Chapter 1

Etude algébrique

1.1 Introduction

Le calcul différentiel est un des sujets les plus classiques en mathématique et les mathématiciens se sont interessés à de nombreux aspects comme l'étude algébrique, l'étude analytique, l'étude des solutions, le comportement des coefficients d'une solution analytique, etc... L'étude algébrique des équations différentielles donne lieu à la définition d'un anneau différentiel: Un opérateur différentiel sur un anneau A est une application linéaire $d : A \to A$, vérifiant $d(xy) = (dx)y + xdy$, pour tout $x, y \in A$. Alors un anneau différentiel est un anneau muni d'un ensemble fini d'opérateurs différentiels, qui commutent deux à deux.

Dans ce premier chapitre nous nous proposons de généraliser l'étude algébrique des anneaux différentiels. Pour ceci on introduit des opérateurs similaires aux opérateurs différentiels: Un opérateur à différences est une application linéaire $\delta : A \in A$, vérifiant $\delta(xy) = \delta x \delta y$, pour tout $x, y \in A$. De plus on demande que $\delta x = 0 \Rightarrow x = 0$. Dit encore différemment, δ est un monomorphisme de l'anneau dans lui-même. L'exemple standard d'un tel opérateur est l'opérateur $\circ_g$ dans un anneau de fonctions, défini par $\circ_g : f \mapsto f \circ g$. En particulier, en algorithmique on rencontre souvent l'opérateur $\cdot \circ z^2$ sur des séries génératrices lorsqu'on étudie des algorithmes de dichotomie. Un anneau aux différences est défini de façon semblable aux anneaux différentiels.

Dans tout ce chapitre nous nous servirons librement des notions et résultats classiques d'algèbre et d'algèbre universel et le lecteur intéressé pourra se rapporter à une des oeuvres suivantes: [Lang 84], [Cohn 65a].

1.2 Définitions et exemples

Dans ce paragraphe nous définissons les différentes nouvelles structures algébriques utilisées dans la suite. Rappelons d'abord:

Définition 1. *Soit A un anneau. Un opérateur différentiel (resp. à différences) sur A est une application (resp. injection) linéaire d (resp. δ) : $A \to A$, telle que pour tout $x, y \in A$ on ait $d(xy) = (dx)y + xdy$ (resp. $\delta(xy) = \delta x \delta y$).*

Remarque. Un opérateur à différences est également appelé *opérateur de transformation*. Lorsqu'on laisse tomber la condition d'injectivité on parle d'un opérateur à différences *dégénéré*. Un opérateur à différences bijectif est dit *inversible*.

Les opérateurs différentiels forment une A-algèbre, si l'on prend le crochet de commutation ($[d, d'] = dd' - d'd$) comme multiplication. Les opérateurs à différences forment uniquement un monoïde multiplicatif avec la composition comme multiplication. On dira que deux opérateurs différentiels sont *compatibles* s'il commutent. On dira qu'un opérateur à différences δ est *compatible* avec un ensemble D d'opérateurs différentiels si pour tout $d \in D$ on peut écrire $d\delta = \sum_{d' \in D} \lambda_{d,d',\delta} \delta d'$, pour certains $\lambda_{d,d',\delta} \in A$. Une *constante* pour un opérateur différentiel d resp. un opérateur à différences δ est un $x \in A$ tel que $dx = 0$ resp. $\delta x = x$. Une constante pour un opérateur à différences s'appelle également *élément invariant*. Plus généralement un *élément périodique* vis à vis d'un opérateur à différences δ est un élément x, tel qu'il existe un $n \geq 1$, avec $\delta^n x = x$.

Exemple 1. Les dérivées partielles sont des opérateurs différentiels compatibles sur l'anneau des polynômes en n variables. Pour des polynômes $P_1, \cdots, P_n$, l'opérateur $\circ_{P_1,\cdots,P_n} : Q(X_1, \cdots, X_n) \mapsto Q(P_1(X_1, \cdots, X_n), \cdots, P_n(X_1, \cdots, X_n))$ est un opérateur à différences compatibles avec les dérivées partielles. Sur $\mathbb{Q}[X_1, \cdots, X_n]$ tout opérateur à différences compatible avec les dérivées partielles est d'ailleurs de cette forme.

Exemple 2. Chaque opérateur $\circ_f$, tel que $X | f(X)$ est un opérateur à différences sur $A[[X]]$.

Exemple 3. Soit M une variété différentiable. Un tenseur T de type (1,1) induit un opérateur à différences sur TM par $X \in TM \mapsto TX$, avec $(TX)_m = T_m X_m$.

Définition 2. *Un anneau différentiel à différences (que nous appellerons par la suite anneau diffdiff) est un anneau A, muni d'un ensemble fini D d'opérateurs différentiels et d'un ensemble Δ d'opérateurs à différences, qui sont tous compatibles.*

Ici la compatibilité veut bien sûr dire: les éléments de D sont deux à deux compatibles et chaque élément de Δ est compatible avec D. Lorsque $\Delta = \emptyset$, on dit que A est un *anneau différentiel* et lorsque $D = \emptyset$, on dit que A est un *anneau à différences*. Si D contient exactement un élément, alors l'anneau est dit *ordinaire*. Dans le cas où D contient plus d'un élément on dit que l'anneau est *partiel*.

On note par $A^c_{D',\Delta'}$ le sous anneau des éléments de A, constants pour chaque opérateur dans $D' \subseteq D$ ou $\Delta' \subseteq \Delta$. L'anneau $A^c = A^c_{D,\Delta}$ est le sous anneau des *constantes* de A. Remarquons que A^c et $A^c_{D',\emptyset}$ sont stables pour tout opérateur dans D ou Δ à cause de la compatibilité.

Fixons un anneau à différences A. Soit $(D \cup \Delta)^*$ le monoïde de composition engendré par $D \cup \Delta$. On appelle un *opérateur diffdiff* sur A toute combinaison linéaire d'éléments de $(D \cup \Delta)^*$ à coefficients dans A. Remarquons qu'un tel opérateur s'écrit canoniquement comme combinaison linéaire d'opérateurs difffiffs de la forme $\delta d_1^{k_1} \cdots d_n^{k_n}$, avec $\delta \in \Delta^*$ et $D = d_1, \cdots, d_n$. On note Θ l'ensemble de tels opérateurs diffdiffs.

Pour des ensembles D et Δ fixes, on peut former la catégorie $\mathbf{Anndd}_{D,\Delta}$ des anneaux à diffdiffs avec D resp. Δ comme ensembles d'opérateurs différentiels resp. à différences. Notons l'abus de notation: pour des anneaux A et B, un élément $d \in D$ ne désigne pas nécessairement le même opérateur. Cet abus ne devrait pas nous étonner: Le $+$ sur A n'est pas nécessairement le même que sur B. Dans des cas de doute on mettra l'anneau sous jacent en indice. Comme les axiomes des objets de la catégorie $\mathbf{Anndd}_{D,\Delta}$ sont tous des équations conditionnelles, cette catégorie est une variété au sens de l'algèbre universelle et donc stable par somme directe, produit direct, limites projectives, etc... (voir [Cohn 65a]). Remarquons qu'un morphisme doit également préserver les $\lambda_{d,d',\delta}$. Dans la section suivante on montre quelques résultats élémentaires sur les anneaux diffdiffs en nous inspirant de l'algèbre universelle.

On a également les notions de module diffdiff et algèbre diffdiff, soit module et algèbre diffdiff à gauche dans le cas où A est non commutatif. Un module diffdiff M est un module sur un anneau diffdiff A muni des mêmes opérateurs que A (c.à.d. pour tout $d \in D$ et $\delta \in \Delta$ on a le même opérateur sur M). De plus on demande que chaque opérateur soit linéaire et vérifie $d(ax) = (da)x + adx$, pour tout $a \in A$ et $x \in M$. Lorsque M est même une algèbre, on dit que c'est une algèbre diffdiff, si M est un anneau à diffdiff pour ses lois internes.

Définition 3. *Un anneau de composition est un anneau A muni d'une opération $(n+1)$-aire $\circ$, tel que pour tout $f, g, h_1, \cdots, h_n \in A$, on ait $(f+g) \circ (h_1, \cdots, h_n) = f \circ (h_1, \cdots, h_n) + g \circ (h_1, \cdots, h_n)$ et $(fg) \circ (h_1, \cdots, h_n) = f \circ (h_1, \cdots, h_n) g \circ (h_1, \cdots, h_n)$. De plus on demande que pour tout $f, g_1, \cdots, g_n, h_1, \cdots, h_n \in A$, on ait $f \circ (g_1, \cdots, g_n) \circ (h_1, \cdots, h_n) = f \circ (g_1 \circ (h_1, \cdots, h_n), \cdots, g_n \circ (h_1, \cdots, h_n))$. On appelle n la dimension de l'anneau de composition. Lorsqu'on a de plus un ensemble $D = \{d_1, \cdots, d_n\}$ de n opérateurs différentiels compatibles sur A, vérifiant $d_i(f \circ (g_1, \cdots, g_n)) = d_i g_1((d_1 f) \circ (g_1, \cdots, g_n)) + \cdots + d_i g_n((d_n f) \circ (g_1, \cdots, g_n))$, pour tout $1 \leq i \leq n$ et $f, g_1, \cdots, g_n \in A$, alors on dira que A est un anneau de composition différentiel.*

1.3 Propriétés élémentaires

Beaucoup de résultats classiques dans cette section sont des applications directes de l'algèbre universelle. Nous avons alors choisi d'abréger nos démonstrations et de nous servir des résultats et de la terminologie de l'algèbre universelle. Il nous semble qu'une présentation moderne du sujet nécessite la mise en place d'un formalisme pratique d'algèbre universelle. Sans doute, nous ferons ceci ultérieurement lors d'une étude plus profonde. Pour le moment nous nous contentons juste à titre de culture de présenter rapidement quelques résultats classiques.

Dans cette section nous supposons pour simplifier que les anneaux sont commutatifs. Pour qu'un idéal I soit compatible avec les opérateurs d'un anneau diffdiff A, il faut déja qu'il soit stable par ces opérateurs. Comme pour chaque opérateur à différences δ on a de plus $\delta x = 0 \Rightarrow x = 0$, pour tout $x \in A$, on doit également avoir $\delta x \in I \Rightarrow x \in I$. On appelle évidemment *idéal diffdiff* un tel idéal. Sinon, on note par $[P]$ l'idéal diffdiff engendré par une partie $P \subseteq A$. Les résultats classiques sur les structures quotientes s'appliquent sans problème:

Proposition 1. *Le noyau d'un morphisme d'anneaux diffdiffs est un idéal diffdiff et à un idéal diffdiff I de A, on peut canoniquement associer l'anneau diffdiff quotient A/I, muni de la projection canonique $\varphi : A \to A/I$, de noyau I.* ♡

L'anneau diffdiff libre sur A dans un ensemble d'indéterminés X est l'anneau de polynômes diffdiffs sur A, noté par $A\{X\}$, pour éviter de confondre avec $A[X]$ et $A(X)$. On peut trivialement généraliser les notions de degré, dépendance algébrique, extensions simples et finiment engendrées, application polynôme, etc. au cas diffdiff. Lorsque A est intègre, $A\{X\}$ l'est aussi. En effet, on vérifie aisément que comme anneau $A\{X\}$ est isomorphe à $A[\Theta X]$.

Comme les opérateurs à différences sont injectifs, on peut également se poser le problème de l'inversion des éléments par rapport à ces opérateurs. Nous avons la:

Proposition 2. *Soit x un élément d'un anneau diffdiff A et δ un opérateur à différences. Alors il existe une extension universelle A dans laquelle x admet un inverse par rapport à δ (c.à.d. tel qu'il existe un x' avec $\delta x' = x$).*

Démonstration. Une telle extension étant nécessairement isomorphe à $A' = A\{x'\}/[\delta x' - x]$, il suffit de vérifier que A' est effectivement une extension de A. Or considérons l'ensemble $\hat{\Theta}$ d'opérateurs $\theta \in \Theta$ qui s'écrivent $\theta = \hat{\delta} d_1^{k_1} \cdots d_n^{k_n}$, où $\hat{\delta}$ est un mot sur Δ, qui n'admet pas δ comme suffixe. On vérifie aisément que tout élément de $A\{x'\}$ se réduit canoniquement vers un élément de $A[\hat{\Theta}]$ modulo $[\delta x' - x]$. Il s'en suit que A' est isomorphe à $A[\hat{\Theta}]$ comme anneau et que c'est donc une extension de A comme anneau diffdiff. ♡

Remarque. Si l'on pose des contraintes algébriques sur les opérateurs de Δ (on pourrait par exemple exiger qu'ils commutent deux à deux), la proposition

précédente reste valable: Il suffit d'ajuster $\hat{\Theta}$ (dans l'exemple des opérateurs commutants, $\hat{\delta}$ serait un "mot ordonné" sur Δ (pour un certain ordre total sur Δ) ne contenant pas δ).

Corollaire. *Pour tout anneau diffdiff A, il existe une extension universelle de A, dans laquelle tout opérateur est inversible.*

Démonstration. Pour toute famille finie de couples $F = (x_i, \delta_i)_{i\in I}$, on a une extension universelle A_F dans laquelle tout élément x_i est inversible par rapport à δ_i. Alors la limite injective $\hat{A}$ des A_F pour l'ordre naturel est une extension universelle dans laquelle tout élément de A est inversible par rapport à n'importe quel opérateur à différences. La limite injective de $A, \hat{A}, \hat{\hat{A}}, \cdots$ vérifie clairement les hypothèses. ♡

Il est clair qu'il n'existe pas d'opérateurs intégraux commes inverses des opérateurs différentiels, à cause de la constante qui apparaît quand on intègre. En revanche de la même façon que tout à l'heure on démontre la:

Proposition 3. *Pour tout anneau diffdiff A, il existe une extension universelle de A, dans laquelle tout élément admet une primitive pour chaque opérateur différentiel.* ♡

On peut également se poser le problème de l'inversion des éléments d'un anneau diffdiff A. En particulier, lorsque A est intègre on peut construire le corps diffdiff de fractions. Dans ce cas on construit également le corps de fractions rationnelles diffdiffs $A< X >$ dans un ensemble d'indéterminés X. On a:

Proposition 4. *Soit x un élément d'un anneau diffdiff A, vérifiant $xy = 0 \Rightarrow y = 0$, pour tout $y \in A$. Alors il existe une extension universelle de A, dans laquelle x est inversible.*

Démonstration. Soit S le monoïde multiplicatif engendré par $\Delta^* x$. Chaque élément de S vérifie la même propriété que x. En effet, ceci est clair lorsque tous les opérateurs à différences sont inversibles: On a $\delta xy = 0 \Rightarrow \delta(x\delta^{-1}y) = 0 \Rightarrow x\delta^{-1}y = 0 \Rightarrow \delta^{-1}y = 0 \Rightarrow y = 0$, pour tout $y \in A$ et $\delta \in \Delta^*$. Comme on peut toujours plonger A dans un anneau diffdiff dans lequel tout opérateur à différences est inversible, le résultat est vrai en toute généralité.

Maintenant considérons l'anneau $A' = A/S$ et munissons cet anneau des opérateurs différentiels $d \in D$, par $d(x/s) = ((dx)s - xds)/s^2$ et des opérateurs à différences $\delta \in \Delta$, par $\delta(x/s) = \delta(x)/\delta(s)$. On vérifie aisément que ces opérateurs sont bien définis. Comme A' vérifie la propriété universelle en tant qu'anneau, il le vérifie en tant qu'anneau diffdiff. On remarque que A' est intègre lorsque A l'est. ♡

Remarque. La démonstration précédente peut se retrouver presque automatiquement. Du fait que dans l'extension demandée tout élément de S doit être inversible,

A' doit se plonger dedans. Réciproquement on voit facilement qu'il y a exactement une façon d'étendre les opérateurs sur A à A'.

Corollaire. *Pour tout anneau diffdiff intègre A, ses opérateurs différentiels et à différences peuvent être prolongés d'une unique façon à son corps de fractions.* ♡

En fait, dans les propositions 2,3,4, nous avons résolu les équations $\delta x = y$, $dx = y$ et $xy = 1$ dans une extension de A. On peut obtenir des résultats beaucoup plus généraux sur la résolution d'équations. Nous nous limitons au cas où $A = K$ est un corps.

Alors nous avons la:

Proposition 5. *Il existe une extension minimale $\hat{K}$ de K, telle que tout polynôme (resp. polynôme linéaire) diffdiff $P \in K\{X\} - K$ admet une racine dans $\hat{K}$.*

Démonstration. Précisons qu'un polynôme diffdiff linéaire est un polynôme qui est combinaison linéaire des $\theta(X)$, avec $\theta \in \Theta$. Nous démontrons le résultat pour des polynômes diffdiffs habituels, la démonstration étant analogue dans l'autre cas. Soit $P \in K\{X\} - K$ irréductible. Alors l'idéal I diffdiff engendré par P dans $K\{X\}$ est premier et ne contient pas 1 (comme on le laisse au lecteur le soin de le vérifier). Il s'en suit que $K_P = K/I$ est un corps diffdiff, dans lequel X est racine de P. De même, pour un nombre fini de polynômes irréductibles $P_1, \cdots, P_n$ deux à deux distincts, l'ensemble $K_{P_1,\cdots,P_n} = \{X_1, \cdots, X_n\}/(P_1(X_1), \cdots, P_n(X_n))$ est un corps diffdiff dans lequel $P_1, \cdots, P_n$ ont des solutions. Il suffit maintenant de prendre la limite directe $\hat{K}$ des $K_{P_1,\cdots,P_n}$. On le laisse au soin du lecteur de vérifier que $\hat{K}$ se plonge dans toute autre extension vérifiant la propriété énoncée. ♡

Remarque. On peut s'arranger pour que la condition de minimalité devienne une condition d'universalité. Dans la pratique cette condition présente cependant peu d'intérêt.

Malheureusement l'extension $\hat{K}$ n'a pas autant de propriétés que la clôture algébrique d'un corps. La véritable clôture algébrique diffdiff d'un corps diffdiff est par exemple la limite injective de $K, \hat{K}, \hat{\hat{K}}, \cdots$. Effectivement, il n'y a pas de raison qu'un polynôme diffdiff à valeurs dans $\hat{k}$ admette une racine dans $\hat{K}$. Néanmoins, on verra que l'on a des bonnes propriétés pour la clôture linéaire diffdiff de K, lorsque $D \cup \Delta$ ne contient qu'un élément.

Classiquement, on étudie beaucoup plus profondément les extensions des corps diffdiffs. Un cerain nombre de résultats de la géométrie algébrique et de la théorie de Galois admettent des analogues diffdiffs. Le lecteur interessé pourra se rapporter aux ouvrages [Ritt 32], [Cohn 65b], [Kol 73]. A partir de maintenant, nous nous concentrons surtout sur les équations diffdiffess linéaires et sur leurs aspects algorithmiques.

1.4 Equations diffdiffess linéaires

Dans cette section, les anneaux considérés ne sont pas nécessairement commutatifs et on suppose que les opérateurs à différences d'un anneau diffdiff commutent deux à deux et sont en nombre fini. Le lecteur pourra éventuellement vérifier que l'hypothèse qu'il n'y a qu'un nombre fini d'opérateurs à différences est convenable, mais pas toujours crucial pour la suite. Dans toute cette section, A et K désignent respectivement un tel anneau resp. corps diffdiff. De plus on suppose que K opère sur A comme anneau diffdiff. On note $\Omega' = D \cup \Delta = \{d_1, \cdots, d_{p'}, \delta_1, \cdots, \delta_{q'}\}$ et on suppose que $\Omega = \{d_1, \cdots, d_p, \delta_1, \cdots, \delta_q\}$ est un sous ensemble des opérateurs sur A et K. On note Θ l'ensemble d'opérateurs de la forme $\delta_1^{k_1} \cdots \delta_q^{k_q} d_1^{l_1} \cdots d_p^{l_p}$. Remarquons que tout opérateur diffdiff qui fait intervenir que des opérateurs de Ω s'écrit canoniquement comme combinaison linéaire d'opérateurs dans Θ_Ω.

Remarque. L'intérêt de prendre Ω pas nécessairement égal à Ω' deviendra clair dans la section suivante lorsqu'on montre des propriétés de clôture des suites mahlériennes.

On appelle une *équation diffdiffe linéaire* utilisant les opérateurs de Ω à coefficients dans K une équation du type:

$$\sum_{\theta \in \Theta} \alpha_\theta \, \theta x = 0, \text{ avec les } \alpha_\theta \in K.$$

On note $Lin(K) = Lin_\Omega(K)$ l'ensemble des solutions de ce genre d'équations dans A. Lorsque Ω ne contient qu'un opérateur ω, l'équation précédente s'écrit:

$$\sum_{k=0}^{n} \alpha_k \, \omega^k x = 0, \text{ avec } \alpha_0, \cdots, \alpha_n \in B \text{ et } \alpha_n \neq 0.$$

Dans cette section on donne des conditions pour que l'ensembles de solutions soit stable par addition, multiplication et des opérateurs différentiels ou diffdiffs.

Remarque. On peut étendre un peu la théorie qui va suivre au cas qu'on prend un anneau diffdiff intègre $B \subseteq K$ au lieu de K, avec la propriété qu'étant donné $\alpha_1, \cdots, \alpha_n \in K$, on peut trouver $\beta \in B$, tel que les $\beta\alpha_k$ sont tous dans A^*, pour $1 \leq k \leq n$. Effectivement, dans ce cas, une équation diffdiffe linéaire à coefficients dans K se transforme en une équation diffdiffe linéaire à coefficients dans B par multiplication par un scalaire.

L'ensemble $\mathcal{G} = K[d_1, \cdots, d_p, \delta_1, \cdots, \delta_q]$ d'opérateurs diffdiffs à coefficients dans K et n'utilisant que des opérateurs dans Ω, resp. Ω' est muni trivialement de structure d'anneau diffdiff non commutatif, où chaque opérateur $\theta \in \Theta$ coïncide avec la multiplication à gauche par θ. Pour un ensemble $X \subseteq A$ fixe, l'ensemble

$I(X) \subseteq \mathcal{G}$ des opérateurs diffdiffs annulant X forme un idéal diffdiff à gauche. De même, un idéal diffdiff à gauche $I \subseteq \mathcal{G}$ induit un ensemble de solutions $Z(I) \stackrel{\text{déf}}{=} \{x \in A | \theta x = 0, \text{ pour tout } \theta \in I\}$ dans A. C'est à ce moment que nous pouvons remarquer la ressemblance avec la géométrie algébrique. Nous allons pousser plus loin cette ressemblance. Un sous ensemble X de A est dit *algébrique*, si $X = Z(I(X))$. Les ensembles algébriques sont en bijection avec un certain sous ensemble de l'ensemble des idéaux diffdiffs à gauche de $\mathcal{G}$. Un idéal à gauche de la forme $I(X)$ s'appelle *idéal à gauche linéair parfait* par rapport à A.

