



HAL
open science

Algébricité modulo p et structure de Frobenius forte

Daniel Vargas Montoya

► **To cite this version:**

Daniel Vargas Montoya. Algébricité modulo p et structure de Frobenius forte. Théorie des nombres [math.NT]. Université de Lyon, 2021. Français. NNT : 2021LYSE1143 . tel-03815107

HAL Id: tel-03815107

<https://theses.hal.science/tel-03815107>

Submitted on 14 Oct 2022

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

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



THESE de DOCTORAT DE L'UNIVERSITE DE LYON

opérée au sein de
l'Université Claude Bernard Lyon 1

Ecole Doctorale InfoMaths, ED 512

Spécialité : Mathématiques
N. d'ordre NNT : 2021LYSE1143

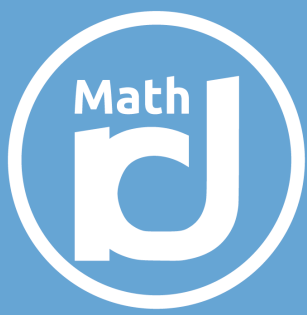
Soutenue publiquement le 13/07/2021 par :

Daniel Esteban Vargas-Montoya

Algébricité modulo p et structure de Frobenius forte

Devant le jury composé de :

M. Boris ADAMCZEWSKI	Directeur de Recherche CNRS, Université Lyon1	Directeur de Thèse
M. Jean-Paul ALLOUCHE	Directeur de Recherche Émérite CNRS, IMJ-PRG	Rapporteur
M. Frits BEUKERS	Full Professor Emeritus, Utrecht University	Rapporteur
M. Eric DELAYGUE	Maître de conférence, Université Lyon 1	Co-directeur de Thèse
Mme. Charlotte HARDOUIN	Maîtresse de conférence, Université Paul Sabatier	Examinatrice
M. Julien ROQUES	Professeur des Universités, Université Lyon 1	Examinateur
Mme. Masha VLASENKO	Professeure, Polish Academy of Sciences	Examinatrice
Mme. Reem YASSAWI	Lecturer, Open University	Examinatrice



Institut
Camille
Jordan

Laboratoire de recherche en mathématiques Lyon/Saint-Étienne

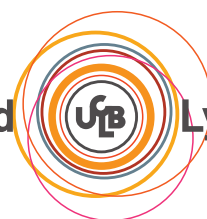
Algébricité modulo p et structure de Frobenius forte



Daniel Vargas-Montoya

Thèse de doctorat

Université Claude Bernard



Lyon 1

Remerciements

Table des matières

1	Introduction	1
1.1	Algébricité modulo p	1
1.2	Diagonales de séries rationnelles et algébriques	6
1.3	Les G -fonctions de Siegel	8
1.4	Résultats principaux, première partie	11
1.4.1	Structure de Frobenius forte	12
1.4.2	Éléments analytiques	12
1.4.3	Structure de Frobenius forte	13
1.4.4	Structure de Frobenius forte et algébricité modulo p	14
1.4.5	Structure de Frobenius forte et rigidité	15
1.4.6	Structure de Frobenius forte et équations hypergéométriques	18
1.5	Algébricité modulo p de G -fonctions et conjecture de Bombieri-Dwork.	20
1.6	Applications combinatoires arithmétiques de l'algébricité modulo p	22
1.6.1	Ensembles p -automatiques et congruences à la Lucas	22
1.6.2	Transcendance de séries formelles	28
1.6.3	Indépendance algébrique de G -fonctions	31
1.7	Résultats principaux, deuxième partie	33
1.7.1	Structure de Frobenius forte et congruences « à la Lucas »	33
1.7.2	Application à indépendance algébrique de G -fonctions	37
2	Structure de Frobenius forte et rigidité	39
2.1	Démonstration du théorème 1.4.6	39
2.2	Structure de Frobenius forte et rigidité	42
2.2.1	Opérateurs rigides et équations qui proviennent de la géométrie.	44
2.3	Démonstration du théorème 1.4.9	45
2.3.1	Disque non singulier et singulier régulier	46
2.3.2	Lemmes préparatoires.	49
2.3.3	Démonstration des pas	55
2.4	Démonstration du théorème 1.4.10 et 1.4.11	60
2.4.1	Démonstration du théorème 1.4.11	61
2.4.2	Démonstration du théorème 1.4.12	62
3	MUM, congruences « à la Lucas » et indépendance algébrique	63
3.1	Stratégie de la démonstration du théorème 1.7.6	63
3.2	Opérateurs différentiels	66
3.3	Un premier exemple	68
3.4	Démonstration du théorème 1.7.6	69
3.5	Démonstration du lemme 3.3.2	70
3.5.1	Démonstration du lemme 3.4.2	71

3.5.2	Démonstration de la proposition 3.5.2	72
3.5.3	Démonstration de la proposition 3.5.4	77
3.6	La série hypergéométrique ${}_2F_1(-1/2, 1/2, 1; 16z)$	91
3.7	Équations de Calabi-Yau	95
3.8	Indépendance algébrique	96
3.9	Démonstration du théorème 1.7.7	98
4	Structure de Frobenius forte pour les opérateurs aux q-différences	101
4.1	Motivation	101
4.1.1	Structure de Frobenius forte pour les opérateurs aux q-différences, une première motivation	102
4.1.2	Structure de Frobenius forte pour les opérateurs aux q-différences : arithmétique et spécialisation	103
4.2	Structure de Frobenius forte pour les opérateurs aux q-différences	106
4.3	Résultats principaux	113
4.3.1	Propositions auxiliaires	116
4.3.2	Démonstration du théorème 4.3.2	119
4.3.3	Réponse à la question 5	120
4.4	Question ouverte	121
4.5	Les travaux d'André et Di Vizio	121

Chapitre 1

Introduction

Le but de cette introduction est d'énoncer les résultats principaux de la thèse. Ces résultats sont divisés en deux parties qui correspondent aux parties 1.4 et 1.7. Nous dédions d'abord les parties 1.1, 1.2 et 1.3 à poser la problématique que nous allons étudier dans la partie 1.4. Les sujets traités dans ces parties sont l'algébricité modulo p , les diagonales de fractions rationnelles, les G -fonctions et la structure de Frobenius forte. Également, dans la partie 1.5 nous énonçons la conjecture de Bombieri–Dwork et montrons le lien entre cette conjecture et l'algébricité modulo p de G -fonctions. Ensuite, dans la partie 1.6 nous donnons quelques applications combinatoires et arithmétiques de l'algébricité modulo p . Les applications traitées portent sur les congruences « à la Lucas », les ensembles automatiques, la transcendance et l'indépendance algébrique de G -fonctions. Finalement, la partie 1.7 est consacrée à énoncer les résultats que nous avons obtenus concernant les congruences « à la Lucas » et l'indépendance algébrique de G -fonctions.

1.1 Algébricité modulo p

Nous commençons par rappeler les notions de série algébrique et de série holonome. Soient K un corps quelconque et $K[z]$ l'anneau de polynômes à coefficients dans K . Nous notons par $K(z)$ le corps de fractions rationnelles à coefficients dans K , c'est-à-dire $K(z) = \left\{ \frac{P(z)}{Q(z)} \text{ tels que } P(z), Q(z) \in K[z] \right\}$ et par $K[[z]]$ l'anneau des *séries formelles* à coefficients dans K , où

$$K[[z]] = \left\{ \sum_{n \in \mathbb{N}} a_n z^n \text{ tel que } a_n \in K \text{ pour tout } n \in \mathbb{N} \right\}.$$

Définition 1.1.1. On dit qu'un élément $f(z)$ de $K[[z]]$ est une *série algébrique* sur $K(z)$ s'il existe un polynôme $P(Y)$ non nul à coefficients dans $K(z)$ tel que $P(f(z)) = 0$. On dit que la série $f(z)$ est *transcendante* sur $K(z)$ si $f(z)$ n'est pas algébrique. Si la série $f(z) \in K[[z]]$ est algébrique sur $K(z)$, il existe un polynôme unitaire $P(Y)$ à coefficients dans $K(z)$ tel que $P(f(z)) = 0$ et si $R(z)$ est un autre polynôme à coefficients dans $K(z)$ tel que $R(f(z)) = 0$ alors $R(Y) = P(Y)T(Y)$. Le *degré d'algébricité* de $f(z)$, noté $\text{deg}(f)$, est le degré du polynôme $P(Y)$. Autrement dit, $\text{deg}(f)$ est la dimension de l'extension de corps $K(z)(f)$ sur $K(z)$.

