible, 112
– rationnel, 114
ordinaire (cas –), 155
ordre de croissance, 90, 151
ordre sur les mots, 77
ordre de multiplicité, 154

palindrome, 51
partie d'un entier étrangère à un autre, 14
partie suffixielle, 84
partition B-aire, 216
partition B-aire, 32, 42, 136, 166
partition d'ensemble, 123
Pascal (parité dans le triangle de –), 106, 139, 160
Patashnik O., 73
période d'un polynôme, 16, 130
Perron (formule de –), 150
pgcd dans $\mathbb{K}(z)[M]$, 23
pliage de papier (suite du –), 95
polynôme cyclotomique, 13
ppcm dans $\mathbb{K}(z)[M]$, 24
preuve par neuf, 90
produit d'Hadamard, 11
produit de Cauchy, 11
produit mahlérien
– évanescent, 59
– B-régulier, 130, 133
promenade, 163, 211

quotient euclidien, 20

racine majeure, mineure, 173
radical d'un entier, 13
rang d'une série B-régulière, 77
Rauzy G., 123
rayon spectral, 151
recherche d'un entier, 88
récurrence typique, 84, 97, 141
Régnier M., 43
Reingold E., 127
représentation linéaire
– d'une série B-régulière, 69
– réduite, 78, 86
– standard, 74
– typique, 85
dimension d'une –, 69
Reutenauer Ch., 94, 95
Rota G.-C., 87
Rudin-Shapiro (suite de –), 39

Schützenberger (théorème de –), 107
série B-automatique, 94
série B-régulière
condensée d'une –, 162
série B-régulière
ordre de multiplicité d'une –, 154
série B-régulière

–, 68
annulateur d'une –, 83
condensée d'une –, 91
rang d'une –, 77
rayon spectrale d'une –, 151
série condensée, 91
série du logarithme, 32, 89, 92
série formelle
–, 11
– de Laurent, 11, 48
ultramétrique des –, 11
série mahlérienne
–, 30
équation minimale d'une –, 30
théorème de structure des –, 149
série rationnelle
–, 68
– associée, 72, 74
série reconnaissable, 68
Shallit J., 65, 75, 86, 88, 94
stable (sous-ensemble –), 12
Steyeart J.-M., 69
Stolarsky K., 160
suite mahlérienne, 31
suite B-régulière, 68
Supowit K., 127
support d'une série, 67

tas (heaps), 69, 99
Thue-Morse (suite de –), 50, 78, 89, 108, 160, 206
tri-fusion (coût du –), 53, 81, 83, 85, 154, 157

valeur d'un mot, 67
valuation, 11, 109
Van der Corput (suite de –), 208
Varricchio S., 160

Wilf H., 76

Table des matières

I Aspect algébrique **7**

1 Opérateurs **11**
1.1 Objets de base 11
1.2 Opérateur de Mahler 12
1.2.1 Comportement des polynômes 12
1.2.2 Polynômes cyclotomiques 13
1.2.3 Périodicité dans les corps finis 16
1.3 Opérateurs de section 19

2 Arithmétique euclidienne non commutative **21**
2.1 Forme normale 21
2.2 Division et pgcd 22
2.3 Ppcm 24
2.4 Factorisation 27
2.5 Interpolation 27

3 Équations de Mahler linéaires **29**
3.1 Propriétés de clôture. 30
3.2 Solutions formelles 33
3.2.1 Réduction au cas $c_0 \neq 0$ 33
3.2.2 Réduction à un système fini d'équations 37
3.3 Aspect qualitatif et analytique 45
3.4 Étude dans les séries de Laurent 48
3.5 Solutions rationnelles 49
3.6 Solutions produits 53
3.6.1 Produit sous forme normale 53
3.6.2 Solution sous forme de produit 56
3.6.3 La méthode de réduction de Kuczma 58
3.6.4 Produits évanescents 59

II Aspect automatique **63**

4 Séries B-régulières **67**
4.1 Définition 67
4.2 Représentations linéaires 68
4.3 Matrices de Hankel 76

4.4 Récurrences . . . 81
4.5 Propriétés de clôture . . . 86
4.6 Coefficients des séries B-régulières . . . 90
4.7 B-machines et séries B-automatiques . . . 96
4.8 Lemme de Fatou . . . 99

5 Récurrences mahlériennes 103
5.1 Equation minimale . . . 103
5.2 Opérateurs B-rationnels . . . 109
5.2.1 Algèbre des séries en z et M . . . 109
5.2.2 Opérateurs B-rationnels . . . 113
5.2.3 Ecriture fractionnaire des opérateurs B-rationnels . . . 117
5.3 Extension aux anneaux . . . 121