Dans ce qui va suivre, nous allons utiliser quelques résultats du chapitre 2. On remarque que $\mathcal{G}$ peut être muni de la structure d'une algèbre de Gröbner (voir section 2.3). Pour $\leq$, on peut par exemple prendre l'ordre lexicographique. Le théorème 2.2 implique alors que tout idéal à gauche de $\mathcal{G}$ est finiment engendré. On en déduit que tout système d'équations diffdiffs linéaires est équivalent à un nombre fini d'équations diffdiffs linéaires. Lorsque $\mathcal{G}$ est algorithmique (voir section 2.4), on a de plus un algorithme pour savoir si une certaine équation est impliquée par un système d'équations donné. On peut sans doute également obtenir des résultats semblables au Nullstellensatz de Hilbert, pour les idéaux à gauche linéaires parfaits de $\mathcal{G}$, mais nous n'avons pas encore eu le temps de regarder ceci en détail. En revanche, présentons maintenant quelques résultats concernant les ensembles $Lin(K)$ et $SLin(K)$.

On remarque que la notion de polynôme de Hilbert se généralise sans problème au cas présent. Plus précisement, appellons $d = k_1 + \cdots + k_p + l_1 + \cdots + l_q$ le degré de l'opérateur ${\delta_1}^{l_1} \cdots {\delta_q}^{l_q} {d_1}^{k_1} \cdots {d_p}^{k_p}$. Notons Θ_n l'ensemble de ces opérateurs. Notons par $\mathcal{G}_n$ le sous espace vectoriel à gauche de $\mathcal{G}$ engendré par les opérateurs de degré inférieur ou égal à n. Pour un idéal à gauche I de $\mathcal{G}$ donné, l'application, qui à n associe la dimension de $\mathcal{G}_n/I$ (où l'on a noté la réstriction de I à $\mathcal{G}$ par I également) est un polynôme à partir d'un certain rang, qu'on appelle polynôme de Hilbert de I et que l'on note par H_I. Pour un $a \in A$, nous notons également $H_a = H_{I(a)}$. Le calcul des polynômes de Hilbert est facile lorsqu'on connaît une base standard de I.

Pour un élément a, on note par $deg(a)$ le degré de H_a et on définit également $\nu(a) = p+q-deg(a)$, qui représente le nombre d'équations "indépendantes" vérifiées par a. Par exemple, si $\mathcal{G}$ désigne l'algèbre de Gröbner de l'exemple 2.7, on a $\nu(\sin) = 1$ et $\nu(\wp) = 2$. Plus généralement, on a $a \in Lin(K) \equiv \nu(a) > 0$ et $\nu(a) = p + q$, pour $a \in K$. Enfin, on note $Lin_n K$ le sous ensemble de $Lin(K)$ des $a \in A$, avec $\nu(a) \geq n$. Le but principal de ce chapitre est le:

Théorème 1. *Si B' soit un corps, alors avec les notations précédentes, on a pour tout $a, b \in A$:*

(a) $\nu(a + b) \geq \min(\nu(a), \nu(b))$.
(b) $\nu(ab) \geq \nu(a) + \nu(b) - (p + q)$.
(c) $\nu(\omega a) \geq \nu(a)$, *pour tout* $\omega \in \Omega'$.
(d) $\nu(\alpha a) = \nu(a)$, *pour tout* $\alpha \in K^*$.

Démonstration. On notera par $\pi_{c,n}$ la projection canonique de $\mathcal{G}_n$ sur $\mathcal{G}_n/I(c)$, pour chaque $c \in A$. Considérons l'application

$$\begin{aligned} \sigma : \mathcal{G}_n/I(a+b) &\to (\mathcal{G}_n/I(a) \times \mathcal{G}_n/I(b))/J, \\ \pi_{a+b,n}(\theta) &\mapsto (\pi_{a,n}(\theta), \pi_{b,n}(\theta)). \end{aligned}$$

Ici J est le sous espace vectoriel à gauche engendré par les $(\pi_{a,n}(\theta), \pi_{b,n}(\theta))$, où $\theta(a+b) = 0$. Il s'en suit que σ est bien définie. De plus elle est clairment injective, d'où à partir d'un certain rang $H_{a+b}(n) = \dim \mathcal{G}_n/I(a+b) \leq \dim(\mathcal{G}_n/I(a) \times \mathcal{G}_n/I(b))/J \leq \dim \mathcal{G}_n/I(a) \times \mathcal{G}_n/I(b) = H_a(n) + H_b(n)$. Il s'en suit que $deg(a+b) \leq deg(a) + deg(b)$, d'où (a).

Considérons maintenant l'application

$$\begin{aligned} \rho : \mathcal{G}_n/I(ab) &\to (\mathcal{G}_n/I(a) \otimes \mathcal{G}_n/I(b))/J, \\ \pi_{ab,n}(\theta) &\mapsto \sum_{\theta_1,\theta_2 \in \Theta_n} \alpha_{\theta_1,\theta_2} \pi_{a,n}(\theta_1) \otimes \pi_{b,n}(\theta_2), \text{ où} \\ \theta(ab) &= \sum_{\theta_1,\theta_2 \in \Theta_n} \alpha_{\theta_1,\theta_2} \theta_1(a)\theta_2(b). \end{aligned}$$

Ici J est défini de façon analogue au cas précédant et le même raisonnement que tout à l'heure donne $H_{ab}(n) \leq H_a(n)H_b(n)$, à partir d'un certain rang, d'où $deg(ab) \leq deg(a) + deg(b)$ et d'où (b).

Ensuite, considérons l'application

$$\begin{aligned} \mu_\omega : \mathcal{G}_n/I(\omega a) &\to (\mathcal{G}_n/I(a))^2/J, \\ \pi_{\omega a,n}(\theta) &\mapsto (\pi_{a,n}(\theta_1), \pi_{a,n}(\theta_2)), \text{ avec} \\ \theta\omega(a) &= \omega\theta_1(a) + \theta_2(a). \end{aligned}$$

Ici J est encore défini de façon analogue aux cas précédants. Il est clair que cette application est bien définie et injective. Il s'en suit que $H_{\omega a}(n) \leq 2H_a$ à partir d'un certain rang, d'où (c).

Considérons enfin l'application

$$\begin{aligned} \mu_c : \mathcal{G}_n/I(\alpha a) &\to \mathcal{G}_n/I(a), \\ \pi_{\alpha a,n}(\theta) &\mapsto \pi_{a,n+1}(\theta a). \end{aligned}$$

Il est clair que cette application est bien définie et bijective. Il s'en suit que $H_{\alpha a}(n) = H_a(n)$ à partir d'un certain rang, d'où (d). ♡

Remarque. Si $\mathcal{G}$ est une algèbre de Gröbner algorithmique, il est possible de donner des algorithmes de calcul des équations vérifiées par $a+b$, ab, ωa, repectivement αa. Remarquons que cet algorithme ne donne pas nécessairement des familles

génératrices de $I(a+b)$,$I(ab)$, etc. Il suffit par exemple de considérer $a+b$, où $b=-a$. Nous expliciterons ces algorithmes ultérieurement.

Corollaire 1. *Pour tout $1 \leq n \leq p+q$, $Lin_n(K)$ est un K-espace vectoriel diffdiff à gauche. De plus, $Lin_{p+q}(K)$ est même un sous algèbre diffdiff à gauche de A.* ♡

Corollaire 2. *Si $p+q=1$, alors $Lin(K)$ est un sous anneau diffdiff de A.* ♡

Remarque. Tenant compte du deuxième corollaire, le fait que $Lin_{p+q}(K)$ forme un anneau ne devrait pas nous étonner. Par exemple, si A est un corps, on vérifie aisément qu'un élément de A appartient à $Lin_{p+q}(K)$ ssi elle vérifie une équation diffdiffe linéaire pour chaque opérateur $\omega \in \Omega$.

Exemple 4. Les fonctions holonomes $\mathcal{H}$ forment un sous anneau de l'anneau des fonctions holomorphes définies sur un ouvert de $\mathbb{C}$. Effectivement, $\mathcal{G} = \mathbb{C}(z)[D]$ est bien une algèbre de Gröbner. On a $\mathcal{H} = Lin(\mathbb{C}(z))$. On a même une généralisation des fonctions holonomes (voir [Car 91]), pour des fonctions en n variables. Cet ensemble de fonctions holonomes généralisées coïncide avec $\mathcal{H}_n = Lin_n(\mathbb{C}(z_1, \cdots, z_n))$, où on peut prendre pour $A = \hat{A}$ l'ensemble des fonctions holomorphes sur un ouvert de $\mathbb{C}^n$, divers espaces de distributions, etc.

Exemple 5. Soit A l'ensemble des fonctions méromorphes sur $\mathbb{C}$. Reprenons l'exemple 2.7, avec cette fois ci $K = \mathbb{C}(z)$ et $\mathcal{G} = K[\delta, \delta']$. Alors $Lin_2(K)$ est un sous anneau diffdiff de A et on appelle ses éléments des *fonctions semiélliptiques* (par rapport à ζ et ζ' et $\leq$). De plus $Lin_2(K)$ est stable par dérivation, dont on s'apperçoit en considérant $\mathcal{G}' = K[\delta, \delta', D]$. Nous avons l'impression que toute fonction sémiélliptique s'écrit comme fraction rationnelle en $\exp(cz), \wp(z), \wp'(z)$ et z, mais pour le moment, nous n'avons pas encore eu le temps de le vérifier. Il sera également intéressant de voir si on peut couvrir des espaces encore plus grands de fonctions pseudo-élliptiques en prenant pour K un surcorps diffdiff de $\mathbb{C}(z)$.

Remarque. La théorie présentée dans cette section s'étend assez facilement au cas des systèmes d'équations diffdiffes linéaires à plusieurs inconnus. Effectivement, dans ce cas on fait opérer un K-espace vectoriel diffdiff à gauche sur un A-module à gauche par produit scalair. Par exemple, pour un n-tuple $(x_1, \cdots, x_n) \in A^2$ fixe, $Z(x_1, \cdots, x_n)$ est défini comme l'ensemble de couples d'opérateurs $(\theta_1, \cdots, \theta_n)$ avec $\theta x_1 + \cdots + \theta x_n = 0$. Le théorème 2.5 ensemble avec le lemme 2.1(c) montrent que l'étude précédente s'étend à ce cas. On peut notamment calculer le module d'opérateurs annulant x_1, lorsque l'ensemble des x_i vérifie un système d'équations

linéaires.

Remarque. On peut également étudier des équations diffdiffes linéaires à second membre. La théorie précédente s'applique à quelques petites modifications près. Ultérieurement, nous ferons une approche unifié, où on considera des systèmes d'équations diffdiffes linéaires à plusieurs inconnus et à second membre.

1.5 Suites mahlériennes et régulières

Considérons d'abord l'anneau $\mathcal{P} = A[z_1, \cdots, z_p]$ de polynômes en p variables sur un anneau A non nécessairement commutatif. Ici, on suppose tout de même que les z_k sont dans le centre de $\mathcal{P}$; C.à.d. que bien que l'anneau A n'est pas nécessairement commutatif, on rajoute des indéterminés commutatifs. Comme d'habitude, un polynôme P s'écrit alors:

$$P = \sum_{k_1,\cdots,k_p \in \mathbb{N}} a_{k_1,\cdots,k_p} z^{k_1} \cdots z^{k_p}, \tag{1.1}$$

où les $a_{k_1,\cdots,k_p}$ sont dans A, et la somme ne comporte qu'un nombre fini de termes non nuls. On peut classifier les opérateurs différentiels et à différences sur $\mathcal{P}$ qui envoient A dans A. Effectivement, le lecteur pourra vérifier qu'un tel opérateur est entièrement déterminé par son action sur A et les images de $z_1, \cdots, z_p$. En particulier, si A est laissé invariant, tout opérateur différentiel est combinaison linéaire des opérateurs de dérivées partielles $D_1, \cdots, D_p$ définis par:

$$D_i \sum_{k_1,\cdots,k_p \in \mathbb{N}} a_{k_1,\cdots,k_p} z^{k_1} \cdots z^{k_p} = \sum_{k_1,\cdots,k_p \in \mathbb{N}} k_i a_{k_1,\cdots,k_p} z^{k_1} \cdots z^{k_p}. \tag{1.2}$$

De même un tel opérateur à différences est de la forme $\circ_{g_1,\cdots,g_p}$.

Par analogie avec l'anneau de polynômes en p variables, on définit l'anneau $\mathcal{F} = A[[z_1, \cdots, z_p]]$ de séries formelles en n variables sur A en convenant qu'un élément de $\mathcal{F}$ se définit également par l'équation (1), mais où la somme peut être infinie. Il n'y a pas de classification simple des opérateurs différentiels et à différences sur $\mathcal{F}$, qui envoient A dans A. Néanmoins, nous nous intéressons surtout aux opérateurs qui se définissent par analogie avec le cas précédent. On définit donc les opérateurs dérivées partielles $D_1, \cdots, D_p$ comme dans (2) et nous considérons des opérateurs à différences de la forme $\circ_{g_1,\cdots,g_p}$. Pour qu'un tel opérateur à différences soit bien défini, nous rajoutons la condition que $z_i | g_i$, pour tout $1 \leq i \leq p$. En particulier, nous définissons les opérateurs de Mahler $M_{k_1,\cdots,k_p} = \circ_{z^{k_1},\cdots,z^{k_p}}$. On remarque que les opérateurs de Mahler commutent deux à deux.

On appelle *équation de Mahler*, toute équation linéaire à coefficients dans $\mathcal{P}$ en $M_{k_1,\cdots,k_p}$. Si $p = 1$, on parle d'équation de Mahler classique. On appelle *équation de Mahler généralisé* toute équation linéaire à coefficients dans $\mathcal{P}$ en un nombre

fini d'opérateurs de Mahler. On appelle *suite mahlérienne (classique, généralisée)*, toute suite $\{f_{k_1,\cdots,k_p}\}_{k_1,\cdots,k_p\in N}$ à valeurs dans A, telle que $f(z_1,\cdots,z_p)=\sum_{k_1,\cdots,k_p\in\mathbb{N}} f_{k_1,\cdots,k_p}z_1^{k_1}\cdots z_p^{k_p}$ vérifie une équation de Mahler (classique,généralisée) non triviale. Dans ce cas on appelle $f(z_1,\cdots,z_p)$ une *série mahlérienne (classique, généralisée)*. En cas d'ambiguïté, on parlera de suites et séries $(k_1,\cdots,k_p)$- mahlériennes.

Supposons maintenant que A est un anneau noethérien commutatif et intègre et soit K son corps de fractions. De la section précedente il suit alors que les séries mahlériennes forment un sous anneau de $\mathcal{F}$ stable par les D_k. De même, les séries mahlériennes généralisées forment un $\mathcal{P}$-module diffdiff. Comme dans le cas des fonctions holonomes, on peut généraliser les notions de suites et de séries mahlériennes pour plusieurs opérateurs de Mahler. Par analogie, nous disons alors qu'une série formelle est une *série mahlérienne*, si elle vérifie une équation de Mahler pour chacun des n opérateurs. Les *suites mahlériennes* se définissent comme on le pense. Si $n=1$ on parlera des séries mahlériennes ordinaires, tandis que pour $n>1$ on parlera de séries mahlériennes partielles. Il est clair que pour cette notion généralisée de séries mahlériennes, l'ensemble de séries mahlériennes est également un sous anneau de $\mathcal{F}$, stable par les dérivées partielles.

Lorsqu'on fait de l'asymptotique, on voudrait exprimer le comportement des suites mahlériennes en fonction de fonctions qui se prêtent à des calculs rapides. Certaines suites mahlériennes ont déjà cette propriété naturellement. Considérons par exemple la suite $\sigma_k(n)$ "somme des chiffres en base k". Cette suite est une suite k-mahlérienne et des grands termes sont facilement calculables, lorsqu'on présente n comme écrit en base k. Avant d'introduire correctement les séries régulières dans un cadre plus général, introduisons quelques nouveaux concepts.

D'abord, soit A un anneau commutatif et Σ un alphabet fini. On note par $A[\Sigma^*]$, respectivement $A[[\Sigma^*]]$, les anneaux de polynômes et séries formelles sur A en des variables non commutatives de Σ. On note par $A^{rat}[[\Sigma^*]]$ l'ensemble des *séries rationnelles* de $A[[\Sigma]]$, c.à.d. la clôture de $A[\Sigma^*]$ dans $A[[\Sigma^*]]$, pour l'addition, produit de Cauchy et produit externe. D'après le théorème de Kleene-Schützenberger, une série f est rationnelle ssi'il existe un morphisme de monoïdes φ de Σ^* dans un ensemble de matrices carrées $\mathcal{M}_n(A)$ sur A et un vecteur ligne λ resp. colonne μ, tel que $f=\sum_{W\in\Sigma^*}\lambda\varphi(W)\mu W$. Pour une démonstration et plus de détails sur les séries rationnelles, le lecteur pourra se reporter à [BeReu 84] ou [Saso 78].

Ensuite, généralisations la notion d'écriture en base k. Etant donné deux couples $(n_1,\cdots,n_p)$ et $(k_1,\cdots,k_p)$, on appelle *représentation en base* $(k_1,\cdots,k_p)$ de $(n_1,\cdots,n_p)$ le mot $\varepsilon_r\cdots\varepsilon_0$ de n-tuplets, c.à.d. $\varepsilon_i=(\varepsilon_{i,1},\cdots,\varepsilon_{i,n})$, tel que chaque mot $\varepsilon_{r,i}\cdots\varepsilon_{0,i}$ est la représentation en base k_i de n_i, avec potentiellement des zéros devant, mais tel que $\varepsilon_i\neq(0,\cdots,0)$. Nous notons cette représentation par $[n_1,\cdots,n_p]_{k_1,\cdots,k_p}$. Réciproquement, nous notons $(n_1,\cdots,n_p)=(\varepsilon_r\cdots\varepsilon_0)_{k_1,\cdots,k_p}$. On vérifie aisément que cette représentation est unique. Dans la suite, notons par $\Sigma=\Sigma_{k_1,\cdots,k_p}$ l'alphabet fini $\{0,\cdots,n_1-1\}\times\cdots\times\{0,\cdots,n_p-1\}$.

On peut maintenant introduire les séries régulières. Considérons la bijection

$$\begin{aligned} \varphi : A[[\Sigma^*]] &\to \mathcal{F} = A[[z_1, \cdots, z_p]], \\ \sum_{W\in\Sigma^*} a_W W &\mapsto \sum_{n_1,\cdots,n_p\in\mathbb{N}} a_{[n_1,\cdots,n_p]_{k_1,\cdots,k_n}} z_1^{n_1}\cdots z_p^{n_p}. \end{aligned}$$

Une *série régulière* est alors une série formelle appartenant à l'image de $A^{rat}[[\Sigma^*]]$ par φ. En cas d'ambiguïté, nous parlerons de série $(k_1, \cdots, k_p)$-régulière. Introduisons également les *opérateurs de* $(k_1, \cdots, k_p)$*-section* $S_{r_1,\cdots,r_p}$, avec $(r_1, \cdots, r_p) \in \Sigma$, par

$$S_{r_1,\cdots,r_p} f = \sum_{n_1,\cdots,n_p\in\mathbb{N}} f_{k_1 n_1 + r_1,\cdots,k_p n_p + r_p} z_1^{n_1}\cdots z_p^{n_p}.$$

Les résultats classiques sur les séries régulières se généralisent alors sans problème:

Théorème 2. *Soit $f \in \mathcal{F}$. Les propositions suivantes sont alors équivalentes:*

(a) f est une série $(k_1, \cdots k_p)$-régulière.

(b) Il existe des matrices carrées $\{M_\varepsilon\}_{\varepsilon\in\Sigma^*}$ dans $\mathcal{M}_n(A)$, un vecteur ligne λ et un vecteur colonne μ, tel que pour tout $(n_1, \cdots, n_p) = (\varepsilon_r \cdots \varepsilon_0)_{k_1,\cdots,k_p}$, on a $f_{n_1,\cdots,n_p} = \lambda M_{\varepsilon_r} \cdots M_{\varepsilon_0} \mu$.

(c) Il existe un sous module de $\mathcal{F}$ de type fini, stable par les opérateurs de $(k_1, \cdots, k_p)$-section et contenant f.

Démonstration. L'équivalence (1)⇔(2) est une traduction directe du théorème de Kleene-Schützenberger. L'équivalence (1)⇔(3) se démontre de façon analogue au résultat classique, pour $r = 1$ (voir par exemple [Dum 93], page 72). ♡

Remarque. Il est clair qu'à cause de la première caractérisation des séries régulières (théorème 2(b)), il existe un algorithme rapide (en $\ln n_1 \cdots n_p$) de calcul des termes d'une suite régulière. Remarquons qu'il est possible de donner une définition plus large de séries régulières, qui permet également de faire des calculs rapides (cette fois ci en $\ln n_1 \cdots \ln n_p$). Nous étudierons cette possibilité ultérieurement.

Théorème 3. *L'ensemble de séries $(k_1, \cdots, k_p)$-régulières forment un sous anneau de $\mathcal{F}$, stable par produit de Hadamard.*

Démonstration. Que l'ensemble des séries régulières soit stable par addition et produit de Hadamard découle directement du résultat semblable pour les séries rationnelles. En ce qui concerne le produit habituel, la démonstration est analogue au cas classique (voir [AllSh 92], page 173 ou [Dum 93], page 91), avec le petit changement que le rang $\operatorname{rg} fg$ de fg (voir encore [Dum 93]) est au plus $2^p \operatorname{rg} f \operatorname{rg} g$ au lieu de $2 \operatorname{rg} f \operatorname{rg} g$. ♡

Il est naturel d'étudier quand une série régulière est mahlérienne et vice versa. Supposons alors que A est un anneau commutatif noethérien intègre. On appelle une équation de Mahler spéciale une équation du type:

$$f = P_1 M f + \cdots + P_m M^m f, \tag{1.3}$$

où les P_i sont dans $\mathcal{P}$ et où $M = M_{k_1,\cdots,k_p}$.

Nous n'avons pas démontré en toute rigueur le théorème qui va suivre, mais nous espérons bientôt donner une démonstration complètement satisfaisante.

Théorème 4.

(a) Toute série régulière est mahlérienne.

(b) Une série mahlérienne f est régulière, si et seulement si Pf vérifie une équation de Mahler spéciale, pour un certain polynôme P.

Démonstration. Soit f une série régulière. D'après le théorème 2(b), on a ce qu'on appelle une *représentation linéaire* pour f. On en tire un système d'équations linéaires dont on tire par élimination une équation de Mahler vérifiée par f. On n'a pas eu le temps de montrer qu'on obtient ainsi une équation de Mahler non triviale, ce qui démontre (a). Néanmoins d'après la remarque après l'exemple 5d, il est possible de trouver une famille génératrice de l'idéal à gauche d'opérateurs annulant f par algorithme en utilisant la théorie des bases standard du chapitre 2.

Supposons maintenant que f vérifie l'équation (3). Soit d le maximum parmi les degrés de $P_1, \cdots, P_m$. Considérons maintenant les vecteurs colonnes $\{v_{n_1,\cdots,n_p}\}_{n_1,\cdots,n_p \in \mathbb{N}}$, composés des éléménts $f_{n_1+s_1,\cdots,n_p+s_p}$, avec les s_i compris entre 0 et d. On vérifie que $v_{n_1 k_1+r_1,\cdots,n_p k_p+r_p}$, avec $(r_1,\cdots,r_p) \in \Sigma$ est exprimable comme la multiplication d'une matrice qui ne dépend que de $(r_1,\cdots,r_p)$ avec $v_{n_1,\cdots,n_p}$. Comme la série f est un des composants de la "série" v, il s'en suit que f est régulière. Il en est de même pour le produit de f par un polynôme.