Remarque 1.1.2. Nous attirons l'attention du lecteur sur le fait que nous utilisons deux notions distinctes de degré : le degré d'algébricité d'une série formelle sur $K(z)$ et la notion usuelle de degré pour un élément de $K[z]$. Ainsi, un élément $P(z) \in K[z]$ a un

degré d'algébricité égal à un en tant que série formelle car il annule le polynôme $Y - P(z)$, tandis que son degré en tant que polynôme de la variable z peut être différent.

Les séries algébriques sur $K(z)$ font partie d'une classe plus large de séries particulièrement étudiées : les *séries holonomes*. Avant de donner la définition d'une série holonome, rappelons, qu'étant donné un entier $j \geq 1$ et $f(z) = \sum_{n \geq 0} a(n)z^n \in K[[z]]$, la j -ième *dérivée formelle* de $f(z)$ est définie par

$$f^{(j)}(z) = \sum_{n \geq j} n(n-1) \cdots (n-j+1) a(n) z^{n-j}.$$

Définition 1.1.3. Soit K un corps quelconque. On dit qu'un élément $f(z) \in K[[z]]$ est une *série holonome* sur $K(z)$ s'il existe des polynômes $P_0(z), \dots, P_n(z) \in K[z]$, non tous nuls, tels que

$$P_0(z)f(z) + P_1(z)f'(z) + \cdots + P_n(z)f^{(n)}(z) = 0,$$

où $f^{(j)}(z)$ est la j -ième dérivée formelle de $f(z)$.

Nous notons \mathbf{Rat}_K l'ensemble des séries formelles à coefficients dans K qui appartiennent à $K(z)$, \mathbf{Alg}_K l'ensemble des séries formelles à coefficients dans K qui sont algébriques sur $K(z)$ et \mathbf{Hol}_K l'ensemble des séries formelles à coefficients dans K qui sont holonomes sur $K(z)$. On obtient alors la classification suivante :

$$\mathbf{Rat}_K \subset \mathbf{Alg}_K \subset \mathbf{Hol}_K.$$

Soient \mathbb{Z} l'anneau des entiers relatifs, \mathbb{Q} le corps des nombres rationnels et $\overline{\mathbb{Q}}$ le corps des nombres algébriques. Étant donné un nombre premier p , \mathbb{F}_p désigne le corps à p éléments et $\mathbb{Z}_{(p)}$ la localisation de \mathbb{Z} en l'idéal (p) , c'est-à-dire que $\mathbb{Z}_{(p)}$ est l'ensemble des nombres rationnels $\frac{a}{b}$ tel que a, b sont premiers entre eux et p ne divise pas b . Ainsi, nous pouvons réduire chaque élément de $\mathbb{Z}_{(p)}$ modulo p . Étant donné un nombre premier p et $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Z}_{(p)}[[z]]$, nous lui associons la série :

$$f|_p(z) = \sum_{n \geq 0} (a(n) \pmod{p}) z^n \in \mathbb{F}_p[[z]],$$

que nous appelons la *réduction modulo p* de $f(z)$.

Définition 1.1.4. Soient p un nombre premier et $f(z) \in \mathbb{Q}[[z]]$. Nous disons que $f(z)$ est *algébrique modulo p* si $f(z)$ appartient à $\mathbb{Z}_{(p)}[[z]]$ et $f|_p(z)$ est algébrique sur $\mathbb{F}_p(z)$.

Une observation simple mais importante est la suivante :

Remarque 1.1.5. Si $f(z) \in \mathbb{Q}[[z]]$ est algébrique sur $\mathbb{Q}(z)$ et que $f(z) \in \mathbb{Z}_{(p)}$, alors $f(z)$ est algébrique modulo p . En particulier, une série algébrique $f(z) \in \mathbb{Q}[[z]]$ est algébrique modulo p pour presque tout nombre premier p , c'est-à-dire à l'exception d'un ensemble fini de nombres premiers.

La contraposée de cette affirmation a pour conséquence le fait suivant : si $f|_p(z)$ est transcendante sur $\mathbb{F}_p[[z]]$ pour un nombre premier p , alors la série $f(z)$ est transcendante sur $\mathbb{Q}(z)$. Grâce au théorème de Christol (théorème D de la partie 1.6.1), on peut par exemple montrer que les séries formelles $\sum_{n \geq 0} z^{n^2}$ et $\sum_{n \geq 0} z^{2^n}$ sont transcendentes sur $\mathbb{Q}(z)$ car leurs réductions modulo 3 sont transcendentes sur $\mathbb{F}_3(z)$.

Néanmoins, l'affirmation faite dans la remarque 1.1.5 n'est pas une équivalence. En effet, considérons la série $f(z) = \sum_{n \geq 0} n!z^n \in \mathbb{C}[[z]]$. Cette série n'est pas algébrique

sur $\mathbb{Q}(z)$ car son rayon de convergence est nul. Par contre, pour tout nombre premier p , $f_p(z) = 1 + z + 2z + \dots + (p-1)!z^{p-1}$. Donc, $f_p(z)$ est un polynôme à coefficients dans \mathbb{F}_p de degré $p-1$ et par conséquent $f_p(z)$ est une série algébrique sur $\mathbb{F}_p(z)$ dont le degré d'algébricité est égal à un.

Considérons maintenant un exemple d'une autre nature. Soit $g(z)$ la série

$$g(z) = \sum_{n \geq 0} \binom{2n}{n}^2 z^n.$$

Le théorème de Lucas (théorème F de la partie 1.6.1) garantit que, pour tout entier n , pour tout nombre premier p et tout entier $m \in \{1, \dots, p-1\}$,

$$\binom{2(np+m)}{np+m}^2 \equiv \binom{2n}{n}^2 \binom{2m}{m}^2 \pmod{p}.$$

Cela implique que, pour tout nombre premier p ,

$$g_{|p} = \left(\sum_{n=0}^{p-1} \left(\binom{2n}{n}^2 \pmod{p} \right) z^n \right) g_{|p}(z^p). \quad (1.1)$$

Rappelons que pour toute série formelle $f(z)$ à coefficients dans \mathbb{F}_p , on a l'égalité fondamentale suivante :

$$f(z^p) = f(z)^p. \quad (1.2)$$

Comme $g_{|p}(z)$ est une série formelle à coefficients dans \mathbb{F}_p , il découle des égalités (1.1) et (1.2) que la série $g_{|p}(z)$ est algébrique pour tout nombre premier p . Par contre, la série $g(z)$ est transcendante sur $\mathbb{Q}(z)$, comme l'a remarqué Stanley [68].

Comme on le verra plus tard, la série $g(z)$ est une G -fonction tandis que ce n'est pas le cas de $f(z)$. Les G -fonctions ont été introduites par Siegel [66] dans son célèbre article de 1929. Elles forment une classe remarquable de séries holonomes à coefficients dans $\overline{\mathbb{Q}}$ et seront définies dans la partie 1.3. Cependant, ces deux séries formelles sont holonomes car

$$z^2 f''(z) + (3z-1)f'(z) + f(z) = 0 \quad \text{et} \quad z(1-16z)g''(z) + (1-32z)g'(z) - 4g(z) = 0.$$

Ainsi, nous avons deux séries à coefficients dans \mathbb{Z} qui sont holonomes et telles que, pour tout nombre premier p , leurs réductions modulo p sont algébriques sur $\mathbb{F}_p(z)$. Il existe de nombreux résultats de ce type dans la littérature. En outre, un résultat de Furstenberg [48] implique que si $f(z) \in \mathbb{Q}[[z]]$ est la diagonale d'une fraction rationnelle de plusieurs variables, alors la série $f(z)$ est algébrique modulo p pour presque tout p . Les diagonales des séries rationnelles et algébriques de plusieurs variables font l'objet de la partie 1.2 et, comme nous le verrons, ces dernières sont toujours holonomes. Cette situation nous conduit naturellement à nous poser la question suivante :

Question 1. Soient $f(z) \in \mathbb{Q}[[z]]$ un série holonome et p un nombre premier tel que $f(z) \in \mathbb{Z}_{(p)}[[z]]$. La série $f(z)$ est-elle algébrique modulo p ?