6 Critères de B-régularité 123
6.1 Critère facile . . . 125
6.2 Critère général . . . 128
6.3 Caractéristique non nulle . . . 130
6.3.1 Premier critère pour les corps finis . . . 132
6.3.2 Deuxième critère pour les corps finis . . . 132
6.3.3 Critère pour les quotients $\mathbb{Z}/(p^a)$ . . . 134
6.3.4 Critère pour un anneau de caractéristique $m \neq 0$ . . . 135
6.3.5 Application aux partitions B-aires . . . 136
6.4 Corps algébriquement clos . . . 138
6.5 Différents types de récurrence . . . 140

III Aspect asymptotique 145

7 Asymptotique des suites mahlériennes 149
7.1 Classification . . . 149
7.2 Séries B-régulières . . . 152
7.2.1 Abscisse de convergence absolue . . . 153
7.2.2 Demi-réseaux . . . 164
7.3 Cas interne . . . 166
7.4 Cas modulaire . . . 168
7.5 Cas externe . . . 170

8 Variations cyclotomiques 173
8.1 Synopsis de la preuve . . . 175
8.2 Etude locale . . . 177
8.2.1 Transformation de Mellin . . . 178
8.2.2 Singularités de Λ_ω^* . . . 180
8.2.3 Développement en série de $\Lambda_\omega(t)$ . . . 185
8.2.4 Développement en série de $F_\omega(t)$ . . . 189
8.3 Méthode de col . . . 194
8.4 Collecte . . . 199

Résumé

L'objet de cette thèse est l'étude d'une classe de séries entières solutions de certaines équations fonctionnelles, dites mahlériennes. Ces séries interviennent en combinatoire avec des problèmes de comptage de mots et en analyse d'algorithmes où elles sont liées aux récurrences *diviser pour régner*.

La résolution des équations mahlériennes est fondée sur les propriétés des fractions rationnelles vis à vis de l'opérateur fondamental, analogue de la dérivation pour les équations différentielles, et sur l'arithmétique des opérateurs sous-jacents à ces équations. Les méthodes décrites fournissent à la fois des procédés effectifs de calcul et des résultats qualitatifs sur les propriétés de clôture de cette classe et, dans le cas complexe, sur les propriétés analytiques des solutions.

Une sous-classe importante de séries mahlériennes est fournie par les séries B-régulières, généralisation des séries B-automatiques. Elles sont la traduction, *via* la numération en base B, des séries rationnelles en indéterminées non commutatives de la théorie des langages formels et héritent de leurs propriétés. On peut par exemple définir les notions de représentation linéaire, de rang et de matrice de Hankel. Sous certaines conditions simples, une série mahlérienne est B-régulière ; en particulier la plupart des récurrences *diviser pour régner* fournissent des séries B-régulières.

L'analyse asymptotique des coefficients des séries mahlériennes complexes s'appuie sur une classification qui met en valeur l'importance des séries B-régulières, sur des techniques d'algèbre linéaire et sur des méthodes de théorie analytique des nombres. Les résultats obtenus permettent de traiter les exemples rencontrés dans la pratique. Ils montrent pour les séries B-régulières un lien entre le comportement asymptotique des coefficients et le spectre des représentations linéaires et dans beaucoup de cas un phénomène de périodicité en échelle logarithmique.

Mots clés : algèbre d'operateurs lineaires, équation fonctionnelle de Mahler, theorie des langages, suite automatique, développement asymptotique, fonction génératrice, analyse d'algorithme.

Abstract

The purpose of this thesis is to study a class of power series, which we call Mahlerian, solutions to certain functional equations. These series arise in combinatorial theory, for problems involving counting words, and in the analysis of algorithms, where they are related to *divide and conquer* recurrences.

Methods of solution of Mahlerian equations are based on the properties of rational functions with respect to the fundamental operation, analogue of the derivative for differential equations, and on the arithmetic of operators implicit in these equations. The methods we describe furnish efficient procedures for calculation, qualitative results concerning the closure of this class, and, in the complex case, analytic properties of the solutions.

An important subclass of Mahlerian series is provided by B-regular series, a generalization of B-automatic series. They are the translation, via base B arithmetic, of rational series in non-commutative variables, inheriting their properties, familiar in the theory of formal languages. One can define, for example, notions of linear representation, of rank, and of Hankel matrix. Under certain simple conditions, a Mahlerian series is B-regular ; in particular most *divide and conquer* recurrences provide B-regular series.

The asymptotic analysis of coefficients of complex Mahlerian series relies on a classification which reveals the significance of B-regular series, on methods from linear algebra, and on methods from the analytic theory of numbers. The results here obtained permit us to handle a number of frequently encountered practical examples. They show, for B-regular series, a connection between the asymptotic behavior of coefficients and the spectra of linear representations. In many cases we exhibit a phenomenon of logarithmic periodicity.