Réciproquement, supposons que f est mahlérienne et régulière. On a donc une équation mahlérienne pour f:

$$P_0 f + P_1 M f + \cdots + P_m M^m f = 0.$$

On utilise le même astuce que pour transformer une équation algébrique à coefficients dans A en une équation intégrale (voir par exemple [Lang 84], page 357). Prenons un polynôme P, tel que $P_0 P | P_i M^i i$, pour chaque $1 \leq i \leq m$. Nous ne savons pas démontrer rigoureusement que ceci est possible généralement, bien que ceci est vrai pour un corps algébriquement clos, si $p = 1$ et pour le corps fini $\mathbb{F}_q$, si $M = M_{q,\cdots,q}$. Effectivement, si $A = \mathbb{F}_q$, il suffit de prendre $P = P_0$, car dans ce cas $MP = P^q$. Alors considérons $g = Pf$. On vérifie aisément que g vérifie une

équation mahlérienne spéciale. ♡

Remarque. Il est possible de donner une démonstration algébrique du fait que les séries régulières forment un anneau, en démontrant que les solutions d'équations à différences ordinaires spéciales forment un anneau. Nous n'avons pas encore eu le temps de vérifier ceci en détail.

La deuxième partie du théorème admet deux corollaires dans le cas où $A = \mathbb{F}_q$ et $M = M_{q,\cdots,q}$ (qu'on a démontré correctement ici), qui généralisent les théorèmes de Christol et al. (voir [Chr+ 80]) et Furstenberg (voir [Fur 67]).

Corollaire 1. *Si $\mathcal{F} = \mathbb{F}_q[[z_1, \cdots z_p]]$, alors l'ensemble des séries $(q, \cdots, q)$-régulières coïncide avec l'ensemble des séries formelles algébriques.* ♡

Corollaire 2. *L'ensemble des séries formelles algébriques de $\mathbb{F}_q[[z_1, \cdots, z_p]]$ est stable par produit de Hadamard.* ♡

Dans le cas des corps finis, en utilisant des bases standard (voir le deuxième chapitre), on a réussi également à obtenir des résultats semblables pour des équations diffdiffes algébriques, comportant la dérivation. Nous énoncons juste notre résultat, dont la démonstration n'est pas encore complètemant au point et que nous espérons généraliser au cas $p > 1$:

Théorème 5. *Supposons qu'une équation différentielle algébrique n'admet qu'un nombre fini de solutions dans $\mathbb{F}_q[[z]]$, alors toutes les solutions sont des séries régulières.* ♡

1.6 Références

[AllSh 92] J.P. Allouche, J. Shallit.
The ring of k-regular sequences
Theoretical Computer Science 98, 163-197.

[BeReu 84] J. Berstel, C. Reutenauer.
Les séries rationnelles et leurs langages.
Masson, Paris.

[Chr+ 80] G. Christol, T. Kamae, M. Mendès France, G. Rauzy.
Suites algébriques, automates et substitutions.
Bulletin de la Société Mathématique de France 108, 401-419

[**Cohn 65a**] P.M. Cohn.
Universal algebra.
Harper Internatial student reprint.

[**Cohn 65b**] R.M. Cohn.
Difference algebra.
Interscience publications, Tracts in Mathematics, No. 17.

[**Dum 93**] P. Dumas.
Récurrences Mahlériennes, suites automatiques, études asymptotiques.
Thèse, Université de Bordeau.

[**Erd+ 87**] P. Erdös, A. Hildebrand, A. Odlyzko, P. Pudaite, B. Reznick.
The asymptotic behaviour of a family of sequences.
Pasific Journal of Mathematics, Vol. 126, No. 2, 227-241.

[**Fur 67**] H. Furstenberg.
Algebraic functions over finite fields.
Journal of algebra 7, 271-277.

[**Her 35**] F. Herzog.
Systems of algebraic mixed difference equations.
Transactions of the American Mathematical Society 37, 286-300.

[**Kol 73**] E.R. Kolchin.
Differential algebra and algebraic groups.
Academic press, Pure and Applied Mathematics, Vol. 54.

[**Kre 64**] H.F. Kreimer.
The foundations for an extension of differential algebra.
Transactions of the American Mathematical Society 111, 482-492.

[**Lang 84**] S. Lang
Algebra.
Addison Wesley.

[**Odl 82**] A.M. Odlyzko.
Periodic oscillations of coefficients of power series that satisfy functional equations.
Advances in Mathematics 44, 180-205.

[**Pol —**] G. Pólya
Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen
—

[**Ritt 32**] J.F. Ritt.
Differential equations from the algebraic standpoint.
American Mathematical Society Colloquium Publications, Vol. 14.

[**SaSo 78**] A. Salomaa, M. Soittola.
Automata-theoretic aspects of formal power series.
Springer, Berlin.

Chapter 2

Sur la théorie de la division

2.1 Introduction

Dans ce chapitre on présentera la théorie de la division de façon très générale. Notre théorie généralise à la fois la division euclidienne, la division de Hironaka (utilisée dans la théorie des bases de Gröbner) mais également la division dans des anneaux de germes d'opérateurs différentiels par exemple. Notre cadre permet également d'étendre la théorie de la division à des anneaux d'opérateurs diffdiffs et bien d'autres. Les sections 2.2 jusqu'à 2.4 présentent la théorie abstraite sous-jacente. Un lecteur non familier avec la théorie des bases standard pourra lire simultanément la section 2.5, dans laquelle sont présentés de nombreux exemples.

Comme applications de la théorie de la division, il y a l'étude des idéaux dans un anneau donné et notamment la théorie des bases standard. Cette théorie permet a son tour d'étudier les équations polynômiales, diffdiffs et d'étudier le comportement des solutions de ce genre d'équations autour de leurs singularités.

Pour garder le maximum de généralité, les anneaux considérés dans ce chapitre ne sont pas nécessairement commutatifs. On dira qu'un tel anneau est noethérien, si les idéaux à gauche vérifient la propriété de chaîne ascendante. Par une algèbre à gauche sur un anneau non commutatif A, on entend un suranneau de A. On ne considera que des algèbres à gauche libres, c.à.d. admettant une base en tant que A-module à gauche.

2.2 Algèbres de division

Diviser un élément a d'un anneau A par un élément b correspond à trouver des $q, r \in A$ tel que $a = qb + r$. Plus généralement, on divise a par rapport à un idéal à gauche I de A. Dans ce cas il faut trouver $x \in I$ et $r \in A$, tel que $a = x + r$. Sauf dans le cas $I = \{0\}$, ce problème admet plusieurs solutions. Dans la théorie de la division, idéalement, on veut qu'il y ait une unique solution pour ce problème,

lorsqu'on restreint r à être d'une certaine forme.

On appelle *division* sur un anneau A une application $\div$, qui à chaque couple (a, I) d'un élément et un idéal à gauche de A associe un élément $a \div I$, congru à a modulo I et et qui ne dépend que de la classe de a modulo I. De plus, on demande que $a \div I$ soit nul, si $a \in I$. On appelle l'image R_I de $\cdot \div I$ *l'ensemble des restes modulo* I . On a $0 \in R_I$, pour tout idéal à gauche I. En fait la famille des R_I détermine la division. Le but de notre affaire est de trouver des R_I "simples" et de rendre la division effectuable par algorithme.

On dira qu'une division est *algorithmique*, lorsque la division par tout idéal à gauche $I = (b_1, \cdots, b_n)$ finiment engendré est effectuable par algorithme et si on fournit également les coefficients c_i tel que $a = c_1 b_1 + \cdots + c_n b_n + a \div I$. On appelle *anneau de division (algorithmique)* un anneau muni d'une division (algorithmique). Si A est un anneau de division, dans lequel pour tout couple d'idéaux à gauche finiment engendrés de A on sait trouver des générateurs de leur intersection par algorithme, on dit que A est *anneau de division augmenté*. Comme de façon algorithmique, des idéaux à gauche sont toujours présentés par un ensemble de générateurs, il sera plus commode de dire qu'on sait calculer des intersections d'idéaux à gauche.

Plus tard nous aurons également besoin de la notion de *A-module de division à gauche*. La définition de tels modules est analogue à celle des anneaux de division en remplacant les idéaux à gauche par des sous modules à gauche. On a également les notions de A-module de division algorithmique à gauche, A-module de réduction à gauche, etc. On dira qu'une division sur un A-module à gauche libre est compatible avec la division sur A, si pour tout sous-module de la forme $\{0\} \cdots \{0\} \times A \times \{0\} \cdots \{0\}$, la division correspond à celle de A.

Les anneaux de division algorithmiques augmentés admettent une caractérisation utile, que nous n'utiliserons pas avant la section 2.4:

Lemme 1. *Soit A un anneau de division algorithmique. Alors les conditions suivantes sont équivalentes:*

(a) A est un anneau de division algorithmique augmenté.
(b) Pour toute forme linéaire $\varphi : A^n \to A; (a_1, \cdots, a_n) \mapsto a_1 b_1 + \cdots + a_n b_n$, on sait construire par algorithme une famille génératrice $\{(a_{l,1}, \cdots, a_{l,n})\}_{l \in L}$ du noyau de φ.
(c) Tout A-module à gauche $\mathcal{M}$ de type fini libre peut être muni d'une division algorithmique augmentée, compatible avec la division sur A.

Démonstration. L'implications (b) $\Rightarrow$ (a) est facile et laissée au lecteur. L'implication (c) $\Rightarrow$ (a) est triviale.

Montrons (a) $\Rightarrow$ (b) par récurrence sur n. Pour $n = 1$ la proposition est triviale. Supposons qu'on l'a vérifiée à l'ordre $n - 1$. Calculons des générateurs $c_1, \cdots, c_m$

de $(b_1, \cdots, b_{n-1}) \cap (b_n)$. Puis calculons des $a_{l,k}$, avec $c_l = a_{l,1}b_1 + \cdots + a_{l,n-1}b_{n-1}$ et $-c_l = a_{l,n}b_n$. Les vecteurs $(\{a_{l,k}\}_{1\leq k\leq n})$ sont bien dans $\ker\varphi$. Complétons cette famille de vecteurs par les générateurs de $\ker\varphi'$, avec $\varphi' : (a_1, \cdots, a_n) \mapsto (a_1b_1 + \cdots + a_{n-1}b_{n-1}, a_n)$. Nous affirmons que cette nouvelle famille de vecteurs $(\{a_{l,k}\}_{1\leq k\leq n})$, avec $1 \leq l \leq m'$ forme une base de $\ker\varphi$. Effectivement, si $a_1b_1 + \cdots + a_nb_n = 0$, on a $a_nb_n = d_1c_1 + \cdots + d_mc_m$, pour certains d_i. Alors le n-tuplet $(a'_1, \cdots, a'_n) = (a_1, \cdots, a_n) + \sum_{l=1}^{m} d_l(a_{l,1}, \cdots, a_{l,n})$ appartient à $\ker\varphi'$, car $a'_n = 0$. D'où le résultat par récurrence.

Montrons (a) $\Rightarrow$ (c). Nous le montrons par récurrence sur le nombre n d'éléments dans la base de $\mathcal{M}$. Pour $n = 1$ c'est trivial. Supposons (c) vrai à l'ordre $n-1$.

Construisons d'abord une division algorithmique sur $\mathcal{M}$. Prenons alors un sous module $\mathcal{M}'$ à gauche de $\mathcal{M}$ engendré par $b_1, \cdots, b_m$ et un élément $c \in \mathcal{M}$. Alors nous divisons d'abord a_1 par l'idéal à gauche de A engendré par $b_{1,1}, \cdots, b_{m,1}$. On peut alors trouver un c', avec $c' - c \in \mathcal{M}'$, dont le premier coefficient est le résultat de cette division. Ensuite nous calculons le sous module $\mathcal{M}'' = \mathcal{M}' \cap \{0\} \times \mathcal{M}^{n-1}$ de $\mathcal{M}$. On peut faire ceci à l'aide de (b). Effectivement, soit $\{(a_{l,1}, \cdots, a_{l,n})\}_{l\in L}$ une famille génératrice du noyau de $\varphi : A^n \to A; (a_1, \cdots, a_n) \mapsto a_1b_{1,1} + \cdots + a_nb_{n,1}$. Alors la famille $\{a_{l,1}b_{i,1}, \cdots, a_{l,n}b_{i,n}\}_{1\leq i\leq n}$ est une famille génératrice de $\mathcal{M}''$. D'après l'hypothèse de récurrence, on a une division vérifiant les hypothèses de (c) pour $\{0\} \times \mathcal{M}^{n-1}$. Nous utilisons cette division, pour ensuite diviser c' par $\mathcal{M}''$. Il est facile de vérifier que cette division est compatible avec la division sur A.

Donnons nous maintenant deux sous modules $\mathcal{M}'$ et $\mathcal{M}''$ de $\mathcal{M}$, engendrés respectivement par $a_1, \cdots, a_p$ et $b_1, \cdots, b_q$. En utilisant la récurrence, on peut facilement calculer le sous module $\mathcal{M}' \cap \mathcal{M}''_{1,\cdots,n-1} \times A$ de $\mathcal{M}$, où $\mathcal{M}''_{1,\cdots,n-1} = \{(a_1, \cdots, a_{n-1}) | a \in \mathcal{M}''\}$ et sans perdre de généralité, on peut supposer qu'on a remplacé $\mathcal{M}'$ par ce sous module. Du coup, il existe des matrices M', M'', N, R à coefficients dans A, avec $M' = M''N + R$, où

$$M' = \begin{pmatrix} a_{1,1} & \cdots & a_{p,1} \\ \vdots & & \vdots \\ a_{1,n} & \cdots & a_{p,n} \end{pmatrix}, M'' = \begin{pmatrix} b_{1,1} & \cdots & b_{p,1} \\ \vdots & & \vdots \\ b_{1,n} & \cdots & b_{p,n} \end{pmatrix}, R = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \\ r_1 & \cdots & r_p \end{pmatrix}.$$

Soit c un vecteur, dans l'intersection de $\mathcal{M}'$ et $\mathcal{M}''$. Alors il existe des vecteurs α et β, avec

$$c = M''N\alpha + R\alpha = M''\beta.$$

Il s'en suit que $R\alpha$ est dans l'intersection de $\mathcal{M}''$ et le module engendré par les vecteurs colonnes de R. Comme il est facile de calculer cette intersection et comme par ailleurs il en est de même pour le noyau de l'application linéaire qui à α associe $R\alpha$, nous savons calculer l'intersection de $\mathcal{M}'$ et $\mathcal{M}''$. ♡

Remarque. Lorsque A est un anneau principal, on a $(a) \cap (b) = (ppcm(a,b))$, donc il suffit de savoir calculer des ppcms dans A. On a même plus: supposons que A soit principal et que pour tout $a, b \in A$ on ait $a|ab$, ce qui est vrai en particulier si A est commutatif ou si A est un corps. Alors on a une relation de Bezout $d_1 b_1 + \cdots + d_{n-1} b_{n-1} = pgcd(b_1, \cdots, b_{n-1}) = p$. On peut également écrire $ppcm(p, b_n) = qp$. Or $qp|qd_k b_k$, pour tout $1 \leq k \leq n-1$ et $q(d_1 b_1 + \cdots + d_{n-1} b_{n-1}) = ppcm(p, b_n)$. Il s'en suit que $ppcm(p, b_n) \in (ppcm(b_1, b_n), \cdots, ppcm(b_{n-1}, b_n))$. Mais ceci veut dire que dans la démonstration de (a) $\Rightarrow$ (b), on aurait pu prendre $c_l = a_{l,l} b_l = q d_l b_l$, avec $1 \leq l \leq m = n-1$. C'est-à-dire que la famille de vecteurs $(0, \cdots, 0, a_{k,k'}, 0, \cdots, 0, a'_{k,k'}, 0, \cdots, 0)$ engendre $\ker \varphi$, où les $a_{k,k'}$ et $a'_{k,k'}$ sont pris tels que $a_{k,k'} b_k = -a'_{k,k'} b_{k'} = ppcm(b_k, b_{k'})$.

Dans ce qui suit, nous considérons un anneau A muni d'une division et un A-algèbre à gauche $\mathcal{D}$ muni d'une base S. En nous inspirant des algèbres de polynômes, nous appelons les éléments de S les *monômes* de G. Nous allons rechercher une division sur $\mathcal{D}$.

Pour faire ceci, nous supposons que S est muni d'un ordre total $\leq$. Tout élément X de G s'écrit de façon unique:

$$X = \sum_{M \in S} X_M M, \text{ avec } X_M \in A.$$

On appelle $supp(X) = \{M | X_M \neq 0\}$ le *support* de X. Puis on appelle $P(X) = \max supp(X)$ le *monôme principal* de X, en convenant que $P(0) = -\infty$. Sinon, on appelle $CP(X) = X_{P(X)}$ le *coefficient principal* de X. Si on se donne un idéal à gauche I de $\mathcal{D}$ on définit également $P(I) = \{P(X) | X \in I\}$ et $I_M = \{X_M | X \in I \wedge P(X) \leq M\}$. Remarquons que I_M est un idéal à gauche de A. Entendons par *algèbre de division* tout $\mathcal{D}$, vérifiant les hypothèses précédentes et tel que $\leq$ soit bien fondé. Alors nous avons le premièr "théorème" fondamental:

Théorème 1. *Soit $\mathcal{D}$ une algèbre de division sur A. Alors pour tout idéal à gauche I de $\mathcal{D}$, l'ensemble*

$$R_I \stackrel{\text{déf}}{=} \{X \in \mathcal{D} | \forall M \in S \quad X_M \in R_{I_M}\}$$

est un ensemble de restes modulo I.

Démonstration. Soit $X \in \mathcal{D}$. Si $X \notin R_I$, alors il y a un monôme M, avec $X_M \notin R_{I_M}$ (d'où $X_M \neq 0$). Prenons M maximal avec cette propriété et notons le $M = O(X)$. Alors il existe un $Y \in I_M$, tel que $X_M - Y_M \in R_{I_M}$. Posons $X' = X - Y$. On vérifie aisément que pour tout monôme $N \geq M$, on a $X'_N \in R_{I_N}$. En réappliquant la procédure décrite plus haut récursivement à X', on construit une suite $X, X', X'', \cdots$ d'éléments de $\mathcal{D}$, tous équivalents modulo I. De plus, cette suite ne peut être infinie, car on a $O(X) > O(X') > O(X'') > \cdots$ et il n'y a pas de suite strictement décroissante infinie pour $\leq$. Le dernier terme de la suite est donc

dans R_I et équivalent à X modulo I. ♡

La démonstration fait croire que si la division dans A et la comparaison $\leq$ se font algorithmiquement, on a une division algorithmique dans $\mathcal{D}$. Mais attention: étant donné un $a \in I_M$, il est nécessaire de pouvoir trouver un $X \in I$, tel que $a = X_M$. Habituellement, I est donné par un ensemble fini de générateurs. Nous allons donner un algorithme de division par rapport à ces générateurs. Dans la section suivante on verra sous quelles conditions sur les générateurs cet algorithme de division correspond à la division du théorème 1.

Avant de donner l'algorithme, introduisons *l'ordre partiel $\preceq$ de divisibilité* sur S en définissant que pour tout $M, N \in S$, on a $M \preceq N$, ss'il existe un $L \in S$, tel que pour tout $X \in \mathcal{D}$, avec $P(X) = M$, on ait $N = P(LX)$. Si on sait tester l'existence d'un tel L et le trouver dans le cas affirmatif de façon algorithmique, on dira que $\preceq$ est algorithmique. Remarquons que dans la section suivante, on impose des conditions supplémentaires sur $\leq$, impliquant que $P(LX) = P(LP(X))$. Dans ce cas on a la définition alternative plus naturelle suivante pour $\leq$:

$$M \preceq N \Leftrightarrow \exists L \in S \quad N = P(LM).$$

Une algèbre de division est dit *algorithmique*, lorsque $\preceq$, A et la division sur A le sont. Maintenant nous avons l'algorithme de division suivant:

Algorithme 1. *Soit $F = \{Y_1, \cdots, Y_n\}$ un sous ensemble fini d'une algèbre de division algorithmique $\mathcal{D}$ et soit $X \in \mathcal{D}$. Alors l'algorithme de division non déterministe suivant termine et on note $X\%F$ un résultat de cette division.*

POUR $M \in supp(X)$ FAIRE (dans ordre décroissant pour $\leq$)
  $K := \emptyset$
  POUR $Y_k \in F$ FAIRE
    SI $P(Y_k) \preceq M$ ALORS
      TROUVER $N_k \in S$ tel que $P(N_k Y_k) = M$
      $K := K \cup \{k\}$
  TROUVER des a_k tel que $X_M = \sum_{k \in K} a_k CP(N_k Y_k) + X_M \div (\{CP(N_k Y_k)\}_{k \in K})$
  $X := X - \sum_{k \in K} a_k N_k Y_k$
RETOURNER X

Remarque. Il est clair que l'algorithme termine, car le M dans la boucle principale décroît strictement pour $\leq$ et $\leq$ est bien fondé. L'algorithme est non déterministe à cause du choix pour les a_k. Remarquons qu'en légèrement modifiant l'algorithme nous pouvons également calculer les Z_k, avec $X = \sum_{k=1}^{n} Z_k Y_k + X \div F$. Si l'algorithme de division par F correspond à la division par (F) du théorème 1, c.à.d. si $x\%F$ est unique et $x\%F = x \div (F)$, alors nous disons que F est une *base standard* de (F). Dans la section suivante, on donnera une autre définition équivalente des bases standard.

2.3 Algèbres de Gröbner

Dans cette section, nous verrons d'abord sous quelles conditions une algèbre de division $\mathcal{G}$ est noethérienne. Ensuite, nous établirons des conditions, pour qu'une partie finie $F \subseteq \mathcal{G}$ soit une base standard de (F). Finalement, nous établirons des conditions pour qu'on puisse construire une base standard d'un idéal à gauche finiment engendré.

Pour poursuivre, il nous faut généraliser un concept, qui est clair, si S est l'ensemble de monômes d'un anneau de polynômes: on dit que $\leq$ est *compatible avec la multiplication* , si:

(a) $1 \in S$ et $1 \leq P(X)$, pour tout $X \in \mathcal{G}$.
(b) $P(X) \leq P(Y) \wedge P(X') \leq P(Y') \Rightarrow P(XX') \leq P(YY')$, pour tout $X, X', Y, Y' \in \mathcal{G}$. De plus, on a égalité, ssi $P(X) = P(Y) \wedge P(X') = P(Y')$.
(c) $CP(XY) = uCP(X)CP(Y)$, pour un certain $u \in A^*$ et tout $X, Y \in \mathcal{G}$.

La troisième condition est satisfaite en particulier, si A est un corps. Remarquons que si les conditions sont satisfaites, alors l'application $\delta_M : A \to A; a \mapsto CP(Ma)$ est un opérateur à différences, pour tout $M \in S$. Effectivement, on peut écrire $CP(Mab) = (\delta_M(a)M + X)b = \delta_M(a)\delta_M(b)M + X' = \delta_M(ab)M + X''$, avec $P(X), P(X'), P(X'') < M$.