Rappelons que, pour tout nombre premier p , le degré d'algébricité de $f_p(z)$ est égal 1 car $f_p(z)$ est un polynôme et il suit de l'égalité (1.1) et (1.2) que le degré d'algébricité de $g_{|p}$ est inférieur ou égal à $p-1$. D'autre part, Sharif et Woodcock [65] ont montré que ce

dernier ne peut être majoré indépendamment de p . Etant donnée $f(z) \in \mathbb{Z}[[z]]$, obtenue comme diagonale d'une série algébrique, Deligne suggère dans [34] que le degré d'algébricité de $f|_p(z)$ sur $\mathbb{F}_p(z)$ est *au plus polynomial en p* , c'est-à-dire qu'il devrait exister un entier c , dépendant de $f(z)$ mais pas de p , tel que, pour presque tout nombre premier p , le degré d'algébricité de $f|_p(z)$ sur $\mathbb{F}_p(z)$ soit inférieur ou égal à p^c . Nous chercherons à étendre cette problématique au-delà du cas des diagonales de séries algébriques en nous posant la question suivante :

Question 2. Soient $f(z) \in \mathbb{Q}[[z]]$ une série holonome et \mathcal{S} un ensemble infini de nombres premiers tel que, pour tout $p \in \mathcal{S}$, $f(z) \in \mathbb{Z}_{(p)}[[z]]$. Supposons que la question 1 ait une réponse affirmative pour la série $f(z)$ et l'ensemble \mathcal{S} . Le degré d'algébricité de $f|_p$ peut-il être majoré par une fonction polynomiale du paramètre p ?

Pour finir, nous rappelons une troisième question importante. Remarquons d'abord que si $f(z)$ est algébrique de degré M sur $\mathbb{Q}(z)$ alors, pour presque tout nombre premier p , la série $f(z)$ est algébrique modulo p et $\deg(f|_p) = M$. Par contre, cette affirmation n'est pas une équivalence et la série $f(z)$ nous fournit un contre-exemple. En effet, pour tout nombre premier p , $f|_p(z)$ est algébrique et $\deg(f|_p) = 1$, alors que $f(z)$ est transcendante sur $\mathbb{Q}(z)$. Notre troisième question concernant l'algébricité modulo p est la suivante :

Question 3. Soit $f(z) \in \mathbb{Z}[[z]]$ une série holonome de rayon de convergence non nul. Supposons que pour presque tout nombre premier p , la série $f(z)$ est algébrique modulo p et qu'il existe un entier $M > 0$, indépendant de p tel que $\deg(f|_p) < M$. La série $f(z)$ est-elle algébrique sur $\mathbb{Q}(z)$?

Notons qu'une conjecture de van der Poorten [71] (la conjecture 3 de cette thèse) prédit que la réponse à question 3 devrait être positive lorsque la série formelle $f(z)$ est la diagonale d'une fraction rationnelle.

Remarque 1.1.6. Soient K un corps de nombres et ϑ_K l'anneau des entiers de K . Nous pourrions formuler les questions 1, 2 et 3 dans le cas où $f(z)$ est une série holonome à coefficients dans K . Étant un idéal premier \mathfrak{p} non nul de ϑ_K et $f(z) = \sum_{n \geq 0} a(n)z^n \in \vartheta_{K,\mathfrak{p}}[[z]]$, où $\vartheta_{K,\mathfrak{p}}$ est la localisation de ϑ_K en l'idéal \mathfrak{p} , nous pouvons considérer la réduction modulo \mathfrak{p} de la série $f(z)$ définie par

$$f|_{\mathfrak{p}}(z) = \sum_{n \geq 0} (a(n) \pmod{\mathfrak{p}}) z^n \in (\vartheta_{K,\mathfrak{p}}/\mathfrak{p})[[z]].$$

Soit p le nombre premier tel que $(p) = \mathfrak{p} \cap \mathbb{Z}$. Nous disons que la série $f(z) \in \vartheta_{K,\mathfrak{p}}[[z]]$ est *algébrique modulo p* si la série $f|_{\mathfrak{p}}(z)$ est algébrique sur $(\vartheta_{K,\mathfrak{p}}/\mathfrak{p})(z)$. Remarquons que le corps $\vartheta_{K,\mathfrak{p}}/\mathfrak{p}$ est une extension finie de \mathbb{F}_p .

Nous allons maintenant énoncer une conjecture attribuée à Grothendieck. Celle-ci est liée à la question 3, mais au lieu de considérer seulement une solution d'une équation différentielle, il s'agit d'en considérer une base. Avant d'énoncer cette conjecture nous rappelons qu'un opérateur différentiel d'ordre n à coefficients dans $K(z)$ est un élément de $K(z)[d/dz]$ de la forme

$$L := \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} + a_n(z), \quad (1.3)$$

où les $a_i(z)$ appartiennent à $K(z)$. Remarquons que pour presque tout idéal premier \mathfrak{p} non nul de ϑ_K , nous pouvons, pour chaque $i \in \{1, \dots, n\}$, réduire les coefficients de la

fraction rationnelle $a_i(z)$ modulo \mathfrak{p} . Nous notons $L_{\mathfrak{p}} \in \vartheta_{K,\mathfrak{p}}/\mathfrak{p}(z)[d/dz]$ l'opérateur obtenu après avoir effectué une telle réduction. Pour chaque idéal premier \mathfrak{p} non nul de ϑ_K , nous notons $\mathfrak{k}_{\mathfrak{p}}$ le corps ϑ_K/\mathfrak{p} .

Conjecture 1 (Conjecture de Grothendieck [51]). *Soient K un corps de nombres et L un opérateur différentiel d'ordre n à coefficients dans $K(z)$. Si pour presque tout idéal premier \mathfrak{p} de ϑ_K , l'opérateur différentiel $L_{\mathfrak{p}}$ a n solutions dans $\mathfrak{k}_{\mathfrak{p}}(z)$ linéairement indépendantes sur $\mathfrak{k}_{\mathfrak{p}}(z^p)$, alors l'opérateur L a une base de solutions formée d'éléments algébriques sur $K(z)$.*

Cette conjecture peut également s'énoncer de la façon suivante : si pour presque tout idéal premier \mathfrak{p} , $L_{\mathfrak{p}}$ a une \mathfrak{p} -courbure nulle, alors L a une base solutions algébriques sur $K(z)$.¹

La conjecture 1 a été démontrée pour les opérateurs d'ordre 1 (voir Honda [50, p.175]). Considérons par exemple l'opérateur différentiel $L = (1 - z)\frac{d}{dz} - 1/2$. Remarquons que pour tout nombre premier p différent à 2, l'opérateur différentiel L_p est bien défini. De plus, l'opérateur L_p a comme solution le polynôme non nul

$$1 + \sum_{n=1}^{p-1} ((1/2)(1/2 + 1) \cdots (1/2 + n - 1) \pmod{p}) z^n.$$

La conjecture 1 prédit donc que les solutions de L doivent être algébrique sur $\mathbb{Q}(z)$ et, en effet, l'opérateur L est annulé par la série

$$(1 - z)^{-1/2} = 1 + \sum_{n \geq 1} (1/2)(1/2 + 1) \cdots (1/2 + n - 1) z^n$$

qui est bien algébrique sur $\mathbb{Q}(z)$.

La conjecture 1 a également été démontrée par Katz [51] pour les opérateurs différentiels dits de *Picard–Fuchs* (à coefficients dans $\overline{\mathbb{Q}}(z)$). Le lecteur trouvera dans [10, Chap. II] la définition d'équation de Picard–Fuchs. Celles-ci jouent un rôle important de part leur origine géométrique. Nous rappelons brièvement comment elles sont obtenues. Soient K un corps et X la $K(z)$ -variété associée aux zéros communs des polynômes $P_0(z, Y), \dots, P_r(z, Y)$, où pour chaque $i \in \{0, \dots, r\}$, $P_i(z, Y)$ est un polynôme en la variable Y à coefficients dans $K(z)$. Un résultat profond de Grothendieck montre que si X est lisse et K un corps de caractéristique nulle, alors $H_{DR}^i(X)$, le i -ième groupe de cohomologie de De Rham algébrique de X , est un $K(z)$ -espace vectoriel de dimension finie muni d'une dérivation D_z en la variable z . Cette dérivation est appelée *connexion de Gauss–Manin*. Ainsi si ω est un élément de $H_{DR}^i(X)$, il existe $a_1(z), \dots, a_n(z) \in K(z)$, non toutes nulles, telles que

$$D_z^n(\omega) + a_1(z)D_z^{n-1}(\omega) + \cdots + a_{n-1}(z)D_z(\omega) + a_n(z)\omega = 0.$$

On dit alors que l'opérateur différentiel $\frac{d}{dz^n} + a_1(z)\frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z)\frac{d}{dz} + a_n(z) \in K(z)[d/dz]$ est un opérateur de Picard–Fuchs à coefficients dans $K(z)$. Toute équation différentielle associée à un tel opérateur est appelée équation de Picard–Fuchs.