Pour pouvoir répondre à la question, à savoir quand les idéaux à gauche de $\mathcal{G}$ sont finiment engendrés, il nous faut encore quelques compléments sur la théorie de l'ordre. On dira qu'un ordre partiel $\preceq$ est un *belordre*, s'il est bien fondé et s'il n'admet pas d'antichaîne infinie. Voir [Krus 72],[PR 81] pour quelques résultats sur ce genre d'ordres. Nous aurons besoin de la:

Proposition 1. *Nous avons:*

(a) Un ordre partiel est un belordre ssi toute partie finale est finiment engendrée.
(b) Un ordre partiel est un belordre ssi toute suite admet une sous suite extraite croissante.
(c) Tout ordre total bien fondé est un belordre.
(d) Tout ordre partiel produit de deux belordres est un belordre.

Démonstration. Soit F une partie finale d'un belordre (c.à.d. $x \in F \wedge x \preceq y \Rightarrow y \in F$). Soit $G \subseteq F$ l'ensemble des élément minimaux de F. G est une antichaîne, donc fini. De plus G engendre F, car un belordre est bien fondé. Réciproquement, si $x_1, x_2, \cdots$ est une antichaîne infinie ou une suite strictement décroissante infinie, pour un certain ordre partiel, la partie finale engendrée par $\{x_1, x_2, \cdots\}$ n'est pas finiment engendrée. Ceci démondre (a).

Soit maintenant une suite $\{x_1, x_2, \cdots\}$ à valeurs dans l'ensemble E muni d'un belordre. Extrayons une sous suite croissante $\{x_{i_1}, x_{i_2}, \cdots\}$ par le procédé suivant: On appelle F_n la partie finale engendrée par les x_k, avec $k > i_n$ et $x_k \succeq x_{i_n}$ en

convenant que $F_0 = E$. On suppose par récurrence que la suite admet une infinité de termes dans F_n. Or F_n admet un nombre fini de générateurs et nous pouvons donc choisir un générateur $x_{i_{n+1}}$, avec $i_{n+1} > i_n$ et tel que la suite admet une infinité de termes dans F_{n+1}. Réciproquement, il est évident qu'on ne peut pas extraire une sous suite croissante d'une antichaîne infinie ou d'une suite strictement décroissante infinie. Ceci démontre (b).

Finalement (c) est trivial et (d) découle facilement de la deuxième caractérisation des belordres. On rappelle que l'ordre produit de deux ordres partiels sur E resp. F est l'ordre partiel par composants sur $E \times F$. ♡

En particulier, $\mathbb{N}^n$, muni de l'ordre produit est un belordre (on appelle ce résultat aussi le lemme de Dickson) et c'est le belordre le plus important qu'on rencontre. En fait, nous avons l'impression que tout ordre partiel de divisibilité d'une algèbre de division, qui est un belordre est en fait un sous ordre partiel de l'ordre partiel produit sur $\mathbb{N}^n$.

On appelle *algèbre de Gröbner* toute algèbre $\mathcal{G}$ de division sur un anneau noethérien tel que $\leq$ est compatible avec la division et tel que l'ordre partiel de divisibilité $\preceq$ soit un belordre. A titre de culture nous remarquons que pour les théorèmes qui vont suivre, des définitions légèrement moins contraignantes sont déja suffisantes. Par exemple pour le théorème qui va suivre, la troisième condition de compatibilité avec la multiplication peut être remplacée par $P(XY)|P(X)P(Y)$, pour tout $X, Y \in \mathcal{G}$. De même pour le théorème suivant, il n'est pas nécessaire que $\preceq$ soit un belordre, ni que A soit noethérien.

Nous avons le deuxième théorème fondamental:

Théorème 2. *Toute algèbre de Gröbner G est noethérienne.*

Démonstration. Remarquons d'abord que $M \preceq N \Rightarrow I_M \subseteq I_N$, pour tout $M, N \in S$. Effectivement, supposons que $M \preceq N$. Il existe un $L \in S$ tel que $N = P(LM)$. Soit maintenant $X \in I_M$. On a $P(LX) = P(LM) = N$ et $CP(LX)|CP(L)CP(X) = CP(X)$, donc $CP(X) \in I_N$.

Montrons ensuite que l'ensemble $E = \{I_M | M \in S\}$ est fini. Dans le cas contraire, d'après la deuxième caractérisation des belordres, on peut trouver une suite strictement croissante $M_1 \prec M_2 \prec \cdots$, tel que les I_{M_n} sont deux à deux distincts. La suite $I_{M_1}, I_{M_2}, \cdots$ est donc une chaîne infinie d'idéaux à gauche de A; Contradiction.

Maintenant, pour tout $J \in E$, l'ensemble $F_J = \{M | I_M \supseteq J\}$ est une partie finale de S et admet une partie génératrice finie, minimale pour l'inclusion $M_{J,1}, \cdots, M_{J,n_J}$. De plus F_J est finiment engendré, disons par $a_{J,1}, \cdots, a_{J,k_J}$. Il existe donc des $X_{J,i,j}$ dans $\mathcal{G}$, avec $P(X_{J,i,j}) = M_{J,i}$ et $CP(X_{J,i,j}) = a_j$, pour tout $1 \leq i \leq n_J$ et $1 \leq j \leq k_J$.

Montrons enfin que I est l'idéal I' engendré par les $X_{J,i,j}$. Dans le cas contraire, il existe un $X \in I - I'$, et on peut supposer $P(X)$ minimal pour $\leq$. Alors soit $J = I_{P(X)}$. Il existe un $M_{J,i}$ avec $M_{J_i} \preceq P(X)$ et donc un $Y \in \mathcal{G}$, avec

$P(X) = P(YM_{J,i})$ et $CP(Y) = 1$. Ensuite, il existe des $b_1, \cdots, b_{J,k_J}$ tels que $CP(X) = b_1 a_{J,1} + \cdots + b_{k_J} a_{J,k_J}$. Soit $X' = Y(b_1 X_{J,i,1} + \cdots + b_{k_J} X_{J,i,k_J})$. On a $X' \in I$, $P(X') = P(X)$ et $CP(X')|CP(X)$. Pour un certain $c \in A$, nous avons donc $X - cX' \in I$ et $P(X - cX') < P(X)$. Contradiction, car $X - cX'$ et cX' sont alors dans I'. ♡

Soient $Y_1, \cdots, Y_n \in \mathcal{G}$ et $I = (Y_1, \cdots, Y_n)$. On appelle *combinaison admissible* de $Y_1, \cdots, Y_n$ tout $X \in I$, qui s'écrit $X = V_1 Y_1 + \cdots + V_n Y_n$, avec $V_1, \cdots, V_n \in \mathcal{G}$, tels que $P(V_k Y_k) \leq P(X)$, pour tout $1 \leq k \leq n$. On note $(Y_1, \cdots, Y_n)_{adm} \subseteq I$ l'ensemble des combinaisons admissibles de $Y_1, \cdots, Y_n$ et $(Y_1, \cdots, Y_n)_{nadm}$ son complémentaire dans I. Remarquons que $X, X' \in (Y_1, \cdots, Y_n)_{adm}$ et $CP(X)P(X) + CP(X')P(X') \neq 0$, implique $X + X' \in (Y_1, \cdots, Y_n)_{adm}$ (ce qui est vrai en particulier, si $P(X) \neq P(X')$). Remarquons également que si $X \in (Y_1, \cdots, Y_n)_{adm}$ et $Y_k \in (Z_1, \cdots, Z_m)_{adm}$ $(1 \leq k \leq n)$, alors $X \in (Z_1, \cdots, Z_m)_{adm}$. Par analogie, avec les définitions de $(I)_M$ et $P(X)$, définissons également $(Y_1, \cdots, Y_n)_{M,adm} = \{CP(X) | X = \sum_{k=1}^n V_k Y_k$, avec $P(V_k Y_k) \leq M\}$ et (en supposant qu'il est clair qu'on raissonne par rapport à $Y_1, \cdots, Y_n$) $P_{adm}(X)$, comme étant le plus petit monôme (pour $\leq$) tel qu'on peut écrire $X = \sum_{k=1}^n V_k Y_k$, avec $P(V_k Y_k) \leq P_a dm(X)$, pour chaque k.

Donnons maintenant une autre définition pour les bases standard et montrons que cette nouvelle définition coïncide avec l'ancienne. On dit que $Y_1, \cdots, Y_n$ est une *base standard* de I, lorsque $(Y_1, \cdots, Y_n)_{adm} = I$. On remarque qu'en particulier l'ensemble $X_{J,i,j}$ figurant dans la démonstration précédente est une base standard, ce qui montre l'existence des bases standard dans des algèbres de Gröbner. Montrons maintenant que cette nouvelle définition des bases standard coïncide avec l'ancienne:

Théorème 3. *Soit $\mathcal{G}$ un algèbre de Gröbner sur un anneau de division algorithmique. Alors les deux définitions des bases standard coïncident. De plus $X\%F = 0 \Rightarrow X \in (F)_{adm}$.*

Démonstration. Dans cette démonstration on notera par $X, \hat{X}, \cdots$ les valeurs successives prises par X dans l'algorithme. Supposons qu'il existe un $X \in (F)_{nadm}$, avec $X\%F = 0$. Prenons un tel X avec $P(X)$ minimal (pour $\leq$). On peut écrire $\hat{X} = X - \sum_{k \in K} a_k N_k Y_k$, avec les notations de l'algorithme 1. Or $\sum_{k \in K} a_k N_k Y_k$ est clairement dans $(F)_{adm}$. De plus, $\hat{X}\%F = 0$ et $P(\hat{X}) < P(X)$, donc $\hat{X}$ est également dans $(F)_{adm}$. Il en est donc de même pour leur somme X; Contradiction.

Supposons réciproquement que tout $X \in (F)$ est dans $(F)_{adm}$. S'il existe un X, avec $X\%F \neq X \div F$, alors on peut prendre un tel X, avec $P(X)$ minimal. Remarquons qu'à cause de cette minimalité, on a $(X\%F)_P(X) \notin R_{(F)_{P(X)}}$. Posons $X' = (X\%F) - (X \div F) \in (F)$. On a $X' \in (F)_{adm}$, donc on peut écrire $X' = V_1 Y_1 + \cdots + V_n Y_n$, avec $F = \{Y_1, \cdots, Y_n\}$ et $P(V_k Y_k) \leq P(X')$, pour $1 \leq k \leq n$. Soit K' l'ensemble des indices k, tel que $P(V_k Y_k) = P(X')$. Il s'en

suit que $P(Y_k) \preceq P(X') = P(X)$, pour $k \in K'$ (donc $K' \subseteq K$, encore avec les notations de l'algorithme 1) et que $CP(X') \in (\{CP(Y_k)\}_{k\in K}) = J$. Ceci implique $(X\%F) \div_A J = (X \div F) \div_A J \in R_{(F)_{P(X)}}$. Mais alors $(X\%F)_{P(X)} = (\hat{X}\%F)_{P(X)} \in R_{(F)_{P(X)}}$; Contradiction. ♡

2.4 Construction des bases standard

Le théorème précédent n'implique pas qu'on ait une division algorithmique sur $\mathcal{G}$. Pour avoir cela, il faudra pouvoir construire une base standard de tout idéal à gauche I finiment engendré. Dans ce but, disons qu'une algèbre de Gröbner est *algorithmique*, si l'anneau A est un anneau de division algorithmique augmenté et si pour tout couple $M, N \in S$, on sait trouver par algorithme une partie génératrice $PG(M,N)$ de $S_M \cap S_N \stackrel{\text{déf}}{=} \{M' \in S | M, N \preceq M'\}$. Pour être très correct, il faudrait rajouter la condition que le lemme 2 (voir ci-dessous) soit vérifié. Nous n'avons pas encore réussi à démontrer ce lemme si le couple $(A, \mathcal{G})$ ne vérifie pas les hypothèses du lemme, mais il nous semble que la conclusion du lemme est toujours vraie.

Lemme 2. *Soit $\varphi : A^n \to A; (a_1, \cdots, a_n) \mapsto a_1b_1 + \cdots a_nb_n$ une forme linéaire, tel que $\{(a_{l,1}, \cdots, a_{l,n})\}_{l\in L}$ soit une base du noyau de φ. On suppose qu'une des conditions suivantes soit vérifiée:*

(a) $\delta_M = Id_A$ pour chaque $M \in S$.
(b) δ_M est inversible pour chaque $M \in S$.
(c) A est un corps commutatif.

Alors pour tout $M \in S$, la famille $\{(\delta_M(a_{l,1}), \cdots, \delta_M(a_{l,n}))\}_{l\in L}$ est une base de $\ker \varphi_M$, *avec $\varphi_M : (a_1, \cdots, a_n) \mapsto a_1\delta_M(b_1) + \cdots + a_n\delta_M(b_n)$.*

Démonstration. Le lemme est évident, si la condition (a) est vérifiée. Plus généralement, lorsque les δ_M sont inversibles, le résultat est vrai, car dans ce cas $a_1\delta_M(b_1) + \cdots + a_n\delta_M(b_n) = 0 \Rightarrow \delta_M^{-1}(a_1)b_1 + \cdots + \delta_M^{-1}(a_n)b_n = 0$. La démarche pour démontrer le résultat plus généralement, est de plonger l'anneau A dans un suranneau A', dans lequel les a_k sont inversibles (par rapport à δ_M). Dans le premier chapitre, on a montré qu'on peut faire ceci. En revanche, il reste à vérifier que le noyau de $\varphi' : A'^n \to A'; (a_1, \cdots, a_n) \mapsto a_1b_1 + \cdots + a_nb_n$ admet encore la famille $\{(a_{l,1}, \cdots, a_{l,n})\}_{l\in L}$ comme base. Jusqu'au présent on n'a su le vérifier que dans le cas où K est un corps commutatif. Effectivement, dans ce cas A' est un K-algèbre admettant une base. Le résultat suit trivialement en décomposant sur cette base. ♡

Supposons que $\mathcal{G}$ est une algèbre de Gröbner algorithmique. Nous aurons également besoin d'une généralisation des S-polynômes, d'après Buchberger (voir [Buch

65], [Buch 85]). Malheureusement, si A ne vérifie pas les conditions de la remarque après le lemme 1, un S-polynôme n'est plus défini relativement à deux polynômes. Plus précisement, considérons une famille finie $Y_1, \cdots, Y_n$ d'éléments de A. Il est facile de vérifier qu'on sait construire par algorithme une partie génératrice $E = PG(P_{Y_1}, \cdots, PY_n)$ de $S_{P_{Y_1}} \cap \cdots \cap S_{P_{Y_n}}$. Soit $M \in E$. On peut trouver par algorithme des N_k, avec $P(N_k Y_k) = M$, pour tout $1 \leq k \leq n$. Par ailleurs, considérons l'application $\varphi := (a_1, \cdots, a_n) \mapsto \sum_{k=1}^{n} a_k CP(N_k Y_k)$. D'après le lemme 1, on sait trouver par algorithme une famille génératrice $\{(a_{l,1}, \cdots, a_{l,n})\}_{1 \leq l \leq m}$ de $\ker \varphi$. Posons $X_l = \sum_{k=1}^{n} Q_{l,k} Y_k$, avec $Q_{l,k} = a_{l,k} N_k$, pour tout $1 \leq l \leq m$. Tout élément X_l construit de cette façon est appellé *S-élément* de $Y_1, \cdots, Y_n$. Comme, l'ensemble E est fini, il n'y en a qu'un nombre fini. Notons cet ensemble de S-éléments $SE(Y_1, \cdots, Y_n)$. Les S-éléments sont importants à cause du lemme suivant:

Lemme 3. *Adoptons les notations précédant le lemme. Soit $Z = V_1 Y_1 + \cdots + V_n Y_n$, avec $P(Z) < L = P(V_1 Y_1) = \cdots = P(V_n Y_n)$ et $E \ni M \preceq L$. Alors il existe un $Z' = W_1 X_1 + \cdots + W_m X_m$, avec $P(W_l X_l) < L$ et $P((V_k - \sum_{l=1}^{m} W_l Q_{l,k}) Y_k) < L$, pour tout k et l.*

Démonstration. Soit $M' \in S$, avec $L = P(M'M)$. Avec les N_k, définis comme tout à l'heure, on a donc $L = P(M' N_k Y_k)$, pour tout k. Il s'en suit qu'on peut écrire $V_k = b_k M' N_k + V'_k$, avec $P(V'_k) < P(V_k)$. On a $\sum_{k=1}^{n} CP(b_k M' N_k Y_k) = \sum_{k=1}^{n} b_k \delta_{M'}(CP(N_k Y_k)) = 0$, donc d'après le lemme 2, ils existent $c_1, \cdots, c_l$, avec $b_k = \sum_{l=1}^{m} c_l \delta_{M'}(a_{l,k})$, pour tout k. Il s'en suit que $CP(b_k M') = \sum_{l=1}^{m} CP(c_l M' a_{l,k})$.

Posons $Z' = \sum_{l=1}^{m} W_l X_l$, avec $W_l = c_l M'$. Par construction, on a $P(X_l) < M$, d'où $P(W_l X_l) < L$, pour tout l. De plus $P(b_k M' Y_k) = P(V_k Y_k) = L$ et $P(\sum_{l=1}^{m} W_l Q_{l,k} Y_k) \leq P(M'M) = L$, pour chaque k. Or le coefficient en M' de $b_k M' - \sum_{l=1}^{m} W_l a_{l,k}$ nul. Il en est donc de même pour le coefficient en L de

$$(V_k - \sum_{l=1}^{m} W_l Q_{l,k}) Y_k = \left(\left(b_k M' - \sum_{l=1}^{m} c_l M' a_{l,k} \right) N_k + V'_k \right) Y_k.$$

Ceci achève la démonstration. ♡

Maintenant, nous sommes en mesure de pouvoir donner l'algorithme de construction des bases standard et de démontrer les derniers théorèmes fondamentaux

Algorithme 2. *Soit $\mathcal{G}$ une algèbre de Gröbner algorithmique et $F \subset \mathcal{G}$ une partie finie de $\mathcal{G}$. Alors nous avons l'algorithme de construction de base standard de (F):*

FAIRE
$\{Y_1, \cdots, Y_n\} := F$
POUR $K \subseteq \{1, \cdots, n\}$, *avec* $|K| \geq 2$, *FAIRE*
CALCULER $SE(\{Y_k\}_{k\in K})$
POUR $X \in SE(\{Y_k\}_{k\in K})$ *FAIRE*
SI $X\%F \neq 0$ *ALORS*
$F := F \cup \{X\%F\}$
JUSQU'A F *n'a plus changé*
RETOURNER F

Remarque. Il est clair qu'en légèrement modifiant l'algorithme, on peut également exprimer les éléments de la base standard rendue comme combinaison linéaire des $Y_1, \cdots, Y_n$ originaux.

Théorème 4. *Soit $\mathcal{G}$ une algèbre de Gröbner algorithmique. Alors $\mathcal{G}$ est un anneau de division algorithmique.*

Démonstration. En utilisant le théorème 3 et la remarque après l'algorithme 1, il reste à montrer que pour toute partie finie $F \subseteq \mathcal{G}$, l'algorithme 2 termine et rend une base standard de F.

Montrons d'abord que l'algorithme 2 termine. Comme dans la démonstration du théorème 2, on a $(F)_{M,adm} \subseteq (F)_{N,adm}$, si $M \preceq N$. De plus, si $F' = F \cup \{X\%F\}$, pour $X\%F \neq 0$, montrons que $(F)_{P(X\%F),adm} \subset (F')_{P(X\%F),adm}$. Effectivement, dans l'algorithme 1, on a $(\{CP(N_kY_k\})_{k\in K}) = (F)_{M,adm}$, pour tout $M \in S$, d'où $(X\%F)_M \in R_{(F)_{M,adm}}$, pour tout $M \in S$. Donc, si par ailleurs $CP(X\%F) \in (F')_{P(X\%F),adm}$, alors $CP(X\%F) = 0$, d'où $X\%F = 0$.

Supposons maintenant que l'algorithme ne termine pas, pour un F donné. Il existe donc une suite infinie $(F_1, X_1), (F_2, X_2), \cdots$, avec $F_1 = F$ et $F_{n+1} = F_n \cup \{X_n\}$, avec $X_n\%F_n \neq 0$. On peut en extraire une sous suite $(F_{n_1}, X_{n_1}), (F_{n_2}, X_{n_2}), \cdots$ telle que $P(X_{n_1}) \preceq P(X_{n_2}) \preceq \cdots$. D'après ce qui précède, on a donc la chaîne ascendante infinie $(F_{n_1})_{P(X_{n_1}\%F_{n_1}),adm} \subset (F_{n_2})_{P(X_{n_2}\%F_{n_2}),adm} \subset \cdots$ d'idéaux à gauche de A; Contradiction.

Montrons maintenant par l'absurde que l'algorithme 2 rend bien une base standard de (F). Supposons alors que F est un résultat de l'algorithme 2, qui n'est pas une base standard de (F). Il existe donc un $Z \in (F)_{nadm}$ et choissisons le de sorte que $L = P_{adm}(Z)$ soit minimal. Ecrivons $Z = V_1Y_1 + \cdots + V_nY_n$. On peut supposer sans perdre de généralité que $P(V_1Y_1) = \cdots = P(V_nY_n)$, quite à remplacer $\{Y_1, \cdots, Y_n\}$ par un sous ensemble $\{Y_k\}_{k\in K}$ pour lequel ceci soit vrai. D'après le lemme 2, on peut trouver un $Z' = W_1X_1 + \cdots + W_mX_m$, avec $P(W_lX_l) < L$ et $P((V_k - \sum_{l=1}^m W_lQ_{l,k})Y_k) < L$, pour tout k et l. Or les X_l sont combinaisons admissibles des Y_k. Il s'en suit que $P_{adm}(Z') < L$ et $P_{adm}(Z - Z') < L$. Mais alors $P_{adm}(Z) < L$; Contradiction. ♡

Remarque. L'algorithme 2 peut encore être optimisé du point de vue de la vitesse. On peut par exemple supprimer des éléments redondants dans F en cours de route et diviser chaque $Y_k \in F$ par $F - \{Y_k\}$. De plus, lorsque les hypothèses de la remarque après le lemme 1 sont vérifiés, on vérifie qu'il suffit de considérer des sous ensembles K de $\{1, \cdots, n\}$ de deux éléments, comme dans l'algorithme classique.

Lorsqu'on considère des algèbres de Gröbner sur des algèbres de Gröbner, on voudrait également pouvoir démontrer qu'une algèbre de Gröbner algorithmique est en fait un anneau de division augmenté. D'après la deuxième caractérisation des anneaux de division augmenté (lemme 1(c)), ceci sert également lorsqu'on considère des divisions sur des modules libres à gauche de type fini sur une algèbre de Gröbner. En effet, nous avons le:

Théorème 5. *Soit $\mathcal{G}$ une algèbre de Gröbner algorithmique. Alors $\mathcal{G}$ est un anneau de division algorithmique augmenté.*

Démonstration. Nous allons montrer ceci en utilisant la première caractérisation des anneaux de division algorithmique augmentés (lemme 1(b)). Considérons donc l'application linéaire

$$\begin{aligned} \varphi : \mathcal{G}^n &\to \mathcal{G}, \\ (V_1, \cdots, V_n) &\mapsto V_1Y_1 + \cdots + V_nY_n. \end{aligned}$$

Traitons d'abord le cas où $F = \{Y_1, \cdots, Y_n\}$ est une base standard. Soit X_l un S-élément d'un sous ensemble K de F. On peut écrire $X_l = \sum_{k=1}^{n} Q_{l,k}Y_k$, avec les notations précedant le lemme 3 et en convenant que $a_{l,k} = 0$, si $k \notin K$. La division de X_l par F nous fournit également une expression de X_l comme combinaison admissible de $Y_1, \cdots, Y_n$, disons $X_l = Q'_{l,1}Y_1 + \cdots + Q'_{l,n}Y_n$. Il est clair que le n-tuple $(Q'_{l,1} - Q_{l,1}, \cdots, Q'_{l,n} - Q_{l,n})$ est dans le noyau de φ. Nous affirmons que le module à gauche $\mathcal{M}$ engendré par la famille de n-tuples ainsi construits est égal à $\ker\varphi$.

Notons par $\mathcal{M}$ le module à gauche engendré par la famille qu'on vient de construire et montrons notre affirmation par l'absurde. Prenons $(V_1, \cdots, V_n) \in \ker\varphi - \mathcal{M}$, tel que $L = \max(P(V_1Y_1), \cdots, P(V_nY_n))$ soit minimal (pour $\leq$). Prenons pour l'ensemble K de tout à l'heure, l'ensemble des indices k tels que $P(V_kY_k) = L$. D'après le lemme 3, appliqué sur les Y_k, avec $k \in K$ et en prenant $Z = 0$, il existe un $Z' = W_1X_1 + \cdots + W_mX_m$, avec $P(W_lX_l) < L$ et $P((V_k - \sum_{l=1}^{m} W_lQ_{l,k})Y_k) < L$, pour tout k et l. Or on a également $P((\sum_{l=1}^{m} W_lQ'_{l,k})Y_k) < L$, pour tout k, car $P(Q'_{l,k}X_k) \leq P(X_l)$, pour tout k et l. Considérons maintenant le n-tuple $(V'_1, \cdots, V'_n)$, où

$$V'_k = V_k + \sum_{l=1}^{m} W_l(Q'l, k - Q'l, k),$$

pour chaque k. D'après ce qui précède, on a $P(V'_kY_k) < L$, pour chaque k et ce n-tuple est donc dans $\mathcal{M}$, d'après l'hypothèse de minimalité. Il s'en suit que $(V_1, \cdots, V_n)$ est également dans $\mathcal{M}$; Contradiction.

Traitons maintenant le cas général. Construisons une base standard $Y'_1, \cdots, Y'_{n'}$ de $(Y_1, \cdots, Y_n)$. D'après la remarque après les algorithmes 1 et 2, on peut trouver des $R'_{k,k'}$ et $R_{k',k}$, tels que $Y_k = \sum_{k'=1}^{n'} R'_{k,k'} Y'_{k'}$ et $Y_{k'} = \sum_{k=1}^{n} R_{k',k} Y_k$. Sinon, d'après ce qui précède, on sait trouver une famille de générateurs $(Q_{l,1}, \cdots, Q_{l,n'})_{l \in L}$ du noyau de $\varphi' : (V'_1, \cdots, V'_{n'}) \mapsto V'_1 Y'_1 + \cdots + V'_{n'} Y'_{n'}$. Alors nous prétendons que les vecteurs lignes de la matrice

$$\begin{pmatrix} R'R - I_n \\ QR \end{pmatrix}$$

engendrent $\ker \varphi$. Effectivement, soit $(V_1, \cdots, V_n)$ dans le noyau de φ. Considérons V comme vecteur ligne et Y et Y' comme vecteurs colonnes. Nous avons donc $VY = 0$, et $VR'Y' = 0$, d'où l'existence d'un vecteur ligne W, avec $VR' = WQ$. On en déduit $VR'R = WQR$, d'où l'expression

$$V = (VW) \begin{pmatrix} R'R - I_n \\ QR \end{pmatrix}.$$

Ceci achève la démonstration. ♡

Bien qu'on puisse réduire canoniquement un élément par rapport à un idéal à gauche dans un anneau de division algorithmique, on peut également demander à avoir des formes canoniques pour ces idéaux à gauche mêmes. On dira qu'un anneau de division algorithmique est un *anneau de réduction*, si pour tout idéal à gauche présenté par des générateurs, on sait trouver des générateurs canoniques par algorithme. Dans ce cas, chaque idéal à gauche est représenté par un unique objet. Si de plus, A est un anneau de division augmenté, on dira que A est un *anneau de réduction augmenté*.

Supposons qu'on ait une algèbre de Gröbner algorithmique sur un corps. En divisant chaque élément d'une base standard par rappport aux autres et en normalisant les termes principaux, on obtient ce qu'on appelle une *base standard réduite*. On montre aisément que pour un ordre $\leq$ fixé, un idéal à gauche donné admet une unique base standard réduite. Nous comptons obtenir un résultat semblable pour une algèbre de Gröbner algorithmique sur un anneau de réduction.

Cependant, nous remarquons qu'on n'a tout de même pas besoin de cette notion plus forte pour tester l'égalité de deux idéaux à gauche. Effectivement, un idéal à gauche est inclus dans un autre, si chaqun des générateurs de l'un se reduit à zéro modulo l'autre. Comme pour un idéal donné, la construction d'une base standard peut se faire beaucoup plus vite pour un certain ordre $\leq$, compatible avec la multiplication que pour un autre ordre $\leq'$, il n'est sans doute pas réaliste de fixer un ordre pour le bon, ce qui est nécessaire pour rendre l'algèbre de Gröbner un anneau de réduction.

2.5 Exemples d'algèbres de Gröbner

Exemple 1. L'exemple le plus classique d'une algèbre de Gröbner est bien entendu l'anneau de polynômes $\mathcal{G} = K[X_1, \cdots, X_n]$, où K est un corps. On prend pour S l'ensemble des monômes de $\mathcal{G}$. Comme ordre $\leq$ sur S, compatible avec la multiplication, il y a plusieurs possibilités: l'ordre lexicigraphique, l'ordre lexicographique gradué , l'ordre lexicographique inverse gradué, etc. Comme S est stable par multiplication, l'ordre partiel de divisibilité coïncide avec la divisibilité dans $\mathcal{G}$. Sinon $S_M \cap S_N = S_{ppcm(M,N)}$, pour tout couple de monôme (M, N) et où le ppcm est pris dans $\mathcal{G}$. Il s'en suit que $\mathcal{G}$ est une algèbre de Gröbner algorithmique. Remarquons qu'on n'a même pas eu besoin de supposer K commutatif, sous la condition que les indéterminés $X_1, \cdots, X_n$ soient dans le centre de $\mathcal{G}$.

Les définitions et les démonstrations des théorèmes dans les sections précédentes se simplifient de façon importante dans ce cas particulier. La condition (b) de la compatibilité avec la multiplication peut être remplacée par $X \leq Y \wedge X' \leq Y' \Rightarrow XX' \leq YY'$, à cause du fait que S est stable par multiplication. La condition (c) est trivialement vérifiée, car K est un corps. La démonstration du théorème 2 se simplifie, car une partie F de $\mathcal{G}$, telle que $P(F)$ engendre $P(I)$ est une base standard, à cause du fait que K est un corps. Sinon, la condition (b) pour que $\mathcal{G}$ soit algorithmique est trivialement vérifiée, toujours parce que K est un corps et d'après la remarque faite à la fin de la section 2.4, il suffit donc de calculer des S-polynômes dans l'algorithme 2, ce qui le simplifie nettement, ainsi que sa démonstration.

Exemple 2. La première extension de l'exemple précédent apparaît, lorsque $\mathcal{G} = A[X_1, \cdots, X_n]$, où A est juste un anneau principal commutatif. Les principaux exemples sont $A = \mathbb{Z}$, $A = K[X]$ et $A = K[[X]]$. Maintenant, les démonstrations des théorèmes 2 et 3 ne se simplifient plus essentiellement. En revanche, l'algorithme 2 ainsi que sa démonstration se simplifient encore, du fait qu'il suffit de calculer des S-polynômes.

Présentons maintenant un exemple de construction de base standard dans $\mathcal{G} = \mathbb{Z}[X, Y]$, avec pour $\leq$ l'ordre lexicographique gradué, avec $X \leq Y$. Prenons

$$F = \{4XY^2 - 2X, 3X^2Y - Y\}.$$

Rajoutons d'abord $3X(4XY^2 - 2X) - 4Y(3X^2Y - Y) = 4Y^2 - 6X^2$ à F et réduisons chaque élément par rapport aux autres. On obtient $4XY^2 - 2X \to 6X^3 - 2X$, d'où

$$F_2 = \{3X^2Y - Y, 6X^3 - 2X, 4Y^2 - 6X^2\}.$$

Calculons à nouveau les S-polynômes: $2X(3X^2 - Y) - Y(6X^3 - 2X) = 0$, $4Y(3X^2Y - Y) - 3X^2(4Y^2 - 6X^2) = 18X^4 - 4Y^2 \to -4Y^2 + 6X^2 \to 0$ et $2Y^2(6X^3 - 2X) - 3X^2(4Y^2 - 6X^2) = 18X^5 - 4Y^2 \to -4XY^2 + 6X^3 \to 0$. Il s'en suit que F_2 est une base standard de (F). Dans la figure 1 on trouve une visualisation de la situation:

$\vdots$								
Y^5	4	4	1	1	1	1	1	
Y^4	4	4	1	1	1	1	1	
Y^3	4	4	1	1	1	1	1	
Y^2	4	4	1	1	1	1	1	
Y			3	3	3	3	3	
1				6	6	6	6	
	1	X	X^2	X^3	X^4	X^5	X^6	$\cdots$

Figure 1

Exemple 3. Considérons l'anneau non commutatif $\mathcal{G} = \mathbb{Q}[z, d]$ d'opérateurs différentiels linéaires à coefficients polynômiaux dans $\mathbb{Q}$, avec bien entendu la composition comme loi multiplicative. On remarque un abus de notation, car $\mathcal{G}$ n'est pas isomorphe à l'anneau des polynômes en deux variables. Néanmoins, la signification de $\mathbb{Q}[z, d]$ est claire et dans la suite on pratiquera systématiquement cet abus de notation.

Cette fois ci, $S = \{z^n d^m\}_{n,m\in\mathbb{N}}$ n'est plus stable par multiplication, car $dz = zd + 1$. En revanche, on vérifie que l'ordre lexicographique sur S, avec $z \leq d$ est compatible avec la division au sens de la définition dans la section 2.3. Donnons un exemple de calcul de base standard dans ce cas non commutatif. Prenons

$$F = \{zd^2 + 2z^2d + z^3 + z, d^3 + zd^2 + 2d\}.$$

Calculons le "S-opérateur" des deux opérateurs de F:

$$\begin{aligned} & d(zd^2 + 2z^2d + z^3 + z) - z(d^3 + zd^2 + 2d) \\ = \;& (z^2 + 1)d^2 + (z^3 + 3z)d + 3z^2 + 1 \\ \to \;& d^2 + (-z^3 + 3z)d - z^4 + 2z^2 + 1. \end{aligned}$$

Ensuite, réduisons les éléments de $F \cup \{d^2 + (-z^3 + 3z)d - z^4 + 2z^2 + 1\}$:

$$\begin{aligned} & zd^2 + 2z^2d + z^3 + z \\ \to \;& (z^4 - z^2)d + z^5 - z^3. \\ & d^3 + zd^2 + 2d \\ \to \;& (z^3 - 2z)d^2 + (z^4 + z^2 - 2)d + 4z^3 - 4z \\ \to \;& (z^6 - 4z^4 + 7z^2 - 2)d + z^7 - 7z^5 + 7z^3 - 2z. \end{aligned}$$

On obtient:

$$F_2 = \{d^2 + (-z^3 + 3z)d - z^4 + 2z^2 + 1, (z^4 - z^2)d + z^5 - z^3, \\ (z^6 - 4z^4 + 7z^2 - 2)d + z^7 - 7z^5 + 7z^3 - 2z\}.$$

En réduisant les deux derniers éléments, on trouve ensuite $z^2d + z^3 \in (F)$. Puis, en réduisant le premier élément, on obtient $zd + z^2 \in (F)$. Enfin, en simplifiant encore ce premier élément (en divisant le terme en d par $zd + z^2$), on obtient la base standard suivante pour (F):

$$F_3 = \{d^2 - z^2 + 1, zd + z^2\}.$$

Exemple 4. Considérons l'anneau $\mathcal{G} = A[d] = \mathbb{C}[[z]][d]$. On sait que $\mathbb{C}[[z]]$ est un anneau local et principal. On prend $S = \{d^n\}_{n\in\mathbb{N}}$ et pour $\leq$ l'ordre naturel sur S. La condition (c) de la compabilité avec la multiplication est trivialement vérifiée, car $\delta_M = Id_A$, pour tout $M \in S$. Ceci est d'ailleurs une situation générale lorsqu'on considère des opérateurs différentiels. On remarque que A n'est pas dénombrable et ne peut donc être algorithmique; On a donc uniquement l'existence théorique des bases standard par le théorème 3. Remarquons en revanche qu'on peut très bien considérer des sous anneaux principaux A au lieu de A, comme par exemple $A = \hat{\mathbb{Q}}(exp(z), sin(z), etc.)[z]$, qui sont algorithmiques. Formellement, les algorithmes 1 et 2 s'appliquent alors.

On peut également prendre pour A l'ensemble des séries formelles, convergentes dans une voisinage de 0. Dans ce cas l'algèbre $\mathcal{G}$ est l'algèbre des germes d'opérateurs différentiels analytiques. On remarque (voir [Sab 90]) que pour ce genre d'algèbres on a un résultats encore plus fort sur la structure des idéaux à gauche en analysant bien leurs bases standard: Tout idéal à gauche est engendré par les deux éléments (ou par l'unique élément) d'une base standard de degré maximal et minimal en d.

Exemple 5. Pour des opérateurs à différences on a des résultats semblables aux opérateurs différentiels. Il faut cependent prendre quelques précautions.

Considérons par exemple l'algèbre à gauche $\mathcal{G} = K[z, \delta]$, avec $\delta z = z^2\delta$. Cette algèbre à gauche n'est pas noethérienne, car l'idéal à gauche $(z\delta, z\delta^2, \cdots)$ n'est pas finiment engendré. Effectivement, quand on considère l'ordre lexicographique naturel $\leq$ sur $S = \{z^n\delta^m\}_{n,m\in\mathbb{N}}$, on s'apperçoit que l'ordre de divisibilité $\preceq$ n'est pas un belordre à cause de l'antichaîne infinie $z\delta, z\delta^2, \cdots$. On se demande d'ailleurs si cette situation est générale (c.à.d. si $\mathcal{G}$ est noethérien, est-ce qu'il existe S et $\leq$ pour lesquels $\preceq$ est un belordre).

La condition (c) de la compabilité avec la multiplication n'est pas nécessairement vérifiée non plus, si A n'est pas un corps. Considérons par exemple $\mathcal{G} = A[\delta] = \mathbb{Z}[z][\delta]$, avec $\delta z = 2z\delta$. Alors $\mathcal{G}$ n'est pas noethérienne, car l'idéal à gauche $(z\delta, z\delta^2, \cdots)$ n'est à nouveau pas finiment engendré.

Considérons maintenant $\mathcal{G} = \mathbb{Q}[z, \circ_{z+1}]$. Ceci est une algèbre de Gröbner algorithmique. De même $\mathbb{Q}(z)[\circ_{z^2}]$ est une algèbre de Gröbner algorithmique, bien qu'il

n'en est pas de même pour $\mathbb{Q}[z, \circ_{z^2}]$.

Remarque. Dans le cas particulier où on considère l'algèbre $\mathcal{G} = K[\star]$, où $\star$ est soit une indéterminé, soit un opérateur différentiel ou autre, on peut remarquer que la division par rapport à un élément de $\mathcal{G}$ est une sorte de division Euclidienne. Effectivement, le théorème 1 donne que pour tout $X, Y \in \mathcal{G}$ il existe d'uniques $Q, R \in \mathcal{G}$, tels que $Y = QX + R$, avec $M(R) < M(X)$ (c.à.d. $deg(R) < deg(X)$). Il s'en suit que $\mathcal{G}$ est principal. Il existe donc des pgcds et des ppcms dans $\mathcal{G}$ et on peut les calculer, lorsque K est algorithmique. L'algèbre à gauche $K(z)[\circ_{z^2}]$ de tout à l'heure est par exemple principale.

Exemple 6. Dans les exemples précédents, l'ordre partiel de divisibilité est chaque fois isomorphe à l'ordre partiel produit sur $\mathbb{N}^n$. Ceci n'est pas nécessairement le cas, comme on voit en considérant $\mathcal{G} = \mathbb{Q}[X^2, Y^2, XY]$. Néanmoins, nous avons l'impression que l'ordre partiel de divisibilité d'une algèbre de Gröbner est chaque fois un sous ordre partiel de l'ordre partiel produit sur $\mathbb{N}^n$. Cet exemple est quand même à garder en tête lorsqu'on classifie les algèbres de Gröbner. Effectivement, en imposant des lois de commutation non commutatives entre X^2, Y^2 et XY, on peut fabriquer des algèbres, qui ne sont pas sous algèbre de $\mathbb{Q}[X, Y]$, pour n'importe quelles lois de commutation qu'on a imposées sur X et Y.

Exemple 7. Soient ζ et ζ' deux éléments non collinéaires avec 0 dans $\mathbb{C}$ et δ et δ' les opérateurs à différences avec $\delta z = z + \zeta$ et $\delta' z = z + \zeta'$. Alors l'algèbre à gauche $\mathcal{G} = \mathbb{C}(z)[\delta, \delta']$ est une algèbre de Gröbner. On peut notamment se demander quel est l'ensemble de zéros $Z(I)$ (voir l'exemple 1.5) d'un idéal à gauche I de $\mathcal{G}$ dans l'ensemble des fonctions méromorphes sur $\mathbb{C}$.

2.6 Références

[Buch 65] B. Buchberger
Ein algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem null-dimensionalen Polynomideal.
Ph.D. Thesis, University of Innsbruck.

[Buch 85] B. Buchberger
An algorithmic method in polynomial ideal theory.
In: N. Bose (ed.), *Multidimensional Systems Theory*, 184-232. Reidel Publication Company, Dordrecht.

[**Car 91**] P. Cartier.
Démonstration automatique d'identités et fonctions hypergéométriques (d'après D.Zeilberger).
Séminaire Bourbaki, 44-ième année, No. 746.

[**Cohn 65**] R.M. Cohn
Difference algebra.
Interscience publications, Tracts in Mathematics, No. 17.

[**Giu 88**] M. Giusti.
Combinatorial dimension theory of algebraic varieties.
Journal of Symbolic Computation 6, 249-265.

[**Hir 64**] H. Hironaka.
Resolution of singularities of an algebraic variety over a field of characteristic zero: I, II.
Annals of Mathematics 79, 109-326.

[**Kol 73**] E.R. Kolchin.
Differential algebra and algebraic groups.
Academic press, Pure and Applied Mathematics, Vol. 54.

[**Krus 72**] J.B. Kruskal
The theory of zell-quasi-ordering: a frequently discovered concept.
Journal of combinatorial theory.

[**Lang 84**] S. Lang
Algebra.
Addison Wesley.

[**PR 81**] M. Pouzet, I. Rival.
Which ordered sets have a complete linear extension.
Canadian Journal of Mathematics 33, 1245-1254

[**Ritt 32**] J.F. Ritt.
Differential equations from the algebraic standpoint.
American Mathematical Society Colloquium Publications, Vol. 14.

[**Sab 90**] C. Sabbah.
Introduction to algebraic theory of linear systems of differential equations.
Lecture given at the CIMPA summer school in august 1990..

[**Zach 78**] G. Zacharias.
Generalised Gröbner Bases in commutative polynomial rings.
Bachelor Thesis, M.I.T.

Chapter 3

Sur certains produits infinis

3.1 Introduction

Dans ce chapitre on étudie l'asymptotique des produits de la forme

$$f(z) = \prod_{k=0}^{\infty} \frac{1}{1 - z^{2^k}/a}$$

Cette fonction vérifie l'équation mahlérienne suivante:

$$f(z^2) = (1 - z/a)f(z), \quad \text{où } a \neq 0 \text{ et } f(0) = 1,$$

L'étude de cette équation est importante, car toute suite mahlérienne est produit de convolution de suites mahlériennes relevant de cette équation et d'une suite régulière (voir [Dum 93]). On montre que le comportement du n-ième coefficient de Taylor $f_n = [z^n]f(z)$ dépend essentiellement du module de a. Si le module de a est inférieur à 1, l'analyse des f_n est facile; $f(z^2)$ étant analytique pour $|z| < \sqrt{a}$, on a:

$$f_n \sim \frac{f(a^2)}{a^n}.$$

En revanche le cas $|a| \geq 1$ donne lieu à des comportements très divers. Dans la quatrième section on montre que pour toute "bonne" fonction h, avec $x \prec h(x) \preceq x \lg x$, il existe un a de module 1, tel que $\lg |\hat{f}_n| \asymp h(\lg n)$; ici $\lg x = \log_2 x$ et $\hat{f}_n = \max_{1 \leq i \leq n} |f_i|$. En fait, le comportement des f_n dépend essentiellement du développement en binaire de $\arg a/2\pi$. Enfin, pour $|a| \geq 2$, les f_n restent bornées, mais se comportent de façon extrêmement chaotique. Il y a donc peu de chance que le comportement des f_n rentre dans une échelle asymptotique habituelle.

3.2 Encadrements de lg $\hat{f}_n$

Fixons d'abord quelques notations. On rappelle qu'on note $\lg z = \log_2 z$ et $\hat{f}_n = \max_{1 \leq i \leq n} |f_i|$. Pour z et z' de module 1, on note par $\mathrm{d}(z, z')$ leur distance sur le

cercle unité divisé par 2π.