Dans cette thèse, nous n'aborderons pas la question 3, ni la conjecture de Grothendieck, mais nous étudierons les questions 1 et 2. Nous verrons notamment qu'elles ont une réponse positive pour de nombreuses séries holonomes appartenant à la classe des G -fonctions.

1. La \mathfrak{p} -courbure de $L_{\mathfrak{p}}$ est définie de la façon suivante. Soit A la *matrice compagnon* de $L_{\mathfrak{p}}$ et définissons la suite de matrices $\{A_i\}_{i \geq 0}$ comme suit : $A_0 = Id_n$ la matrice identité, $A_1 = A$ et $A_{i+1} = \frac{d}{dz}A_i + A_iA$, alors la \mathfrak{p} -courbure de $L_{\mathfrak{p}}$ est la matrice A_p . Dire que la \mathfrak{p} -courbure de $L_{\mathfrak{p}}$ est nulle signifie donc que $A_p = 0$.

1.2 Diagonales de séries rationnelles et algébriques

Étant donné un corps K et un entier n strictement positif, on définit l'opérateur de diagonalisation $\Delta_n : K[[z_1, \dots, z_n]] \rightarrow K[[z]]$ par

$$\Delta_n \left(\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a(i_1, \dots, i_n) z_1^{i_1} \cdots z_n^{i_n} \right) = \sum_{j \geq 0} a(j, j, \dots, j) z^j.$$

Nous disons que $f(z) \in K[[z]]$ est la diagonale d'une fraction rationnelle s'il existe un entier n strictement positif et $g(z_1, \dots, z_n) \in K[[z_1, \dots, z_n]]$ tels que $f(z) = \Delta_n(g(z_1, \dots, z_n))$ et $g = \frac{P}{Q}$, où P et Q appartiennent à $K[z_1, \dots, z_n]$ et $Q(0, \dots, 0) \neq 0$. On pose $\mathfrak{D}_{K,n}$ l'ensemble des éléments de $K[[z]]$ qui peuvent être obtenus comme la diagonale d'une série rationnelle de n variables. Finalement, on pose

$$\mathbf{Diag}_K = \bigcup_{n \geq 2} \mathfrak{D}_{K,n}.$$

Une observation due à Furstenberg [48] et Deligne [34] montre que lorsque le corps de base est le corps de nombres complexes \mathbb{C} , le processus de diagonalisation correspond à une intégration. Plus précisément, si $f \in \mathfrak{D}_{\mathbb{C},n}$ et $f = \Delta_n\left(\frac{P(z_1, \dots, z_n)}{Q(z_1, \dots, z_n)}\right)$, alors

$$f(z) = \frac{1}{(2\pi i)^{n-1}} \int_{\mathcal{C}} \frac{P dz_1 \cdots dz_{n-1}}{Q z_1 \cdots z_{n-1}},$$

où \mathcal{C} est le cycle donné par $|z_1| = \cdots = |z_{n-1}| = \epsilon$, $z_1 \cdots z_{n-1} = \lambda$, où ϵ et $|\lambda|$ sont suffisamment petits pour que Q ne s'annule pas sur ce cycle. Ce cycle est dit cycle « évanescent ». Ainsi, le processus de diagonalisation peut être vu comme une « intégration formelle ».

La série $\mathfrak{g}(z)$ appartient à $\mathbf{Diag}_{\mathbb{Q}}$. En effet, considérons la fraction rationnelle donnée par $R(z_1, z_2, z_3, z_4) = \frac{1}{(1-z_1-z_2)(1-z_3-z_4)}$. Il se trouve que

$$R(z_1, z_2, z_3, z_4) = \sum_{(i_1, i_2, i_3, i_4) \in \mathbb{N}^4} \binom{i_1 + i_2}{i_1} \binom{i_3 + i_4}{i_3} z_1^{i_1} z_2^{i_2} z_3^{i_3} z_4^{i_4}. \quad (1.4)$$

Donc,

$$\Delta_4(R) = \sum_{n \geq 0} \binom{2n}{n} z^n = \mathfrak{g}(z).$$

Un deuxième exemple est la série $(1 - 4z)^{-1/2} = \sum_{n \geq 0} \binom{2n}{n} z^n$ qui est la diagonale de la fraction rationnelle

$$\frac{1}{1 - (z_1 + z_2)} = \sum_{(i_1, i_2) \in \mathbb{N}^2} \binom{i_1 + i_2}{i_1} z_1^{i_1} z_2^{i_2}.$$

Notons que la série $(1 - 4z)^{-1/2}$ est algébrique sur $\mathbb{Q}(z)$. Le fait que la série $(1 - 4z)^{-1/2}$ soit algébrique et appartienne à $\mathfrak{D}_{\mathbb{Q},2}$ n'est pas une coïncidence. En effet, il est montré dans [19, corollaire 13] que si K est un corps parfait, alors toute série algébrique sur $K(z)$ appartient à $\mathfrak{D}_{K,2}$ et dans [69, théorème 6.3.3] il est montré que si $f(z) \in \mathfrak{D}_{K,2}$ alors $f(z)$ est algébrique sur $K(z)$. Ainsi, lorsque K est un corps de caractéristique zéro, $\mathfrak{D}_{K,2}$ est précisément l'ensemble des séries algébriques sur $K(z)$. Par conséquent, $\mathbf{Alg}_{\mathbb{Q}} \subset \mathbf{Diag}_{\mathbb{Q}}$.

Par exemple, d'après [48, Proposition 2], si K est un corps quelconque et f est une série algébrique sur $K(z)$ tel que $P(z, f(z)) = 0$ et $(\partial P / \partial z_2)(0, 0) \neq 0$ alors f est la diagonale de la fraction rationnelle

$$z_2^2 \frac{\partial P}{\partial z_2}(z_1 z_2, z_2) / P(z_1 z_2, z_2).$$

De plus, il suit de la proposition 5 de [28] que $\mathbf{Diag}_{\mathbb{Q}} \subset \mathbf{Hol}_{\mathbb{Q}}$. Ainsi, nous obtenons la classification suivante :

$$\mathbf{Rat}_{\mathbb{Q}} \subset \mathbf{Alg}_{\mathbb{Q}} \subset \mathbf{Diag}_{\mathbb{Q}} \subset \mathbf{Hol}_{\mathbb{Q}},$$

qui affine celle de la partie précédente. Comme nous venons de le voir, $\mathbf{Diag}_{\mathbb{Q}}$ contient toutes les séries formelles à coefficients dans \mathbb{Q} qui sont algébriques sur $\mathbb{Q}(z)$. Mais il existe aussi des séries formelles transcendantales appartenant à $\mathbf{Diag}_{\mathbb{Q}}$, comme la série $\mathbf{g}(z)$. Par contre, pour chaque nombre premier p , la série $\mathbf{g}_{|p}(z)$ est algébrique sur $\mathbb{F}_p(z)$ et $\mathbf{g}_{|p}(z) \in \mathbf{Diag}_{\mathbb{F}_p}$ parce que $\mathbf{g}_{|p}(z)$ est la diagonale de la fraction rationnelle

$$R_{|p}(z_1, z_2, z_3, z_4) = \sum_{(i_1, i_2, i_3, i_4) \in \mathbb{N}^4} \left(\binom{i_1 + i_2}{i_1} \binom{i_3 + i_4}{i_3} \pmod{p} \right) z_1^{i_1} z_2^{i_2} z_3^{i_3} z_4^{i_4}.$$

Cette situation est un cas particulier d'un résultat du à Furstenberg [48] :

Théorème A (Furstenberg [48]). *Soit K un corps de caractéristique non nulle. Tout élément de \mathbf{Diag}_K est algébrique sur $K(z)$.*

Deligne a ensuite étendu le théorème A en montrant qu'il est encore valable pour les diagonales de séries algébriques. On dit que $f(z)$ est la diagonale d'une série algébrique s'il existe un entier n strictement positif et une série $g(z_1, \dots, z_n) \in K[[z_1, \dots, z_n]]$ algébrique sur $K(z_1, \dots, z_n)$ tels que $f = \Delta_n(g)$. Notons $\mathfrak{D}_{K,n}^{alg}$ l'image par Δ_n des séries qui sont algébriques sur $K(z_1, \dots, z_n)$ et $\mathbf{Diag}_K^{alg} = \bigcup_{n \geq 2} \mathfrak{D}_{K,n}^{alg}$.