Pour tout $0 < r < 1$ l'inégalité triangulaire nous donne alors:

$$|1 - rz| \leq |1 - z| + 1 - r \leq 2\pi \mathrm{d}(1, z) + 1 - r.$$

En utilisant la concavité de lg on obtient alors:

$$-\lg |1 - rz| \geq \min(-\lg \mathrm{d}(1, z), -\lg(1 - r)) - 4. \tag{3.1}$$

Puis on a pour $z = e^{2\pi i\alpha}$ et $|\alpha| \leq 1/2$:

$$|1 - rz|^2 - (2\mathrm{d}(1, z))^2 =$$

$$1 + r^2 - 2r\cos(2\pi\alpha) - 4\alpha^2.$$

On vérifie aisément que cette expression est toujours positive. On obtient donc:

$$|1 - rz| \geq 2\mathrm{d}(1, z) \Rightarrow$$

$$-\lg |1 - rz| \leq \min(-\lg \mathrm{d}(1, z), -\lg(1 - r)). \tag{3.2}$$

Dans un premier temps on va essayer de minorer $\lg |f(ra)|$, pour $r = 1/2^{1/2^n}$:

$$\lg |f(ra)| = \sum_{k=0}^{\infty} -\lg \left|1 - \frac{a^{2^k-1}}{2^{2^k-n}}\right| \geq \sum_{k=0}^{n-1} -\lg \left|1 - \frac{a^{2^k-1}}{2^{2^k-n}}\right|.$$

Puis, d'après l'inégalité (1):

$$\lg |f(ra)| \geq \sum_{k=0}^{n-1} \min \left\{ -\lg \mathrm{d}(1, a^{2^k-1}), -\lg \left(1 - \frac{1}{2^{2^k-n}}\right)\right\} - 4n.$$

Or, comme

$$\begin{aligned} \lg \left(1 - \frac{1}{2^{2^{-x}}}\right) &= \lg \left(1 - e^{-(\ln 2)2^{-x}}\right) \\ &= \lg \left((\ln 2)2^{-x} + O(2^{-2x})\right) \\ &= \lg \ln 2 - x + O(2^{-x}), \end{aligned}$$

il existe des constantes C_1 et C_2 tel que pour $k < n$:

$$C_1 + k - n < \lg \left(1 - \frac{1}{2^{2^k-n}}\right) < C_2 + k - n, \tag{3.3}$$

d'où on tire enfin:

$$\lg |f(ra)| \geq A_n + O(n), \text{ où:} \tag{3.4}$$

$$A_n \stackrel{\text{déf}}{=} \sum_{k=0}^{n-1} \min(\lfloor -\lg \mathrm{d}(a, a^{2^k})\rfloor, n-k).$$

Essayons de comprendre intuitivement ce que représente A_n. Si on développe $\arg a/2\pi$ en binaire, alors la quantité $\alpha_n \stackrel{\text{déf}}{=} \lfloor -\lg \mathrm{d}(a, a^{2^n})\rfloor$, qu'on appelle le n-ième autocorrélateur de a, mesure plus ou moins le nombre de chiffres en commun après la virgule entre ce développement et le même développement décalé de n chiffres vers la gauche (en convenant qu'on tient compte des irrégularités dues à $1,000\cdots \approx 0,111\cdots$). On mesure donc quelque chose comme le taux de réappararition des premiers chiffres de $\arg a/2\pi$ dans son développement binaire. Si ensuite on met dans un diagramme le nombre $d = \alpha_k$ en fonction de k, alors A_n représente le nombre de cases du diagramme en dessous de la ligne d'équation $d = n - k$ ce qui revient à "tronquer" le diagramme. On appelle A_n la série d'autocorrélation associée à a. Dans les figures 1.a et 1.b on montre les diagrammes associés à différentes valeurs de a.

Maintenant qu'on a donné un sens physique aux A_n, on peut affirmer que si $\arg a/2\pi$ est rationnel, son développement binaire est périodique à partir d'un certain rang, donc $A_n \sim cn$ ou $A_n \sim cn^2$. Dans ce cas on peut obtenir des estimations précises des f_n par la méthode de col (voir [Dum 93]). Sinon, pour que la formule (4) nous soit utile, il faut que $A_n \succ n$. C.à.d. il faut qu'il y ait suffisamment d'autocorrélation (ce qui par exemple n'est pas le cas si $a = -1$).

Dans un deuxième temps, on cherche à majorer $\lg|f(z)|$, pour $|z| = r$. Soit donc b de module 1. On a:

$$\lg|f(rb)| = \sum_{k=0}^{\infty} -\lg\left|1 - \frac{b^{2^k}}{a\,2^{2^{k-n}}}\right| \le \sum_{k=0}^{n-1} -\lg\left|1 - \frac{b^{2^k}}{a\,2^{2^{k-n}}}\right| + M, \text{ avec}$$

$$M = \sup_{|z|\le 1/2} \lg|f(z)|.$$

En utilisant (2) on obtient ensuite:

$$\lg|f(rb)| \le \sum_{k=0}^{n-1} \min\left\{-\lg \mathrm{d}(a, b^{2^k}), -\lg\left(1 - \frac{1}{2^{2^{k-n}}}\right)\right\} + M$$

et finalement, en utilisant (3):

$$\lg|f(rb)| \ge B_{b,n} + O(n), \text{ où:} \tag{3.5}$$

$$B_{b,n} \stackrel{\text{déf}}{=} \sum_{k=0}^{n-1} \min(\lfloor -\lg \mathrm{d}(a, b^{2^k})\rfloor, n-k).$$

Intuitivement $\beta_n \stackrel{\text{déf}}{=} \lfloor -\lg \mathrm{d}(a, b^{2^n})\rfloor$ mesure le nombre de chiffres en commun entre le développement en binaire de $\arg a/2\pi$ et $\arg b/2\pi$, décalé de n chiffres vers

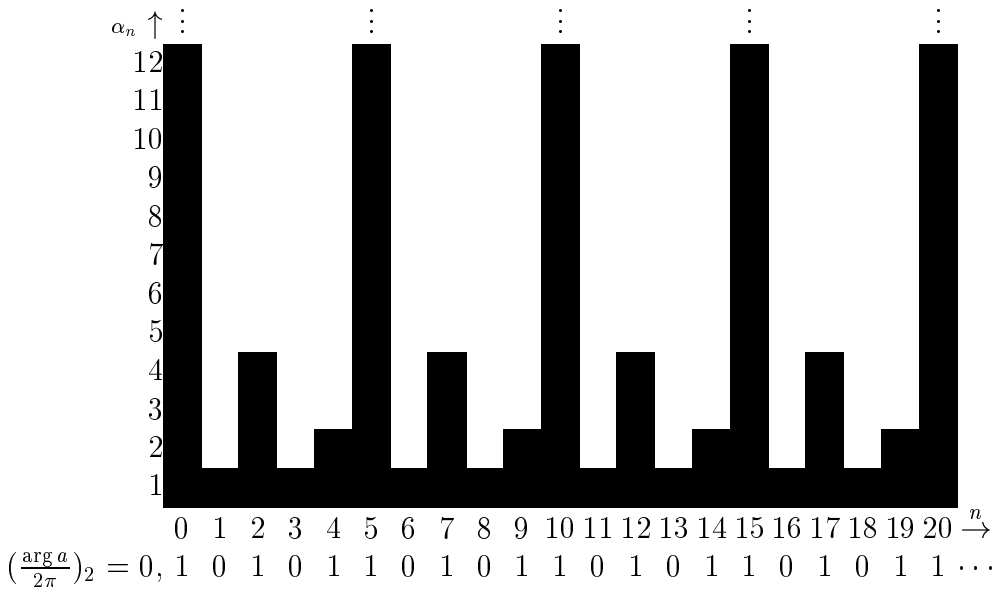

Figure 1.a: Comportement de α_n, pour a racine d'unité et où A_n a un comportement en Cn^2.

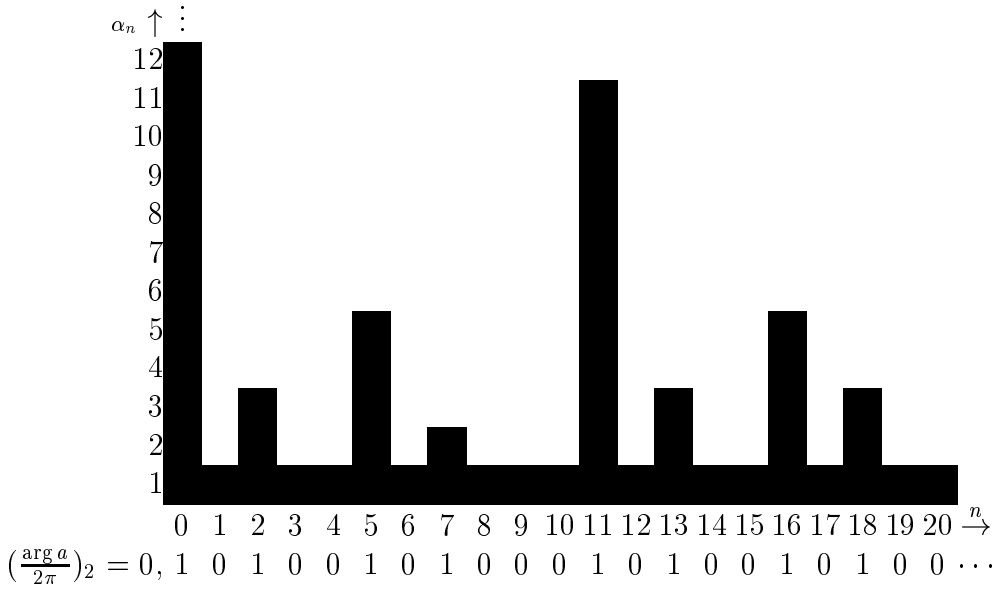

Figure 1.b: Comportement de α_n, pour un a tel que A_n a un comportement en $Cn \lg n$.

la gauche. Ceci implique que quand ce nombre est grand, alors $\beta_{n+\delta}$ est voisin de α_δ. Dans la section suivante, on utilisera cette remarque pour montrer que la seconde série d'autocorrélation $B_n \stackrel{\text{déf}}{=} \sup_{|b|=1} B_{b,n} \geq A_n$ est asymptotiquement équivalente à A_n.

Pour terminer, montrons maintenant comment obtenir un encadrement de $\lg \hat{f}_n$ à l'aide de (4) et (5).

Premièrement soit C_r le cercle de centre 0 et de rayon $r = 1/2^{1/n}$:

$$\begin{aligned} |f_n| &\leq \frac{1}{2\pi} \int_{C_r} \frac{|f(rz)|}{r^{n+1}} dz \\ &\leq 2^{B_{\lceil \lg n \rceil} + O(\lg n)} \cdot \frac{1}{r^n} \\ &= 2^{B_{\lceil \lg n \rceil} + O(\lg n)}. \end{aligned}$$

On en déduit la première inégalité pour $\lg \hat{f}_n$ en utilisant le fait que B_n est croissant:

$$\lg |f_n| \leq \lg \hat{f}_n \leq B_{\lceil \lg n \rceil} + O(\lg n). \tag{3.6}$$

Pour obtenir une inégalité dans l'autre sens, on supposera que:

- $A_n \sim B_n$,
- $n = o(A_n)$.
- $A_{n'} \leq A_n + M(n' - n) \lg n'$ pour un certain M et tout $n' > n \geq 1$.

Dans la section suivante on donne des conditions impliquant ces hypothèses.

D'après l'inégalité (4), on a pour $r = 1/2^{1/n}$:

$$2^{A_{\lfloor \lg n \rfloor} + O(\lg n)} \leq |f(ra)| \leq \sum_{k=0}^{\infty} |f_k| r^k \leq \sum_{k=0}^{\infty} \frac{\hat{f}_n}{2^{k/n}} = \hat{f}(r).$$

On en déduit en particulier que $\lg n = o(\lg \hat{f}_n)$ (sinon $\hat{f}(r)$ est à croissance polynomiale en n contrairement à $2^{A_{\lfloor \lg n \rfloor}}$. Posons maintenant:

$$\varphi(n) = \sup_{k \geq n} \frac{\lg \hat{f}_k}{A_{\lfloor \lg k \rfloor}} A_{\lfloor \lg n \rfloor}.$$

On a clairement $\lg n \prec \lg \hat{f}_n \leq \varphi(n) \prec A_{\lfloor \lg n \rfloor}$. De plus, si n est suffisamment grand, on a pour tout $k \geq 4n\varphi(n)$:

$$\begin{aligned}
\varphi(k) &\leq \sup_{l \geq k} \frac{\lg \hat{f}_l}{A_{\lfloor \lg l \rfloor}} A_{\lfloor \lg k \rfloor} \\
&\leq \sup_{l \geq n} \frac{\lg \hat{f}_l}{A_{\lfloor \lg l \rfloor}} (A_{\lfloor \lg n \rfloor} + M(\lg \frac{k}{n} + 1) \lg \lg k) \\
&\leq \varphi(n) + 2M(\lg \frac{k}{n} + 1) \lg \lg k \\
&\leq \frac{k}{4n} + 3M \lg \frac{k}{n} \lg(\lg \frac{k}{n} + \lg n) \\
&\leq \frac{k}{4n} + 3M \lg \frac{k}{n} \lg(\lg \frac{k}{n} + \frac{k}{n}) \\
&\leq \frac{k}{2n}.
\end{aligned}$$

On en déduit que:

$$\begin{aligned}
\sum_{k=\lfloor 4n\varphi(n) \rfloor}^{\infty} \hat{f}_k 2^{-\frac{k}{n}} &= \sum_{k=\lfloor 4n\varphi(n) \rfloor}^{\infty} 2^{\varphi(k) - \frac{k}{n}} \\
&\leq \sum_{k=\lfloor 4n\varphi(n) \rfloor}^{\infty} 2^{-\frac{k}{2n}} \\
&\leq \frac{1}{1 - 2^{-\frac{1}{2n}}} \\
&= O(n).
\end{aligned}$$

On a également:

$$A_{\lfloor \lg 4n\varphi(n) \rfloor} - A_{\lfloor \lg n \rfloor} \leq M \lceil \lg 4\varphi(n) \rceil \lg \lfloor \lg 4n\varphi(n) \rfloor = O(\lg n).$$

Ceci entraîne:

$$\begin{aligned}
2^{A_{\lfloor \lg(4n\varphi(n)) \rfloor} + O(\lg n)} &\leq 2^{A_{\lfloor \lg n \rfloor}} \\
&\leq \sum_{k=0}^{\infty} \hat{f}_k 2^{\frac{k}{n}} \\
&= \sum_{k=0}^{\lfloor 4n\varphi(n) \rfloor - 1} \hat{f}_k 2^{\frac{k}{n}} + \sum_{k=\lfloor 4n\varphi(n) \rfloor}^{\infty} \hat{f}_k 2^{\frac{k}{n}} \\
&\leq \lfloor 4n\varphi(n) \rfloor \hat{f}_{\lfloor 4n\varphi(n) \rfloor} 2^{4\varphi(n)} + O(n).
\end{aligned}$$

D'où finalement:

$$\begin{aligned}
A_{\lfloor \lg 4n\varphi(n) \rfloor} + O(\lg n) &\leq \lg \hat{f}_{\lfloor 4n\varphi(n) \rfloor} + 4\varphi(n) \\
&\leq 5\varphi(4n\varphi(n)).
\end{aligned}$$

On a donc:

$$\lg \hat{f}_n \asymp A_{\lfloor \lg n \rfloor}. \tag{3.7}$$

3.3 Sur les liens entre les deux séries d'autocorrélation

Dans toute cette section nous supposons que les conditions (C) suivantes sont vérifiés:

- $n = o(A_n)$.
- $\alpha_n = O(n)$.
- Pour tout $\lambda < 1$, il existe un N tel que

$$\forall n' \geq n \geq N \quad \frac{A_{n'}}{A_n} \geq \lambda \frac{n'}{n} \tag{3.8}$$

Intuitivement ceci veut dire qu'à la fois il y a suffisamment et pas trop d'autocorrélation et que A_n croît de façon "régulière". La deuxième condition entraîne l'existence d'une constante $C \geq 1$, telle que $\alpha_n \leq Cn$, pour tout $n > 0$. Fixons cette constante une fois pour toutes. Le but de cette section sera alors de d'établir le lemme 1 et le théorème 1. Combinant ces résultats avec ceux de la section précédente on obtient alors un encadrement de $\lg \hat{f}_n$, lorsque les conditions (C) sont vérifiées.

Remarquons tout d'abord que pour $0 < \delta < \beta_n$ et $\beta_{n+\delta} \leq \beta_n - \delta - 2$, (où on peut remplacer la condition $\beta_{n+\delta} \leq \beta_n - \delta - 2$ par $\alpha_\delta \leq \beta_n - \delta - 2$, menant de façon semblable au même résultat) on a:

$$\begin{aligned} \mathrm{d}(a, b^{2^n}) &\leq 2^{-\beta_n} \Rightarrow \\ \mathrm{d}(a^{2^\delta}, b^{2^{n+\delta}}) &\leq 2^{-(\beta_n - \delta)} \Rightarrow \\ |\mathrm{d}(a, b^{2^{n+\delta}}) - \mathrm{d}(a, a^{2^\delta})| &\leq 2^{-(\beta_n - \delta)} \end{aligned}$$

et comme $\mathrm{d}(a, b^{2^{n+\delta}}) \geq 2^{-(n-\delta-1)}$,

$$|\lg \mathrm{d}(a, b^{2^{n+\delta}}) - \lg \mathrm{d}(a, a^{2^\delta})| \leq 1 \Rightarrow$$

$$|\beta_{n+\delta} - \alpha_\delta| \leq 1. \tag{3.9}$$

Nous sommes maintenant en mesure de pouvoir démontrer le:

Lemme 1. *Avec les conditions (C), il existe M tel que pour tout $n' > n \geq 1$, on a:*

$$A_{n'} - A_n \leq M(n' - n) \lg n'.$$

Démonstration. Raisonnons par récurrence sur $n'-n$; il suffit de trouver un M, tel que $A_{n+1}-A_n \leq M\lg(n+1)$, pour tout $n \geq 1$. Or $A_{n+1}-A_n = \mathrm{Card}\{k \leq n | \alpha_k > n-k\}$. Soient alors $0 = n_0 < n_1 < \cdots < n_j \leq n$ les nombres tels que $\alpha_{n_i} > n - n_i$. Pour $0 \leq i \leq j$ et $\delta \leq (n-n_i-2)/(C+1)$, on a:

$$\alpha_\delta \leq C\delta \leq (n-n_i-2)(1-\frac{1}{C+1}) \leq n-n_i-2-\delta \leq \alpha_{n_i}-\delta-2.$$

Donc d'après (9), on a $\alpha_{n_i+\delta} \leq \alpha_\delta + 1$, d'où $\alpha_{n_i+\delta} \leq n-n_i-\delta$ et

$$n_{i+1}-n_i \geq \frac{n-n_i-2}{C+1}.$$

Par récurrence, il s'en suit que:

$$n_i \geq (1-\left(\tfrac{C}{C+1}\right)^i)(n-2).$$

En particulier:

$$n-3 \leq n_{j-3} \leq (1-\left(\tfrac{C}{C+1}\right)^{j-3})(n-2), \text{ d'où}$$

$$j-3 \leq \frac{\lg(n-2)}{\lg\left(\frac{C+1}{C}\right)}.$$

Alors $A_{n+1}-A_n = j \leq M'\lg(n+1)$, pour $M' = 2/\lg((C+1)/C)$ et tout n à partir d'un certain rang N. Pour finir, il suffit de poser

$$M = \max\left(M', \frac{A_2-A_1}{\lg 2}, \cdots, \frac{A_N-A_{N-1}}{\lg N}\right). \qquad \heartsuit$$

Lemme 2. *Soit b de module 1. Alors:*

$$B_{b,n} = \sum_{k=0}^{n-1} \min(\beta_k, nC) + O(n),$$

le terme d'erreur étant uniforme en b. En particulier dans le cas $\beta = \alpha$, on a:

$$A_n = \sum_{k=1}^{n-1} \alpha_k + O(n).$$

Démonstration. D'abord, posons $C' = 3C^2 + 11C + 5$. Ensuite raisonnons par récurrence. Plus précisément, supposons par récurrence qu'on ait l'inégalité suivante pour tout $n' < n$:

$$\sum_{k=1}^{n-1} \alpha_k - A_n \leq C'n'. \tag{3.10}$$

Alors montrons qu'on a l'inégalité pour $n' = n$ et donc pour tout n' par récurrence. Ceci nous donne le cas particulier du lemme. Par ailleurs, toujours sous l'hypothèse de récurrence, on montrera également que:

$$0 \leq \sum_{k=0}^{n-1} \min(\beta_k, Cn) - B_{b,n} \leq C'n.$$

Ceci achèvera bien la démonstration du lemme.

Fixons donc b de module 1. Comme pour $n = 0$ il n'y a rien à démontrer, on peut supposer que $n > 0$. Soient $0 \leq n_0 < n_1 < \cdots < n_j < n_{j+1} = n$ les nombres définis par

$$\begin{cases} n_0 = \min\{k \geq 0 \quad | \beta_k > n - k\} \\ n_1 = \min\{k > n_0 \quad | \beta_k > n - k\} \\ n_i = \min\{k > n_{i-1} | \beta_k > \beta_{n_{i-1}} - (k - n_{i-1}) - 2\} \text{ , pour } 2 \leq i \leq j. \end{cases}$$

Alors pour $\delta \leq (n - n_0 - 2)/(C + 1)$, on trouve $\alpha_\delta \leq n - n_0 - 2 - \delta \leq \beta_{n_0} - \delta - 2$. Puis en utilisant (9), on obtient $n_1 - n_0 \geq (n - n_0 - 2)/(C + 1)$. Ceci nous donne enfin:

$$n_1 \geq \frac{n-2}{C+1}.$$

Soit maintenant $1 \leq i \leq j - 1$. Pour $\delta < (\beta_{n_i} - 3)/(C + 1)$, on trouve $\alpha_\delta \leq \beta_{n_i} - 3 - \delta$ et en utilisant (9),

$$n_i - n_{i-1} \geq (\beta_{n_{i-1}} - 3)/(C + 1).$$

Puis encore à cause de (9), on a $|\beta_k - \alpha_{k-n_{i-1}}| \leq 1$, pour $n_{i-1} < k < n_i$. Il s'en suit que:

$$\begin{aligned} \sum_{k=n_{i-1}+1}^{n_i-1} \alpha_{k-n_{i-1}} + n_i - n_{i-1} &\geq \sum_{k=n_{i-1}+1}^{n_i-1} \beta_k \\ &\geq \sum_{k=n_{i-1}+1}^{n_i-1} \min(\beta_k, n - k) \\ &\geq \sum_{k=n_{i-1}+1}^{n_i-1} \min(\beta_k, n_i - k) \\ &\geq \sum_{k=n_{i-1}+1}^{n_i-1} \min(\alpha_{k-n_{i-1}}, n_i - k) - (n_i - n_{i-1}) \\ &= A_{n_i - n_{i-1}} - 2(n_i - n_{i-1}). \end{aligned}$$

Or, comme $n_i - n_{i-1} < n$, on a d'après (10):

$$\sum_{k=n_{i-1}+1}^{n_i-1} \alpha_{k-n_{i-1}} - A_{n_i-n_{i-1}} \leq C'(n_i - n_{i-1}). \tag{3.11}$$

Il s'en suit que:

$$\sum_{k=n_{i-1}+1}^{n_i-1} \beta_k - \sum_{k=n_{i-1}+1}^{n_i-1} \min(\beta_k, n-k) \leq (C'+3)(n_i - n_{i-1}).$$

Par ailleurs on avait montré $\beta_{n_i} - 3 < (C+1)(n_{i+1} - n_i)$, donc:

$$\begin{aligned}
\sum_{i=0}^{j} \beta_{n_i} &\leq \beta_{n_0} + \beta_{n_j} + (C+1)\left(\sum_{i=2}^{j-1} n_{i+1} - n_i\right) + 3(j+1) \\
&\leq \beta_{n_0} + \beta_{n_j} + (C+4)n \Rightarrow \\
\sum_{i=0}^{j} \min(\beta_{n_i}, Cn) &\leq (3C+4)n.
\end{aligned}$$

En rassemblant tous les morceaux, on obtient:

$$\begin{aligned}
0 \leq \sum_{k=0}^{n-1} \min(\beta_k, Cn) - B_{b,n} &= \sum_{i=0}^{j} \min(\beta_{n_i}, Cn) - (n - n_i) + \\
&\quad \sum_{i=1}^{j} \sum_{k=n_i+1}^{n_{i+1}-1} \min(\beta_k, Cn) - \min(\beta_k, n-k) \\
&\leq \sum_{i=0}^{j} \min(\beta_{n_i}, Cn) + \sum_{i=1}^{j} (C'+3)(n_{i+1} - n_i) \\
&\leq (3C+4)n + (C'+3)(n - n_1) \\
&\leq (3C+4)n + (C'+3)(1 - \frac{1}{C+1}))n + \frac{2}{C+1} \\
&\leq C'n.
\end{aligned}$$

En particulier, lorsque $b = a$, on obtient:

$$\sum_{k=1}^{n-1} \alpha_k - A_n \sum_{k=0}^{n-1} \min(\alpha_k, Cn) - A_n - Cn \leq C'n$$

Ceci est la relation (10), pour $n' = n$. ♡

Lemme 3. *Soit b de module 1. Il existe une suite $\{p_i\}$, avec des termes potentiellement infinis, telle que*

$$B_{b,n} = A_{p_0} + \cdots + A_{p_j} + A_r + O(n),$$

pour tout $n = p_0 + \cdots + p_j + r$, avec $1 \leq r \leq p_{j+1}$. De plus le terme d'erreur est uniforme en b.