Théorème B (Deligne [34]). *Soit K un corps de caractéristique non nulle. Tout élément de \mathbf{Diag}_K^{alg} est algébrique sur $K(z)$.*

Il est clair que, pour tout corps K , on a $\mathbf{Diag}_K \subset \mathbf{Diag}_K^{alg}$. D'après Denef et Lipshitz [35, Théorème 6.2], si $f(z) \in K[[z]]$ est la diagonale d'une série algébrique $g(z_1, \dots, z_n)$, alors il existe une série rationnelle R de $2n$ variables telle que f s'obtient également comme la diagonale de la fraction rationnelle R . Cela entraîne que $\mathbf{Diag}_K^{alg} \subset \mathbf{Diag}_K$ et ainsi $\mathbf{Diag}_K^{alg} = \mathbf{Diag}_K$. Les théorèmes B et A sont donc équivalents.

Comme l'a remarqué Deligne, une conséquence remarquable de ces deux théorèmes est la suivante : si $f \in \mathbb{Z}[[z]]$ est la diagonale d'une série algébrique à coefficients dans \mathbb{Z} , alors, pour tout nombre premier p , la série $f(z)$ est algébrique modulo p . Cela découle du fait que, pour tout entier $n \geq 1$, on a

$$\Delta_n \circ (\text{reduction mod } p) = (\text{reduction mod } p) \circ \Delta_n.$$

Notamment, le théorème B permet de répondre positivement à la question 1 lorsque la série $f(z) \in \mathbb{Q}[[z]]$ est une diagonale de série algébrique.

Montrons maintenant que la question 2 a aussi une réponse affirmative lorsque la série $f(z)$ appartient à $\mathbf{Diag}_{\mathbb{Q}}^{alg}$. Soit $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Q}[[z]]$ une diagonale de série algébrique à coefficients dans \mathbb{Q} . Le théorème B et la remarque précédente entraînent que, pour presque tout nombre premier p , la série $f(z)$ est algébrique modulo p . Deligne suggère dans [34] qu'il existe un entier c indépendant de p tel que $\deg(f_{|p}) < p^c$. De plus, il prouve qu'une telle constante existe dans le cas où $f(z)$ appartient à $\mathfrak{D}_{\mathbb{Q},2}^{alg}$. L'entier c obtenu par Deligne dépend de quantités géométriques associées à fz (voir [34, p. 140]). Plus récemment, Adamczewski et Bell [1] ont montré le résultat suivant qui répond positivement à la question de Deligne :

Théorème C (Adamczewski and Bell [1]). *Soit $g(z_1, \dots, z_n) \in \mathbb{Z}[[z_1, \dots, z_n]]$ une série formelle algébrique de degré² inférieur ou égal à d et de hauteur³ inférieure ou égale à h . Alors, il existe un entier c dépendant uniquement de d , n et h , tel que, pour tout nombre premier p , le degré d'algébricité de $\Delta_n(g)|_p$ est inférieur ou égal à p^c .*

Autrement dit, si $f(z) \in \mathbb{Z}[[z]]$ appartient à $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ alors il existe un entier c tel que, pour tout nombre premier p , $\deg(f|_p) < p^c$. De plus, ces auteurs montrent également qu'on ne peut, en général, espérer mieux qu'une majoration polynomiale en p . Grâce au théorème C, la question 2 a donc une réponse positive lorsque la série $f(z)$ est la diagonale d'une série algébrique.

Nous finissons cette partie en énonçant deux conjectures. Rappelons d'abord que si $f(z) \in \mathbb{Q}[[z]]$ appartient à $\mathbf{Diag}_{\mathbb{Q}}$ alors elle est *globalement bornée*, c'est-à-dire que le rayon de convergence de $f(z)$ est non nul dans \mathbb{C} et qu'il existe $a, b \in \mathbb{Z}$ tels que $af(bz) \in \mathbb{Z}[[z]]$ (voir proposition 5 de [28]).

Conjecture 2 (Christol [27, 28]). *Si $f(z) \in \mathbb{Q}[[z]]$ est holonome et globalement bornée alors $f(z)$ appartient à $\mathbf{Diag}_{\mathbb{Q}}$.*

D'après les théorèmes A et C, cette conjecture impliquerait une réponse positive aux questions 1 et 2 pour les séries holonomes qui sont globalement bornées.

Finalement, la conjecture suivante due à van der Poorten [71] prédit une réponse positive à la question 3 dans le cas des diagonales de séries rationnelles.

Conjecture 3 (van der Poorten [71]). *Soit $f(z) \in \mathbb{Z}[[z]] \cap \mathbf{Diag}_{\mathbb{Q}}$. S'il existe un entier M tel que, pour tout nombre premier p , $\deg(f|_p) \leq M$, alors $f(z) \in \mathbf{Alg}_{\mathbb{Q}}$.*

Notons que l'hypothèse que $f(z)$ soit la diagonale d'une fraction rationnelle est importante. En effet, rappelons que pour tout nombre premier p , $\deg(f|_p(z)) = 1$, alors que la série $f(z)$ est transcendante sur $\mathbb{Q}(z)$. La série $f(z)$ est bien holonome, mais elle n'est pas une diagonale de fraction rationnelle. Cela vient du fait, déjà mentionné, que f n'est pas une G -fonction, alors que les diagonales de fractions rationnelles sont des G -fonctions.

1.3 Les G -fonctions de Siegel

Les G -fonctions, introduites par Siegel [66] en 1929, forment une classe remarquable de séries formelles convergentes à coefficients algébriques et globalement bornées.

Définition 1.3.1. Une série formelle $f(z) = \sum_{\geq 0} a_n z^n \in \overline{\mathbb{Q}}[[z]]$ est une G -fonction s'il existe un nombre réel $C > 0$ tel que :

1. la fonction f annule un opérateur différentiel L à coefficients dans $\overline{\mathbb{Q}}(z)$;
2. la valeur absolue de chaque conjugué de Galois de a_n est inférieure à C^{n+1} pour tout $n \geq 0$;
3. il existe une suite D_m d'entiers strictement positifs tels que $D_m < C^{m+1}$ et $D_m a_n$ est un entier algébrique pour tout $n \leq m$.

2. Le degré d'une série algébrique est le degré du polynôme minimal de cette série.

3. La hauteur d'une série algébrique est définie comme la hauteur du polynôme minimal de cette série. La hauteur d'un polynôme $P(Y) \in \mathbb{Q}[z_1, \dots, z_n][Y]$ est le degré total de P en les variables z_1, \dots, z_n .

Les éléments de $\mathbf{Diag}_{\overline{\mathbb{Q}}}^{alg}$ sont des exemples de G -fonctions. En effet, d'après le théorème 6.2 de [35], $\mathbf{Diag}_{\overline{\mathbb{Q}}}^{alg} = \mathbf{Diag}_{\overline{\mathbb{Q}}}$ et donc, grâce au lemme de la partie 4.2 du chapitre I de [10], les diagonales de séries algébriques à coefficients dans $\overline{\mathbb{Q}}$ sont des G -fonctions. Notons par $\mathbf{G}_{\mathbb{Q}}$ l'ensemble des G -fonctions qui sont à coefficients dans \mathbb{Q} . Nous pouvons donc affiner notre classification de la façon suivante :

$$\mathbf{Rat}_{\mathbb{Q}} \subset \mathbf{Alg}_{\mathbb{Q}} \subset \mathbf{Diag}_{\mathbb{Q}} \subset \mathbf{G}_{\mathbb{Q}} \subset \mathbf{Hol}_{\mathbb{Q}}.$$

Ainsi, la série $\mathfrak{g}(z)$ est une G -fonction car c'est une diagonale de fraction rationnelle. Remarquons que la condition 2 de la définition implique qu'une G -fonction a un rayon de convergence non nul. Ainsi, $\mathfrak{f}(z)$ n'est pas une G -fonction.

Si $f(z)$ est une G -fonction alors la définition précédente implique qu'il existe un corps de nombres K tel que $f(z) \in K[[z]]$. Dans la suite considérons un tel K . Soient ϑ_K l'anneau des entiers de K et \mathfrak{p} un idéal premier de ϑ_K tel que les coefficients de $f(z)$ appartiennent à $\vartheta_{K,\mathfrak{p}}$, la localisation de ϑ_K en \mathfrak{p} . Notons $\mathbf{k}_{\mathfrak{p}}$ le corps résiduel de $\vartheta_{K,\mathfrak{p}}$, c'est-à-dire $\mathbf{k}_{\mathfrak{p}} = \vartheta_{K,\mathfrak{p}}/\mathfrak{p}\vartheta_{K,\mathfrak{p}} = \vartheta_K/\mathfrak{p}$. On peut alors réduire f modulo \mathfrak{p} et poser

$$f_{|\mathfrak{p}}(z) = \sum_{n \geq 0} (a_n \bmod \mathfrak{p}) z^n \in \mathbf{k}_{\mathfrak{p}}[[z]].$$

Rappelons que $\mathbf{Diag}_K = \mathbf{Diag}_K^{alg}$. D'après le lemme de la partie 4.2 du chapitre I de [10], si $f(z) \in K[[z]]$ appartient à \mathbf{Diag}_K alors $f(z)$ est *globalement bornée*, c'est-à-dire il existe $\beta, \gamma \in K$ non nuls tels que $\gamma f(\beta z) \in \vartheta_K[[z]]$. En particulier, pour presque tout idéal premier \mathfrak{p} de ϑ_K , la série $f(z)$ est à coefficients dans $\vartheta_{K,\mathfrak{p}}$ et alors, nous pouvons considérer la série $f_{|\mathfrak{p}}(z)$. Donc, si $f(z) \in K[[z]]$ est la diagonale d'une série algébrique et \mathcal{S} est l'ensemble des idéaux premiers \mathfrak{p} de ϑ_K tel que $f(z) \in \vartheta_{K,\mathfrak{p}}[[z]]$, alors \mathcal{S} est un ensemble infini et nous avons les deux faits remarquables suivants :

- (a) pour tout $\mathfrak{p} \in \mathcal{S}$, la série $f_{|\mathfrak{p}}(z)$ est algébrique sur $\mathbf{k}_{\mathfrak{p}}(z)$;
- (b) il existe $c > 0$ tel que pour tout $\mathfrak{p} \in \mathcal{S}$, $\deg(f_{|\mathfrak{p}}) < p^c$, où p est la caractéristique du corps $\mathbf{k}_{\mathfrak{p}}$.

Le point (a) découle du théorème B et les résultats d'Adamczewski et Bell [1] entraînent le point (b). Ainsi, les éléments de $\mathbf{Diag}_{\overline{\mathbb{Q}}}^{alg}$ sont des G -fonctions pour lesquelles les questions 1 et 2 ont une réponse positive. En revanche, il existe des G -fonctions qui ne sont pas dans $\mathbf{Diag}_{\overline{\mathbb{Q}}}^{alg}$ et qui vérifient les points (a) et (b) pour un ensemble infini d'idéaux premiers. Illustrons cela à l'aide d'un exemple. Considérons la série hypergéométrique

$$\mathfrak{f}_1(z) := {}_2F_1(1/2, 1/2; 2/3, z) = \sum_{n \geq 0} \frac{(1/2)_n^2}{(2/3)_n n!} z^n \in \mathbb{Q}[[z]],$$

où pour $x \in \mathbb{R}$, $(x)_0 = 1$ et $(x)_n = x(x+1) \cdots (x+n-1)$. La série $\mathfrak{f}_1(z)$ est une G -fonction car elle annule l'opérateur différentiel

$$z(1-z) \frac{d^2}{dz^2} + (2/3 - 2z) \frac{d}{dz} - 1/4$$

et, à la suite du lemme de la partie 4.4 du chapitre I de [10], $\mathfrak{f}_1(z)$ satisfait aux conditions 2 et 3 de la définition des G -fonctions. La proposition 1 de [27] entraîne que la série $\mathfrak{f}_1(z)$ n'est pas globalement bornée et par conséquent, elle n'appartient pas à $\mathbf{Diag}_{\overline{\mathbb{Q}}} = \mathbf{Diag}_{\overline{\mathbb{Q}}}^{alg}$. Rappelons que l'anneau $\mathbb{Z}_{(p)}$ désigne la localisation de \mathbb{Z} en l'idéal (p) . Si \mathcal{S} est l'ensemble

des nombres premiers p congrus à 1 modulo 3 alors, la proposition 8.5 de [5] implique que, pour tout $p \in \mathcal{S}$, la série $f_1(z)$ est à coefficients dans $\mathbb{Z}_{(p)}$ et $f_{1|p}(z) = A_p(z)f_{1|p}(z)^p$, où $A_p(z)$ est un polynôme à coefficients dans \mathbb{F}_p . Ainsi, pour tout nombre premier p congru à 1 modulo 3, la série $f_{1|p}(z)$ est algébrique sur $\mathbb{F}_p(z)$ et $\deg(f_{1|p}) \leq p - 1 < p$. Ainsi, $f_1(z)$ satisfait aux points (a) et (b). Notons par ailleurs que, d'après le théorème de Dirichlet, l'ensemble des nombres premiers p congru à 1 modulo 3 est infini. La série $f_1(z)$ appartient à une famille de G -fonctions qui a été étudiée par Adamczewski, Bell et Delaygue dans [5]. Leurs résultats montrent que toute série appartenant à cette famille vérifient les points (a) et (b) pour un ensemble infini de nombre premiers. En effet, ils montrent plus précisément que ces séries sont p -Lucas⁴ pour une infinité de nombres premiers. Nous soulignons que dans le contexte décrit précédemment l'importance de la classe des G -fonctions étudiée par Adamczewski, Bell et Delaygue vient du fait qu'elle n'est pas contenue dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ et que ses éléments vérifient les points (a) et (b). Par conséquent, les points (a) et (b) sont vérifiés pour toute série appartenant à $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ et également pour de nombreux exemples de G -fonctions n'appartenant pas à $\mathbf{Diag}_{\mathbb{Q}}^{alg}$. Cette situation a conduit Adamczewski et Delaygue à formuler la conjecture suivante [4].

Conjecture 4 (Adamczewski–Delaygue [4]). *Soient K un corps de nombres et $f(z) \in K[[z]]$ une G -fonction. Supposons que l'ensemble \mathcal{S} des idéaux premiers \mathfrak{p} de ϑ_K tel que $f \in \vartheta_{K,\mathfrak{p}}[[z]]$ soit infini. Alors, on a :*

- (i) $f|_{\mathfrak{p}}$ est algébrique sur $\mathbf{k}_{\mathfrak{p}}(z)$ pour presque tout $\mathfrak{p} \in \mathcal{S}$;
- (ii) il existe $c > 0$ tel que, pour tout \mathfrak{p} vérifiant (i), $\deg(f|_{\mathfrak{p}}) < p^c$, où p désigne la caractéristique du corps $\mathbf{k}_{\mathfrak{p}}$.

Cette conjecture prédit donc une réponse positive aux questions 1 et 2 pour la classe des G -fonctions. Les résultats de Deligne [34] et d'Adamczewski et Bell [1] mentionnés dans la partie 1.2 montrent que cette conjecture est vérifiée pour toute série dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ et l'article [5] fournit également d'autres familles d'exemples parmi les séries hypergéométriques généralisées ou certaines séries dont les coefficients sont des sommes multiples de produits de coefficients binomiaux.

La méthode utilisée dans [1] est spécifique aux diagonales de séries formelles algébriques tandis que les résultats de [5] se fondent sur une analyse minutieuse de la valuation p -adique des coefficients et ne concernent pas toutes les séries hypergéométriques généralisées. Avant de voir la méthode utilisée dans [1], nous rappelons la définition de certains opérateurs que nous appelons *opérateurs de Cartier*⁵.