Démonstration. Soit la suite $n_0 = 0 < n_1 < \cdots$ telle que pour tout $i \geq 1$, n_i soit le plus petit nombre plus grand que n_{i-1} et tel que β_{n_i} soit plus grand que $\beta_{n_{i-1}} - (n_i - n_{i-1})$. Montrons que la suite $\{p_i\}$ définie par $p_i = n_{i+1} - n_i$ convient. Reprenons les notations du lemme précédent. D'après (10), on a:

$$\begin{aligned} & A_{p_0} + A_{p_1} + \cdots + A_{p_j} + A_r = \\ = & \sum_{i=0}^{j-1} \sum_{k=1}^{p_i - 1} \alpha_k + \sum_{k=1}^{r-1} \alpha_k + O(n) \\ = & \sum_{i=0}^{j-1} \sum_{k=n_i+1}^{n_{i+1}-1} \alpha_{k-n_i} + \sum_{k=n_j+1}^{n-1} \alpha_{k-n_j} + O(n). \end{aligned}$$

Puis, remarquons que pour les mêmes raisons que dans la démonstration du lemme précédent, on a:

$$\beta_{n_i} - 3 \leq (C+1)(n_{i+1} - n_i) \text{ , d'où}$$

$$\sum_{i=0}^{j} \min(\beta_{n_i}, Cn) = O(n).$$

D'autre part, d'après (9), on a $|\beta_k - \alpha_{k-n_i}| \leq 1$, pour $n_i < k < n_{i+1}$ ou $n_j < k < n$. On en déduit:

$$\begin{aligned} B_{b,n} &= \sum_{k=0}^{n-1} \min(\beta_k, Cn) + O(n) \\ &= \sum_{i=0}^{j-1} \sum_{k=n_i}^{n_{i+1}-1} \min(\beta_k, Cn) + \sum_{k=n_j}^{n-1} \min(\beta_k, Cn) + O(n) \\ &= \sum_{i=0}^{j-1} \sum_{k=n_i}^{n_{i+1}-1} \min(\alpha_{k-n_i}, Cn) + \sum_{k=n_j}^{n-1} \min(\alpha_{k-n_j}, Cn) + \\ &\quad \sum_{i=0}^{j} \min(\beta_{n_i}, Cn) + O(n) \\ &= \sum_{i=0}^{j-1} \sum_{k=n_i+1}^{n_{i+1}-1} \alpha_{k-n_i} + \sum_{k=n_j+1}^{n-1} \alpha_{k-n_j} + O(n). \end{aligned}$$

Finalement on remarque que tous les termes d'erreur utilisés sont uniformes en b, d'où le lemme. ♡

Démontrons maintenant le théorème principal de cette section:

Théorème 1. *Lorsque les conditions (C) sont vérifiées, on a $A_n \sim B_n$.*

Démonstration. Supposons qu'on ait (8) pour certains λ et N. D'après le lemme 3 on peut écrire pour tout b de module 1:

$$B_{b,n} = A_{p_0} + \cdots + A_{p_j} + O(n),$$

pour certains nombres $p_0, \cdots, p_j$ de somme n. Alors:

$$B_{b,n} = \sum_{i,p_i<N} A_{p_i} + \sum_{i,p_i\geq N} A_{p_i} + O(n).$$

Or

$$\sum_{i,p_i<N} A_{p_i} \leq n \max_{0<k<N} \frac{A_k}{k} = O(n)$$

et d'autre part:

$$\sum_{i,p_i\geq N} \frac{A_{p_i}}{A_n} \leq \sum_{i,p_i\geq N} \frac{p_i}{\lambda n} \leq \frac{1}{\lambda}.$$

D'où:

$$\frac{B_{b,n}}{A_n} \leq \frac{1}{\lambda} + O(\frac{n}{A_n}) = \frac{1}{\lambda} + o(1).$$

Le terme reste étant uniforme en b, pour tout $\lambda' < \lambda$, on a donc à partir d'un certain rang:

$$B_n \leq \frac{1}{\lambda'} A_n.$$

Ceci étant vrai pour tout $\lambda < 1$, on a donc $A_n \sim B_n$. ♡

Remarque. Nous pensons qu'on a même la chose suivante: Lorsque les deux premières conditions de (C) sont vérifiées alors il y a équivalence entre la trosième proposition et la proposition $A_n \sim B_n$.

3.4 Sur la diversité de comportements possibles de lg $\hat{f}_n$

On dira qu'une fonction $h : \mathbb{R}^+ \to \mathbb{R}^+$ est régulière, si:

- $\bar{h}(x) = h(x)/x$ est croissante et tend vers l'infini.

– $\exists M\, \forall x' > x \quad \bar{h}(x') - \bar{h}(x) \leq M \lg \dfrac{x'}{x}$.

Remarquons que toute fonction régulière h vérifie nécessairement $x \prec h(x) \preceq x \lg x$. Si h est dérivable, alors la deuxième condition est notamment vérifiée si $\bar{h}'(x) \preceq 1/x$. En particulier toute fonction dérivable h telle que

$$\frac{1}{x \lg x} \preceq \bar{h}'(x) \preceq \frac{1}{x}$$

est régulière; Ceci nous permet d'associer injectivement une fonction régulière à chaque fonction continue asymptotiquement comprise entre $1/(x \lg x)$ et $1/x$.

Montrons maintenant comment on peut construire des a de module 1, tels que $\lg \hat{f}_n$ ait le même comportement que $h(\lg n)$, à un facteur constant près, étant donnée une bonne fonction h. Fixons d'abord quelques notations. Pour a de module 1, on pose

$$\frac{\arg a}{2\pi} = \sum_{i=1}^{\infty} \frac{a_i}{2^i}, \quad \text{avec } a_i \in \{0, 1\}.$$

Sinon pour a' de module 1, on définit A'_n, α'_n, etc. de la même façon que pour a. Démontrons tout d'abord quelques lemmes:

Lemme 4. *Soient a et a' de module 1 et N tel que $\mathrm{d}(a, a') \leq 2^{-N}$. Alors:*

(a) $|\alpha_k - \alpha'_k| \leq 1$, *pour tout k, tel que $\alpha_k \leq N - k - 3$.*
(b) $|A_n - A'_n| \leq 3n$, *pour tout $n \leq N$.*
(c) *Si* $\mathrm{d}(a, 1) \geq 2^{-(N-1)}$, *alors* $|\lg \mathrm{d}(a, 1) - \lg \mathrm{d}(a', 1)| \leq 1$.

Démonstration. Pour tout k, on a:

$$|\mathrm{d}(a, a^{2^k}) - \mathrm{d}(a', a'^{2^k})| \leq \mathrm{d}(a, a') + \mathrm{d}(a^{2^k}, a'^{2^k}) \leq 2^{k+1-N}.$$

En particulier, si $\alpha_k \leq N - k - 3$ (et de même si $\alpha'_k \leq N - k - 3$), alors:

$$\begin{aligned} & -\lg \mathrm{d}(a, a^{2^k}) \leq \alpha_k + 1 \leq N - (k+2) \Rightarrow \\ \Rightarrow \quad & \mathrm{d}(a, a^{2^k}) \geq 2^{k+2-N} \\ \Rightarrow \quad & |\lg \mathrm{d}(a, a^{2^k}) - \lg \mathrm{d}(a', a'^{2^k})| \leq 1 \\ \Rightarrow \quad & |\alpha_k - \alpha'_k| \leq 1. \end{aligned}$$

Il s'en suit que pour $n \leq N$:

$$|A_n - A'_n| \leq \sum_{k=0}^{n-1} |\min(\alpha_k, n-k) - \min(\alpha'_k, n-k)| \leq 3n.$$

Finalement (c) est trivial. ♡

Maintenant soit n un entier. On dira que (a, n) vérifie la propriété (P) ssi:

- $\forall k \geq n-(\alpha_n+3)\ \ a_k = 0.$
- $\forall 1 \leq k \leq n-(\alpha_n+3)\ \ \alpha_k \leq n-k-3.$
- $n \geq (\alpha_n+3)^2.$

Si (a,n) vérifie la propriété (P), définissons pour tout entier $p \geq 2$ le nombre $a' = \tau_{p,n}(a)$ de module 1 par $a'_k = a_{((k-1) \bmod n)+1}$, pour $k < pn$ et $a'_k = 0$, sinon. Calculons maintenant les α'_k, définis par cette transformation:

Lemme 5. *Si la paire (a,n) vérifie la propriété (P), alors les autocorrélateurs de $a' = \tau_{p,n}(a)$ vérifient les relations suivantes:*

(a)	*Pour $k < n-\alpha_n-3$,*	*on a $\lvert\alpha'_k - \alpha_k\rvert \leq 1$.*
(b)	*Pour $n-\alpha_n-3 \leq k < n$,*	*on a $\alpha'_k \leq \alpha_n+2$.*
(c)	*Pour $n \leq k < pk-\alpha_n-3, n\not\vert k$,*	*on a $\lvert\alpha'_k - \alpha'_{k \bmod n}\rvert \leq 1$.*
(d)	*Pour $n \leq k < pk-\alpha_n-3, n\vert k$,*	*on a $\lvert\alpha'_k - (pn-k)\rvert \leq \alpha_n+1$.*
(e)	*Pour $k \geq pn-\alpha_n-3$,*	*on a $\lvert\alpha'_k - \alpha_n\rvert \leq 1$.*

Démonstration. (a) découle directement du lemme précédent.

Puis pour $n-\alpha_n-3 \leq k \leq n$, soit a'' de module 1 tel que $\arg a'' = \arg a / 2^{n-k}$. Alors:

$$\lvert \mathrm{d}(a', a'^{2^k}) - \mathrm{d}(a, a'')\rvert \leq \mathrm{d}(a,a') + \mathrm{d}(a'', a'^{2^k}) \leq 2^{-(n-1)}.$$

Comme par ailleurs $\mathrm{d}(a,a'') = (1-2^{k-n})\mathrm{d}(a,1) \geq 2^{-(\alpha_n+1)} \geq 2^{-(n-2)}$, on a $\mathrm{d}(a', a'^{2^k}) \geq 2^{-(\alpha_n+2)}$, d'où (b).

Ensuite, on a $\alpha_n = \lfloor -\lg \mathrm{d}(a,1)\rfloor = \lfloor -\lg(\arg a/2\pi)\rfloor$. On en déduit que $a_k = 1$, pour un certain $k \leq \alpha_n+1$. Pour $n \leq k < pn-\alpha_n-3$, les développements en binaire de $\arg a'^{2^k}/2\pi$ et $\arg a'^{2^{k \bmod n}}/2\pi$ ont donc au moins $pn-k$ et au plus $pn+\alpha_n-k$ chiffres en commun au début. On en déduit:

$$2^{-(pn+\alpha_n+1-k)} \leq \mathrm{d}(a'^{2^k}, a'^{2^{k \bmod n}}) \leq 2^{-(pn-k)}.$$

Or dans le cas où $n\vert k$, ceci nous donne (d).

Dans l'autre cas, en utilisant

$$\begin{cases} \alpha'_{k \bmod n} \leq n - (k \bmod n) - 2 \leq pn-k-2, & \text{si } k \bmod n < n-\alpha_n-3 \\ \alpha'_{k \bmod n} \leq \qquad \alpha_n+1 \qquad \leq pn-k-2, & \text{sinon,} \end{cases}$$

on trouve (c).

Finalement, pour $k \geq pn-\alpha_n-3$, on trouve:

$$\lvert \mathrm{d}(a', a'^{2^k}) - \mathrm{d}(a, a^{2^n})\rvert = \lvert \mathrm{d}(a',1) - \mathrm{d}(a,1)\rvert \leq 2^{-n}.$$

Or $\mathrm{d}(a,1) \geq 2^{-(\alpha_n+1)} \geq 2^{-(n-1)}$, d'où (e). ♡

Corollaire 1. *La paire (a', n') vérifie la propriété (P), pour $n' \geq pn + \alpha_n + 4$.*

Démonstration. On a $|\alpha_n - \alpha'_{n'}| = ||\lfloor -\lg(a,1)\rfloor - \lfloor -\lg(a',1)\rfloor| \leq 1$, d'après le lemme 4(c). Ensuite toutes les conditions se vérifient trivialement. ♡

Corollaire 2. *On a $\alpha'_k \leq (p+1)k$, pour tout $k \geq n$.* ♡

Corollaire 3. *On a $\left|A'_{n'} - \left(qA_n + A_r + \frac{q^2}{2}\right)\right| \leq 10n'$, pour $n' = qn + r$, où $1 \leq q \leq p$ et $0 \leq r \leq n$.*

Démonstration. On a:

$$\begin{aligned} A_n &= n + \sum_{k=1}^{n-\alpha_n-4} \alpha_k + \sum_{k=n-\alpha_n-3}^{n-1} \min(\alpha_k, n-k), \\ A'_{n'} &= \sum_{q'=0}^{q-1} \left\{ \sum_{k=0}^{0} + \sum_{k=1}^{n-\alpha-4} + \sum_{k=\alpha_n-3}^{n-1} \right\} \min(\alpha'_{q'n+k}, n'-k) + \sum_{k=qn}^{qn+r-1} \min(\alpha'_n, n'-k). \end{aligned}$$

Or:

$$\begin{aligned} \sum_{k=n-\alpha_n-3}^{n-1} \min(\alpha_k, n-k) &\leq (\alpha_n+3)^2, \\ \left|\sum_{q'=0}^{q-1} \min(\alpha'_{q'n}, n'-k) - \frac{1}{2}q(r + \frac{q+1}{2}n)\right| &\leq q(\alpha_n+3), \\ \left|\sum_{q'=0}^{q-1} \sum_{k=1}^{n-\alpha_n-4} \alpha'_{q'n+k} - q \sum_{k=1}^{n-\alpha_n-4} \alpha_k\right| &\leq 2qn, \\ \sum_{q'=0}^{q-1} \sum_{k=n-\alpha_n-3}^{n-1} \min(\alpha'_{q'n+k}, n'-k) &\leq q(\alpha_n+3)^2, \\ \left|\sum_{k=qn}^{n'-1} \min(\alpha'_k, n'-k) - \sum_{k=0}^{r-1} \min(\alpha'_k, n-k)\right| &\leq 2r + 2(\alpha_n+3)^2. \end{aligned}$$

D'où le résultat en sommant et en utilisant $(\alpha_n+3)^2 \leq n$. ♡

Corollaire 4. *On a $\left|\bar{A}'_{n'} - \bar{A}_n - \frac{p}{2}\right| \leq \alpha_n + 14$, pour $n' = pn + \alpha_n + 4$.*

Démonstration. On a:

$$\begin{aligned} |\bar{A'}_{n'} - \bar{A}_{pn}| &\leq \left| \frac{A'_{pn}}{n'} - \frac{A'_{pn}}{pn} \right| + \frac{(\alpha_n + 4)(\alpha_n + 1)}{n'} \\ &\leq (\alpha_n + 4)\frac{A_{pn}}{pnn'} + 1 \\ &\leq \alpha_n + 3. \end{aligned}$$

On conclut en appliquant le corollaire précédent. ♡

On est maintenant en mesure de démontrer le théorème principal:

Théorème 2. *Soient a' de module 1, $\varepsilon > 0$ et h une fonction régulière. Alors il existe un a de module 1, tel que $|a - a'| < \varepsilon$ et $\lg \hat{f}_n \asymp h(\lg n)$.*

Démonstration. Quitte à remplacer a' par un nombre proche et à prendre n suffisamment grand, on peut supposer sans perdre de généralité qu'il existe un n tel que (a', n) vérifie la propriété (P) et $(2\pi)2^{-n} < \varepsilon$. Soit M une constante telle que

$$\forall x' > x \quad \bar{h}(x') - \bar{h}(x) \leq M \lg \frac{x'}{x}. \tag{3.12}$$

Posons $K = 2(M + \alpha'_n + 15)$. Encore sans perdre de généralité on peut supposer que n est suffisamment grand pour que $\bar{h}(n) \geq \bar{A'}_n + K$.

On va construire une suite $\{(a^{(i)}, n_i)\}$ de couples vérifiant la propriété (P) et telle que $a_k^{(i)} = a'_k$, pour tout i et $k < n$. On en déduit déjà $|\alpha'_n - \alpha_{n_i}^{(i)}| \leq 1$, pour tout i (comme dans dans la démonstration du corollaire 1). On prend $(\alpha^{(1)}, n_1) = (\tau_{n,p}(a'), np + \alpha'_n + 4)$, avec p minimal tel que $\bar{A}_{n_1}^{(1)} \geq \bar{h}(n_1) - K$. Un tel p existe, car le premier membre croît en p (corollaire 3) et le deuxième en $\lg p$ (à cause de (12)). Comme de plus $\bar{A}_{n_1}^{(1)} - \bar{A}_{n_1-p}^{(1')} \leq 2(\alpha_n + 14) + 1/2 \leq K$, pour $a^{(1')} = \tau_{n,p-1}$ et comme $\bar{h}$ est croissant, on a même $\bar{h}(n_1) - K \leq \bar{A}_{n_1}^{(1)} \leq \bar{h}(n_1)$.

Construisons les autres couples par récurrence. Fixons un P tel que $P \geq 2(2K + M \lg(P + 1))$ et supposons par récurrence que pour un certain $i \geq 1$ on ait:

$$\bar{h}(n_i) - K \leq \bar{A}_{n_i}^{(i)} \leq \bar{h}(n_i). \tag{3.13}$$

Alors on prend $a^{(i+1)} = \tau_{n_i,P}(a^{(i)})$ et n_{i+1} suffisamment grand pour que $(a^{(i+1)}, n_{i+1})$ vérifie la propriété (P) et pour qu'on ait la relation (13), pour $i + 1$ au lieu de i. Ceci est possible, car d'après le corollaire 3 et la choix de P, on a $\bar{A}_{n'_{i+1}}^{(i+1)} \geq \bar{h}(n'_{i+1})$, pour $n'_{i+1} = Pn_i + \alpha_{n_i}^{(i)} + 4$. Sinon, comme $\bar{h}(k) - \bar{A}_k^{(i+1)}$ tend vers l'infini, on peut prendre $n_{i+1} = \min\{k \geq n'_{i+1} | \bar{h}(k) \geq \bar{A}_k^{(i+1)}\}$. Finalement $|\bar{h}(n_{i+1}) - \bar{h}(n_{i+1} - 1)| + |\bar{A}_{n_{i+1}}^{(i+1)} - \bar{A}_{n_{i+1}-1}^{(i+1)}| \leq M + 1 \leq K$.

Alors soit a la limite des $a^{(i)}$ et montrons que a est le nombre désiré dans le théorème. D'après sa construction, on a $a_k = a_k^{(i)}$, pour tout i et $k < n_i$. Il s'en suit en particulier que $d(a, a') < 2^{-n}$, d'où $|a - a'| \leq \varepsilon$.

Puis posons $C = 2 + \max(\alpha_1^{(1)}/1, \cdots, \alpha_{n_1}^{(1)}/n_1, P)$. Montrons alors que $\alpha_k^{(i)} \leq Ck$, pour tout $i, k \geq 1$. Ceci est évident pour $i = 1$. Supposons donc $i \geq 2$. Si $1 \leq k < n_1$, on a $|\alpha_k^{(i)} - \alpha_k^{(1)}| \leq 1$, d'après le lemme 4(a). On en déduit $\alpha_k^{(i)} \leq Ck$. Si $n_{j-1} \leq k < n_j$, pour un certain $1 < j < i$, alors d'après le lemme 4(a), on a $|\alpha_k^{(i)} - \alpha_k^{(j)}| \leq 1$ et en utilisant le corollaire 2, on en déduit également $\alpha_k^{(i)} \leq (P+1)k + 1 \leq Ck$. Enfin, pour $k \geq n_i$, c'est encore le corollaire 2. Par passage à la limite on en tire $\alpha_k \leq (C+1)k$, pour tout $k \geq 1$.

Il nous reste finalement à montrer que $\bar{h}(k) \sim \bar{A}_k$; Effectivement, comme $\bar{h}$ est croissante, ceci implique que A_n est surlinéair de paramètre λ, pour tout $\lambda < 1$. On conclut en appliquant le théorème 1.

Posons $\mu_i = \max\{|\bar{h}(k) - \bar{A}_k| \mid n_{i-1} \leq k < n_i\}$, pour tout $i \geq 1$ et convenons que $n_0 = 1$. Soit $i \geq 2$ et $n_{i-1} \leq k < n_i$. Si $k \geq n_i'$, on a d'après la construction de $(a^{(i)}, n_i)$:

$$\bar{h}(n_i') \leq \bar{h}(k) \leq \bar{A}_k^{(i)} \leq \bar{A}_{n_i'}^{(i)}.$$

Sinon, si $Pn_{i-1} \leq k \leq n_i'$, on a:

$$|\bar{h}(k) - \bar{A}_k^{(i)}| - |\bar{h}(Pn_{i-1} - 1) - \bar{A}_{Pn_{i-1}-1}^{(i)}| \leq M + \alpha_n + 5.$$

En utilisant le lemme 4(b), on en déduit:

$$\mu_i \leq \max\{|\bar{h}(k) - \bar{A}_k| \mid n_{i-1} \leq k \leq Pn_{i-1}\} + M + \alpha_n + 17.$$

Finalement, supposons $k = qn_{i-1} + r$, avec $q < P$ et $r < n_{i-1}$. Pour un certain $j < i$, nous avons $n_{j-1} \leq r < n_j$. Alors en utilisant le lemme 4(b), le corollaire 3, (12) et (13), on a:

$$\begin{aligned}
|\bar{h}(k) - \bar{A}_k| &\leq |\bar{h}(k) - \bar{A}_k^{(i)}| + 3 \\
&\leq \left|\bar{h}(k) - \left(\frac{qn_{i-1}}{k}\bar{A}_{n_{i-1}}^{(i-1)} + \frac{r}{k}\bar{A}_r^{(i-1)}\right)\right| + \frac{P}{2n_{i-1}} + 13 \\
&\leq \left|\bar{h}(k) - \left(\frac{qn_{i-1}}{k}\bar{A}_{n_{i-1}}^{(i-1)} + \frac{r}{k}\bar{A}_r\right)\right| + P + 16 \\
&\leq \left|\bar{h}(k) - \left(\frac{qn_{i-1}}{k}\bar{h}(n_{i-1}) + \frac{r}{k}\bar{h}(r)\right)\right| + \frac{r}{k}\mu_j + P + K + 16 \\
&\leq \frac{r}{k}\mu_j + M\left(\frac{qn_{i-1}}{k}\lg\frac{k}{n_{i+1}} + \frac{r}{k}\lg\frac{k}{r}\right) + P + K + 16 \\
&\leq \frac{1}{2}\mu_j + M(\lg P + e\lg e) + P + K + 16.
\end{aligned}$$

Au total, nous obtenons donc:

$$\mu_i \leq \frac{1}{2}\max(\mu_1, \cdots, \mu_{i-1}) + Cte,$$

où la constante ne dépend pas de i. Mais ceci implique que les μ_i restent bornés, d'où $\bar{h}(k) \sim \bar{A}_k$, car $\bar{h}$ tend vers l'infini. ♡

3.5 Conclusion

Dans un certain sens la contribution de ce chapitre est négative; Effectivement, le théorème 2 montre l'inexistance d'un développement asymptotique général pour les suites mahlériennes. Ceci est une situation, qu'on ne rencontre pas très souvent pour des séries génératrices vérifiant une équation simple. Regardons donc l'intérêt de ce théorème dans un cadre plus large.

Considérons les fonctions g vérifiant une équation construite à partir de $g, z, +, \cdot, \hat{\circ}$, les constantes complexes (qu'on appelle les paramètres de l'équation) et éventuellement la dérivation. Ici on définit $\hat{\circ}$ par $a(z)\hat{\circ}b(z) = a(zb(z))$. Ce genre de fonctions couvre une très grande classe de fonctions relevant de la combinatoire et de l'analyse.

Or l'asymptotique de ce genre de fonctions est souvent miraculeusement simple. Jusqu'au présent, on a rencontré peu de types de comportements possibles. Ceci est dû au fait qu'on se trouve souvent dans le cas, où la plus petite singularité est isolée (souvent c'est même un pôle simple, comme dans le cas de f si $|a| < 1$). Mais même dans le cas où la plus petite singularité n'est pas isolée, comme par exemple dans le cas des arbres 2-3, où g vérifie l'équation

$$g(z) = g(z^2 + z^3) + z,$$

le comportement est encore assez "simple" et admet un équivalent exprimable dans une échelle habituelle (voir [Odl 82]). Ceci est dû au fait que la singularité principale est un point d'accumulation de singularités de module plus grand.

De plus, dans la plupart des cas, quand on modifie légèrement les paramètres dans l'équation de g, on trouve souvent un comportement "voisin". Plus précisément, le nombre de types de comportements qu'on peut obtenir en variant légèrement les paramètres est fini. En plus, dans le cas où le type ne change pas, les "paramètres du type" ne varient que légèrement.

Ce chapitre donne une exception à cette "règle". Effectivement on montre qu'il y a une infinité de comportements différents pour f_n, quand on fait varier a sur le cercle d'unité, même si on ne considère que des légères variations.

Dans le cadre que nous venons de fixer, l'équation de f est donc "singulière" dans un certain sens. Une question intéressante qui reste donc à étudier est de savoir à quel moment on se trouve dans une telle situation. Nous avons l'impression que la propriété essentielle distinguant ce cas du cas "normal" est que f admet un cercle de centre O comme frontière naturelle, si $|a| \geq 1$. On peut donc s'attendre à ce que

les équations suivantes soient également "singulières":

$$g(z^2) = (1-z)g'(z) + g(z)^2,$$

$$g(2z) = (1-z)g(z),$$

$$g(z^2) = (1-z)g(z)g(z^3), \cdots$$

On pourrait aussi étudier des produits du style:

$$g(z) = \prod_{k=0}^{\infty} \frac{1}{1-z^k/a}$$

En revanche les équations suivantes ne sont pas singulières:

$$g(z^2) = (1-z)g(z)g(z^2+z^5),$$

$$g(z) = zg(zg(z)) + z, \cdots$$

Néanmoins, même dans le cas des équations singulières, on peut souvent dire quelque chose quand même. Premièrement, si $|a| > \rho$, nous avons montré qu'on a un équivalent de $\hat{f}_n$. Pour $|a| > 1$ il y a d'ailleurs de bonnes chances de pouvoir obtenir également un équivalent simple de $\hat{f}_n$. En utilisant des fonctions un peu moins habituelles, comme la fonction "sommes des chiffres de n en base 2", on pourra peut-être même obtenir un équivalent de f_n. D'ailleurs le cas où on connaît un équivalent de $\hat{f}_n$, mais pas de f_n, est déjà plus fréquent en asymptotique.

Deuxièmement, en combinatoire, comme les séries génératrices ont normalement des coefficients réels et même entiers, a ne pourra pas prendre n'importe quelle valeur dans la pratique. En revanche, le théorème 2 montre bien, qu'il y a peu de chances de rencontrer des développements classiques pour $\hat{f}_n$, dès qu'on prend des nombres de module 1 pour a, qui ne sont pas racine d'unité.

3.6 Références

[Bru 48] N.G. de Bruyn.
On Mahler's partition problem.
Indagationes Math. 10, 210-220.

[Dum 93] P. Dumas.
Récurrences Mahlériennes, suites automatiques, études asymptotiques.
Thèse, Université de Bordeau.

[**ErRich 76**] P. Erdös, B. Richmond.
Concerning periodicity in the asymptotic behaviour of partition functions
Journal of the Australian Mathematical Society 21. (series A), 447-456.

[**Mah 40**] K. Mahler.
On a special functional equation.
Journal of the London Mathematical Society 15, 115-123.

[**Odl 82**] A.M. Odlyzko.
Periodic oscillations of coefficients of power series that satisfy functional equations.
Advances in Mathematics 44, 180-205.

Appendix A

Sur l'asymptotique des suites mahlériennes

A.1 Introduction

Comme nous le disions déjà dans la préface nous n'avons pas eu le temps de traiter en profondeur l'aspect asymptotique des suites mahlériennes, sauf dans le chapitre 3, où nous avons montré que certaines suites n'ont probablement pas de développement asymptotique classique. Dans cette appendice nous nous proposons de donner une idée des résultats obtenus par d'autres, par nous et des résultats à obtenir.

On viens d'indiquer qu'un traitement général de l'asymptotique des suites mahlériennes n'est sans doute pas faisable et est certainement loin d'être achevé de nos jours. En revanche, on a obtenu des résultats convenables pour d'assez grandes classes de suites et les méthodes utilisées peuvent se généraliser dans certains cas. Considérons d'abord l'équation de Mahler classique:

$$a_0(z)f(z) + \cdots + a_n(z)f(z^{2^n}) = b(z).$$

Le comportement des coefficients de Taylor f_n de $f(z)$ dépend essentiellement de $a_0(z)$. Si a_0 admet des racines à l'intérieur du cercle de rayon 1, on a juste une étude classique d'analyse de singularités à faire. Si les $|f_n|$ sont bornés par un polynôme en n, alors on peut utiliser la transformation de Mellin, ce qui donne même des solutions exactes dans certains cas. Dans ce cas où la suite mahlérienne $\{f_n\}$ est régulière, on a une représentation linéaire de la suite, ce qui entraîne non seulement que les $|f_n|$ sont bornés par un polynôme en n, mais ce qui nous donne également une majoration, voir même un équivalent de $\hat{f}_n$.

Le dernier cas, où les $|f_n|$ ne sont pas bornés par un polynôme en n (ce qui entraîne que a_0 admet au moins une racine de module 1) présente le plus de difficultés. Dans le chapitre 3 on a vu qu'il y a peu de chances de pouvoir donner un développement asymptotique classique dans le cas général. Si a_0 n'admet que des racines d'unités comme racines de module 1, on espère à nouveau pouvoir dire

quelque chose. On sait par exemple donner un développement asymptotique des produits infinis rencontrés dans le chapitre 3, lorsque a est racine d'unité (voir [Mah 40],[Bru 58] et [Dum 93]). Néanmoins, il sera souhaitable de généraliser ce résultat, car ceci permettra par exemple de faire des études statistiques plus élaborées sur le problème de partition de Mahler et autres.

Remarquons enfin qu'il faudrait également se poser le problème en fonction de quoi on veut obtenir des développements asymptotiques des suites mahlériennes. Le calcul asymptotique a été inventé pour rapidement pouvoir donner des bonnes approximations des valeurs prises par une suite f_n (ou autre) pour des grands n. Dans ce cadre on peut noter que les suites régulières sont en soi déjà des bonnes approximations d'elles-mêmes, car le temps de calcul de f_n est polynômial en $\lg n$ sur $\mathbb{C}$ et en $\lg n$ sur un corps fini. Néanmoins, cette observation ne donne pas de réponse à l'interdépendance entre le comportement asymptotique de différentes suites régulières et classiques. La question plus précise qu'on n'a pas encore résolue est la suivante: Est-ce qu'il existe un ensemble naturel de suites régulières, classiques et d'opérations, tel qu'on peut exprimer le comportement asymptotique de chaque suite régulière en fonction de ces suites en utilisant ces opérations? Bien entendu, après, nous nous posons la même question pour des suites mahlériennes et leurs généralisations.

A.2 Sur l'exploit de la transformation de Mellin

La possibilité d'utiliser la transformation de Mellin repose sur deux choses:

- Il faut que les $|f_n|$ soient bornés par un polynôme en n, pour que la série de Dirichlet
$$F(s) \stackrel{\text{déf}}{=} \sum_{n=1}^{\infty} \frac{f_n}{n^s}$$
converge à partir d'une certaine abcisse.
- Le fait que si $f(z) \to F(s)$, alors $f(z^k) \to F(s)/k^s$.

L'équation fonctionnelle de f se traduit alors en une équation fonctionnelle pour F, avec la seule précaution de supposer $f_0 = 0$ (ce qui n'est pas grave, comme le lecteur pourra vérifier). Ensuite, on applique la formule de Mellin-Perron pour trouver l'asymptotique d'une certaine itérée de la fonction sommatoire de $\{f_n\}$. Lorsque les $\{f_n\}$ se comportent de façon suffisamment lisse ou lorsqu'on peut appliquer ce procédé à une dérivée itérée de $\{f_n\}$, ceci nous donne l'asymptotique des $\{f_n\}$. Remarquons également que parfois, l'aspect formel de la transformation de Mellin suffit pour pouvoir obtenir des solutions exactes pour les coefficients $\{f_n\}$.

Exemple 1. Considérons l'équation de Mahler à coefficients constants et à second membre $P(z)/Q(z) \in \mathbb{C}(z)$:

$$a_0 f(z) + \cdots + a_n f(z^{2^n}) = \frac{P(z)}{Q(z)}. \tag{A.1}$$

On suppose que les racines de Q sont soit de module supérieur à 1, soit des racines d'unité. Comme l'équation est linéaire, on peut décomposer $P(Z)/Q(Z)$ en éléments simples et sans perdre de généralité, on peut supposer que $P(z)/Q(z)$ est soit de la forme z^k, soit de la forme $1/(1-az)^k$.

La suite $\{f_n\}$ est régulière et on peut donc appliquer la méthode. On obtient (où $G(s)$ est la transformée de $P(z)/Q(z)$):

$$\left(a_0 + \cdots + \frac{a_n}{2^{sn}}\right) F(s) = G(s).$$

A nouveau, on peut décomposer $1/(a_0 + \cdots + a_n 2^{-sn})$ en éléments simples et la solution générale de l'équation est donc une combinaison linéaire de fonctions qui vérifient des équations plus simples. Sans perdre de généralité on peut donc supposer que:

$$F(s) = \frac{G(s)}{(1-b2^{-s})^m}. \tag{A.2}$$

En retransformant cette équation dans l'autre sens, il est facile d'obtenir des solutions explicites. Ainsi, si $P(z)/Q(z)$ est juste un polynôme en z, nous obtenons:

$$f(z) = \sum_{n=0}^{\infty} b^n R(n) P(z^{2^n}),$$

pour un certain polynôme R. Supposons maintenant que $P(z)/Q(z) = 1/(1-az)^k$. Traitons d'abord le cas $l = 1$. On a la récurrence suivante pour les f_n:

$$\begin{cases} f_{2n} &= bf_n + a^{2n}, \\ f_{2n+1} &= a^{2n+1}. \end{cases}$$

Ceci conduit à l'expression explicite:

$$f_{2^k(2n+1)} = a^{2n+1} b^k \varphi(a,b)_k, \text{ où}$$

$$\varphi(a,b)_k = \sum_{j=0}^{k} \frac{a^{2^k}}{b^k}.$$

Si $|a| < 1$, $\varphi(a,b)_k$ converge trés vite, lorsque k tend vers l'infini. En revanche, à l'exception de la formule sommatoire, nous n'avons pas une expression à l'aide des

fonctions habituelles de $\varphi(a,b)_k$. Si a est une racine de l'unité, les a^{2^k} ne prennent qu'un nombre fini de valeurs. En regroupant, $\varphi(a,b)_k$ est alors combinaison linéaire de séries géométriques en k. Enfin, le cas $l > 1$ donne lieu à un peu plus de calculs, mais se traite fondamentalement de la même manière.

L'équation (2) peut également être utilisée pour obtenir le développement asymptotique des séries sommatoires de f_n (plus précisement des séries doublement sommatoires ou plus) en utilisant la formule de Mellin-Perron, pour $m \geq 1$ et c dans le demi-plan de convergence de $F(s)$ (voir [Fla+ 91]):

$$\frac{1}{m!}\sum_{k=1}^{n-1} f_k \left(1-\frac{k}{n}\right)^m = \frac{1}{2\pi}\int_{c-i\infty}^{c+i\infty} \frac{F(s)n^s ds}{s(s+1)\cdots(s+m)}.$$

De plus, du fait qu'on a une expression explicite pour $F(s)$, on obtient souvent des solutions exactes. En effet, si a est racine de l'unité, la transformée de $1/(1-az)^n$ est une série de Dirichlet qui s'exprime à l'aide de variantes de la fonction ζ de Riemann. Ensuite, on peut souvent se servir de la formule suivante pour obtenir des solutions exactes:

$$\int_{-\frac{1}{4}-\infty}^{-\frac{1}{4}+\infty} \zeta(s)n^s \frac{ds}{s(s+1)} = 0.$$

Le lecteur pourra par exemple vérifier que tous les exemples traités dans l'article [Fla+ 91], sauf l'exemple du nombre de nombres impairs dans le triangle de Pascal, sont fondés sur l'équation fonctionnelle (1).

Il y a un problème avec la transormation $f(z) \to F(s)$, lorsque les coefficients dans l'équation de Mahler ne sont plus nécessairement constants, ou lorsqu'on considère des équations diffdiffs plus générales, à cause du fait que si on connait la transformée de $f(z)$, on n'a a priori pas d'expression simple pour la transformée de $zf(z)$, ni pour celle de $f'(z)$. En revanche, nous pouvons écrire formellement:

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{f_n}{(n+1)^s} &= \sum_{n=1}^{\infty} \frac{f_n}{n^s}\left(1+\frac{1}{n}\right)^{-s} \\
&= \sum_{n=1}^{\infty}\sum_{k=0}^{\infty} \binom{-s}{k} \frac{f_n}{n^{s+k}} \\
&= \sum_{k=0}^{\infty} \binom{-s}{k} \sum_{n=1}^{\infty} \frac{f_n}{n^{s+k}} \\
&= \sum_{k=0}^{\infty} \binom{-s}{k} F(s+k).
\end{aligned}$$

On vérifie que cette écriture est justifiée, lorsque s est dans le demi-plan de convergence absolue de F et lorsque $f_1 = 0$, ce qu'on peut supposer sans perdre de

généralité (vérifiez le!). On a donc une expression en série pour la transformée de $zf(z)$ et il en est de même pour $f'(z)$, comme on vérifie aisément. Il s'en suit que si $f(z)$ vérifie une équation Mahlerienno-différentielle à coefficients polynômiaux et à second membre (et si $F(s)$ a un sens), alors on peut prolonger F analytiquement en se servant de la transformée de cette équation fonctionnelle. En particulier, on peut localiser ses singularités et, parfois, en tirer profit. Dans le cas d'une équation de Mahler, on retrouve par exemple le résultat que les singularités sont une réunion finie de demi-résaux, bandes verticales discrètes et points isolés (voir [AllCo 85]).

Exemple 2. Considérons l'équation

$$(1-az)f(z) = f(z^2),$$

avec $|a| < 1$. En transformant, on obtient:

$$(1-a)F(s) + R(s) = \frac{F(s)}{2^s}.$$

Grosso modo, on peut donc dire que f_n a un comportement en $n^{-\lg(1-a)-1}$, si $a > 1/2$ et que les f_n restent bornés sinon. Graphiquement, ceci semble effectivement être le cas, bien qu'il reste une étude plus fine à faire.

Exemple 3. Considérons l'équation suivante:

$$f(z) = (1+z)f(z^2) + (1+z+z^2)f(z^3) + (1+z+\cdots+z^5)f(z^6) - 2. \tag{A.3}$$

Cette équation est la traduction de la récurrence suivante (voir [Erd+ 87]):

$$\begin{cases} f_0 = 1, \\ f_n = f_{\lfloor \frac{n}{2} \rfloor} + f_{\lfloor \frac{n}{3} \rfloor} + f_{\lfloor \frac{n}{6} \rfloor}, \text{ pour } n \geq 1. \end{cases}$$

Pour faire l'asymptotique des f_n, il faut d'abord connaître la suite $\nabla\nabla f_n = f_n - 2f_{n-1} + f_{n-2}$, dérivée seconde de f_n. Le résultat de stabilité par addition du chapitre 2 entraîne que la série formelle associée à $\nabla\nabla f_n$ vérifie également une équation fonctionnelle du même type que (3). En appliquant notre méthode, on trouve alors que f_n tend vers une constante et en raffinant on peut même la calculer (on trouve $12/\ln 432$).

A.3 Autres méthodes et généralisations

La transformation de Mellin n'est pas la seule technique utile, lorsqu'on étudie des suites mahlériennes. Dans le cas du problème des paritions de Mahler (voir [Bru 58]), on utilse par exemple la transformation de Mellin, ainsi que la méthode de

col, pour faire une étude plus raffinée. Cette démarche se généralise d'ailleurs pour d'autres suites mahlériennes (voir [Dum 93]).

Par ailleurs, pour les suites régulières, on peut utiliser leurs représentations linéaires pour obtenir de l'information asymptotique. En particulier, ceci nous permet de voir directement, que les $|f_n|$ sont bornés par un polynôme en n. Dans sa thèse, Philippe Dumas donne également une méthode pour calculer un équivalent de $\hat{f}_n$, pour la plupart des suites régulières. Nous pensons que cette méthode pourra être légèrement amélioré, pour valoir en toute généralité.

Pour certains équations, il faut transformer l'équation afin de pouvoir appliquer la transformation de Mellin. Considérons par exemple l'équation suivante:

$$f(z) = (1+z)(f'(z^2) - f(z^2) + \frac{1}{1-z^2}.$$

Cette équation donne lieu à la récurrence:

$$\begin{cases} f_{2n} &= nf_n + 1, \\ f_{2n+1} &= nf_n. \end{cases}$$

Considérons maintenant la suite $h_n = f_n/g_n$, où g_n vérifie la récurrence:

$$\begin{cases} g_{2n} &= ng_n, \\ g_{2n+1} &= ng_n. \end{cases}$$

Alors nous obtenons la récurrence suivante pour h_n:

$$\begin{cases} h_{2n} &= h_n + \frac{1}{g_{2n}}, \\ h_{2n+1} &= h_n. \end{cases}$$

La transformée au sens de la section précédente de $1/g_{2n}$ est une fonction entière, car g_n croît comme $2^{\lg^2 n}$. Il s'en suit que les méthodes de la section précédentes s'appliquent à la nouvelle récurrence. Ceci est une situation assez générale lorsqu'on considère des équations Mahlerienno-différentiels. Nous ne savons pas s'ils existent des problèmes combinatoires ou des algorithmes naturels, qui donnent lieu à ce genre d'équations.

Enfin, il est clair que les suites mahlériennes se généralisent de beaucoup de façons. On vient de voir qu'on peut considérer des équations mixtes, avec l'opérateur de dérivation. On a également vu qu'on peut simultanément considérer des opérateurs du type $f(z) \to f(z^2)$ et $f(z) \to f(z^3)$, mais on pourrait ajouter tout opérateur de la forme $f(z) \to f(zg(z))$. On pourrait également considérer des équations en plusiers variables, des équations non linéaires, des systèmes d'équations, etc. Il reste donc du travail à faire pour la thèse.

A.4 Références

[**AllCo 85**] J.P. Allouche, H. Cohen.
Dirichlet series and curious infinite products.
Bulletin of the London Mathematical Society 17, 531-538.

[**AllSh —**] J.P. Allouche, J. Shallit.
Sums of digits and the Hurwitz zeta-function
Lecture notes in Mathematics 1434.

[**Bru 48**] N.G. de Bruyn.
On Mahler's partition problem.
Indagationes Math. 10, 210-220.

[**Dum 93**] P. Dumas.
Récurrences Mahlériennes, suites automatiques, études asymptotiques.
Thèse, Université de Bordeau.

[**Erd+ 87**] P. Erdös, A. Hildebrand, A. Odlyzko, P. Pudaite, B. Reznick.
The asymptotic behaviour of a family of sequences.
Pasific Journal of Mathematics, Vol. 126, No. 2, 227-241.

[**FlaGo 92**] P. Flajolet, M. Golin.
Mellin transforms and asymptotics: The mergesort recurrence.
Report 1498, Institut National de Recherche en Informatique et en Automatique (jan 1992). Communication given at *ICALP'93*.

[**Fla+ 91**] P. Flajolet, P. Grabner, P. Kirschenhofer, H. Prodinger, R. Tichy.
Mellin transforms and asymptotics: Digital sums. 23 pages.
INRIA research report, to appear in *Theoretical computer science.*

[**HwSt 93**] H.K. Hwang, J.M. Steyaert.
On the number of heaps.
Research Report LIX/RR/93/01, Ecole Polytechnique.

[**Mah 40**] K. Mahler.
On a special functional equation.
Journal of the London Mathematical Society 15, 115-123.

[**Odl 82**] A.M. Odlyzko.
Periodic oscillations of coefficients of power series that satisfy functional equations.
Advances in Mathematics 44, 180-205.

[**TitHB 86**] E.C. Titmarsh, D.R. Heath-Brown.
The theory of the Riemann zeta-function.
Oxford Science Publications, second edition.