Définition 1.3.2. Soient n entier strictement positif et p un nombre premier. Étant donné $\mathbf{j} = (j_1, \dots, j_n) \in \{0, 1, \dots, p - 1\}^n$, l'opérateur de Cartier $\Lambda_{\mathbf{j}} : \mathbb{F}_p[[z_1, \dots, z_n]] \rightarrow \mathbb{F}_p[[z_1, \dots, z_n]]$ est donné par

$$\Lambda_{\mathbf{j}} \left(\sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} b(i_1, \dots, i_n) z_1^{i_1} \cdots z_n^{i_n} \right) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} b(pi_1 + j_1, \dots, pi_n + j_n) z_1^{i_1} \cdots z_n^{i_n}.$$

La stratégie utilisée dans [1] pour montrer le théorème C est la suivante : soit $f \in \mathbb{Z}[[z]]$ la diagonale de la série algébrique $g \in \mathbb{Z}[[z_1, \dots, z_n]]$. Alors, tout nombre premier p , la série $g|_p \in \mathbb{F}_p[[z_1, \dots, z_n]]$ est une série algébrique à coefficients dans \mathbb{F}_p . Les auteurs construisent un \mathbb{F}_p -espace vectoriel $V_{g|_p}$ tel que :

4. Le lecteur trouvera la définition de série p -Lucas dans la partie 1.6.1

5. Dans [7, Section 2] le lecteur trouvera le pourquoi de ces opérateurs sont nommés opérateurs de Cartier.

- la série $g|_p$ appartient à $V_{g|_p}$;
- le \mathbb{F}_p -espace vectoriel $V_{g|_p}$ est invariant par l'action des opérateurs de Cartier ;
- le \mathbb{F}_p -espace vectoriel $V_{g|_p}$ est de dimension finie majorée par un entier c .

D'après la proposition 5.1 de [1], ces trois conditions garantissent que f est algébrique modulo p et que le degré d'algébricité de $f|_p$ est inférieur ou égal à p^c . De plus, ils démontrent que l'entier c dépend uniquement des données suivantes : le degré d'algébricité de g , la hauteur de g et l'entier n . Le fait que f soit la diagonale de la série algébrique g est utilisé dans la construction de l'espace vectoriel $V_{g|_p}$.

Nous montrerons une version explicite de la conjecture 4 pour la plupart des séries hypergéométriques généralisées à paramètres rationnels. L'avantage de ce résultat (théorème 1.4.12) est qu'il offre des exemples de G -fonctions qui ne sont ni dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ ni dans la classe des G -fonctions étudiée dans [5], mais pour lesquelles la conjecture d'Adamczewski–Delaygue est vraie. Notre outil principal pour démontrer ce résultat est la notion de structure de Frobenius forte associée aux équations différentielles linéaires p -adiques.

1.4 Résultats principaux, première partie

Dans cette partie, nous expliquons pourquoi la notion de structure de Frobenius forte associée aux équations différentielles linéaires p -adiques est un outil pertinent pour l'étude de l'algébricité modulo p . Avant de rappeler la définition de structure de Frobenius forte, nous décrivons brièvement notre approche. Comme nous l'avons mentionné, les questions 1 et 2 ont une réponse positive pour les éléments de $\mathbf{Diag}_{\mathbb{Q}}$ [1] et pour une grande famille de G -fonctions étudiées dans [5]. Bien que les approches utilisées dans [1] et [5] soient différentes, aucune n'utilise directement le fait que les séries considérées sont holonomes. L'objectif de cette thèse est d'aborder cette problématique sous un angle différent, en plaçant l'holonomie au cœur de notre étude.

Si $f(z) \in \mathbb{Q}[[z]]$ est une G -fonction, alors f annule un opérateur différentiel $L \in \mathbb{Q}(z)[d/dz]$. Pour tout nombre premier p , l'opérateur L peut également être vu comme un opérateur différentiel à coefficients dans $\mathbb{Q}_p(z)$ puisque $\mathbb{Q}(z) \subset \mathbb{Q}_p(z)$. On peut donc considérer « p -adiquement » l'équation différentielle annulée par $f(z)$ et utiliser les outils de la théorie des équations différentielles p -adiques. C'est dans ce contexte qu'est définie la notion de structure de Frobenius forte. Si l'opérateur $L \in \mathbb{Q}_p(z)[d/dz]$ admet une structure de Frobenius forte, on montre que la série $f(z)$ satisfait à une *équation p -mahlérienne* (ou au Frobenius) à coefficients dans un certain corps E_p , appelé corps des *éléments analytiques*, c'est-à-dire qu'il existe $a_0(z), \dots, a_r(z) \in E_p$, non tous nuls, tels que

$$a_0(z)f(z) + a_1(z)f(z^p) + \dots + a_r(z)f(z^{p^r}) = 0.$$

La définition du corps E_p est donnée dans la partie 1.4.2, mais on peut déjà dire que les éléments de E_p sont obtenus ici comme limite de fractions rationnelles à coefficients dans le corps \mathbb{C}_p et qu'il est complet pour la norme de Gauss. Nous renvoyons le lecteur à [6], où il trouvera des résultats récents sur les équations mahlériennes et leur lien avec des questions de transcendance.

D'après le lemme 2.1.1, le corps résiduel de E_p est $\overline{\mathbb{F}_p}(z)$, où $\overline{\mathbb{F}_p}$ est la clôture algébrique de \mathbb{F}_p . Après certaines réductions nous pouvons supposer que $1 = \{|a_0(z)|_{\mathcal{G}}, \dots, |a_r(z)|_{\mathcal{G}}\}$. Ainsi, lorsque l'on peut réduire $f(z)$ modulo p , il devient possible de réduire cette relation modulo p afin d'obtenir une équation du type

$$a'_0(z)f|_p(z) + a'_1(z)f|_p(z)^p + \dots + a'_r(z)f|_p(z)^{p^r} = 0,$$

où $a'_i(z) \in \overline{\mathbb{F}_p}(z)$. On en déduit donc que $f(z)$ est algébrique modulo p et que son degré d'algébricité est majoré par p^r . Dans la suite, nous nous intéresserons particulièrement à des séries formelles holonomes qui annulent un opérateur différentiel $L \in \mathbb{Q}(z)[d/dz]$ admettant une structure de Frobenius forte pour presque tout nombre premier p .

1.4.1 Structure de Frobenius forte

Soit p un nombre premier. Le complété de \mathbb{Q} pour la norme p -adique est noté \mathbb{Q}_p , nous notons par \mathbb{Z}_p le sous-anneau de \mathbb{Q}_p formé des éléments dont la norme p -adique est inférieure ou égale à 1 et \mathbb{C}_p le complété de la clôture algébrique de \mathbb{Q}_p . Le corps \mathbb{Q}_p est le corps des nombres p -adique et \mathbb{Z}_p est l'anneau des entiers p -adiques. Nous rappelons que la valuation de \mathbb{Q}_p s'étend de manière unique à \mathbb{C}_p et que \mathbb{C}_p est algébriquement clos. Nous désignerons par π_p , un élément de \mathbb{C}_p vérifiant $\pi_p^{p-1} = -p$.

1.4.2 Éléments analytiques

Soit K un corps de caractéristique nulle muni de la norme ultramétrique $|\cdot|$, c'est-à-dire pour tout $x, y \in K$, $|x| = 0$ si et seulement si $x = 0$, $|x + y| \leq \max\{|x|, |y|\}$ et $|xy| = |x||y|$. Nous notons ϑ_K les éléments de K qui ont norme inférieure ou égale à 1. Comme la norme $|\cdot|$ est ultramétrique alors ϑ_K est un anneau local dont l'idéal maximal \mathfrak{m}_K est constitué par les éléments de ϑ_K ayant norme strictement inférieure à 1. Par définition, le corps résiduel de K est le corps $k := \vartheta_K / \mathfrak{m}_K$. Nous supposons dans la suite que la caractéristique de k est $p \neq 0$.

Pour $x \in K$ tel que $|x| \leq 1$, nous notons \bar{x} l'élément de k qui représente la classe résiduelle de x . Nous supposons que K est complet pour la norme $|\cdot|$. Nous dirons que $\sigma : K \rightarrow K$ est un automorphisme de Frobenius si les conditions suivantes sont vérifiées :

1. pour tout $x \in K$, $|\sigma(x)| = |x|$;
2. pour tout $x \in K$, $|x| \leq 1$, $|\sigma(x) - x^p| < 1$. Autrement dit, $\bar{\sigma} : k \rightarrow k$ donné par $\bar{\sigma}(\bar{x}) = \overline{\sigma(x)}$ est l'endomorphisme de Frobenius. Remarquons que $\bar{\sigma}$ est bien défini par le point 1.

Remarque 1.4.1. La proposition 1.10.1 de [23] montre que le corps \mathbb{C}_p possède un automorphisme de Frobenius, mais celui-ci n'est pas unique. Dans la suite, nous fixons un tel automorphisme que nous notons $Frob : \mathbb{C}_p \rightarrow \mathbb{C}_p$ et que nous appellerons l'*automorphisme de Frobenius* de \mathbb{C}_p .

Nous montrons à présent comment construire le corps des éléments analytiques. Nous désignons par \mathcal{W} l'anneau d'Amice qui est l'ensemble des séries formelles

$$f(z) = \sum_{n \in \mathbb{Z}} a_n z^n$$

telles que les a_n sont des éléments de K dont la valeur absolue est bornée et tend vers zéro lorsque n tend négativement vers l'infini. D'après la proposition 1.1 de [26], l'anneau \mathcal{W} est un K -espace vectoriel complet pour la norme définie par $|f| = \sup\{|a_n| : n \in \mathbb{Z}\}$. L'anneau $K[z]$ est contenu dans l'anneau \mathcal{W} et ainsi, l'anneau $K[z]$ est muni de la norme de Gauss

$$\left| \sum a_j z^j \right|_{\mathcal{G}} = \sup |a_j|.$$

De plus, d'après la proposition 1.2 de [26], tout élément non nul de $K[z]$ est inversible dans \mathcal{W} , ce qui implique que l'anneau des fractions rationnelles $K(z)$ est contenu dans \mathcal{W} . La

norme de \mathcal{W} induit une norme sur $K(z)$ qui s'exprime comme

$$\left| \frac{\sum a_j z^j}{\sum b_i z^i} \right|_{\mathcal{G}} = \frac{\sup |a_j|}{\sup |b_i|}.$$

Comme \mathcal{W} est complet, le complété de $K(z)$ pour la norme de Gauss est également contenu dans \mathcal{W} .

Définition 1.4.2 (Éléments analytiques). Le corps des éléments analytiques E_K est le complété du corps $K(z)$ pour la norme de Gauss dans \mathcal{W} . Dans le cas où $K = \mathbb{C}_p$, le corps des éléments analytiques est noté E_p et l'analogue de \mathcal{W} est noté \mathcal{W}_p .

Remarque 1.4.3. Pour tout $f \in K(z)$, on a

$$\left| \frac{d}{dz}(f) \right|_{\mathcal{G}} \leq |f|_{\mathcal{G}}.$$

Ainsi, la dérivation $\frac{d}{dz} : K(z) \rightarrow K(z)$ est une fonction continue pour la norme de Gauss et elle s'étend naturellement au corps E_K des éléments analytiques. On note encore son extension $\frac{d}{dz} : E_K \rightarrow E_K$.

Définition 1.4.4 (E_p -équivalence). Soient A et B dans $\mathcal{M}_n(E_p)$. Nous disons que A et B sont E_p -équivalentes s'il existe $H \in \text{GL}_n(E_p)$ telle que

$$\frac{d}{dz}H = AH - HB.$$

1.4.3 Structure de Frobenius forte

Nous définissons l'application $Frob_{z^p} : \mathbb{C}_p(z) \rightarrow E_p$ par

$$Frob_{z^p} \left(\frac{\sum a_i z^i}{\sum b_j z^j} \right) = \frac{\sum Frob(a_i) z^{pi}}{\sum Frob(b_j) z^{pj}}.$$

Cette application est une isométrie. Il s'agit donc d'une application continue qui s'étend au corps des éléments analytiques E_p . Nous la notons encore $Frob_{z^p} : E_p \rightarrow E_p$. C'est à nouveau une isométrie et, pour tout $e \in E_p$, on a

$$\frac{d}{dz}(Frob_{z^p}(e)) = pz^{p-1} \left(Frob_{z^p} \left(\frac{d}{dz} e \right) \right). \quad (1.5)$$

Soit A une matrice de taille n à coefficients dans E_p , nous considérons la matrice $F_{z^p}(A) := \frac{d}{dz}(z^p)A^{Frob_{z^p}} = pz^{p-1}A^{Frob_{z^p}}$, où $A^{Frob_{z^p}}$ est la matrice obtenue après avoir appliqué $Frob_{z^p}$ à chaque entrée de A .

Étant donné un opérateur différentiel d'ordre n

$$L := a_0(z) \frac{d}{dz^n} + a_1(z) \frac{d}{dz^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} + a_n(z) \in \mathbb{Q}[z][d/dz], \quad (1.6)$$

on définit la *matrice compagnon* associée à L par

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ \frac{-a_n(z)}{a_0(z)} & \frac{-a_{n-1}(z)}{a_0(z)} & \frac{-a_{n-2}(z)}{a_0(z)} & \cdots & \frac{-a_2(z)}{a_0(z)} & \frac{-a_1(z)}{a_0(z)} \end{pmatrix}.$$

Définition 1.4.5 (Structure de Frobenius forte). Soit $L \in \mathbb{Q}(z)[d/dz]$ un opérateur différentiel et soit A sa matrice compagnon. Nous disons que L a une structure de Frobenius forte de période h pour un nombre premier p s'il existe un entier strictement positif h tel que la matrice A et la matrice obtenue en appliquant h -fois F_{z^p} à A sont E_p -équivalentes. Comme $A \in \mathcal{M}_n(\mathbb{Q}(z))$, cela revient à dire qu'il existe $H \in \mathrm{GL}_n(E_p)$ telle que

$$\frac{d}{dz}H = AH - p^h z^{p^h-1} HA(z^{p^h}). \quad (1.7)$$

Le plus petit entier $h \geq 1$ ayant cette propriété est appelé *la période* de la structure de Frobenius associée au couple (L, p) .

Par exemple, d'après [54, Chap. 22, Theorem 22.2.1]⁶ ou [10, Chap. V, p. 111], les *équations de Picard–Fuchs* sont munies d'une structure de Frobenius forte pour presque tout nombre premier p . Par exemple l'opérateur différentiel

$$z(z-1)\frac{d}{dz^2} + (2z-1)\frac{d}{dz} + \frac{1}{4}$$

est un opérateur de Picard–Fuchs parce qu'il est obtenu à partir de la famille de courbes elliptiques de Legendre E_z définie par $y^2 = x(x-1)(x-z)$. Comme nous le verrons, cet opérateur est muni d'une structure de Frobenius forte de période 1 pour tout nombre premier différent de 2. La série

$$\mathfrak{g}\left(\frac{1}{16}z\right) = \sum_{n \geq 0} \frac{1}{16^n} \binom{2n}{n}^2 z^n$$

est solution de cet opérateur.

1.4.4 Structure de Frobenius forte et algébricité modulo p

Le résultat que nous énonçons dans cette partie établit le lien entre l'existence d'une structure de Frobenius forte pour le couple (L, p) et l'algébricité modulo p de ses solutions. Voici le premier résultat de la thèse.

Théorème 1.4.6. *Soit $L \in \mathbb{Q}(z)[d/dz]$ d'ordre n . Soit p un nombre premier pour lequel l'opérateur différentiel L a une structure de Frobenius forte de période h et $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Z}_{(p)}[[z]]$ une solution de L . Alors $f(z)$ est algébrique modulo p et le degré de $f|_p(z)$ sur $\mathbb{F}_p(z)$ est majoré par p^{n^2h} .*

Ainsi, le théorème 1.4.6 établit un lien entre l'existence, pour un nombre premier p , d'une structure de Frobenius forte de période h pour un opérateur différentiel d'ordre n et le degré d'algébricité modulo p des solutions (séries formelles à coefficients dans $\mathbb{Z}_{(p)}$) de cet opérateur en fonction de p , n et h . Nous faisons les remarques suivantes.

- (i) Nous pourrions énoncer ce théorème dans le cas d'un opérateur à coefficients dans $\overline{\mathbb{Q}}[z]$ et $f \in \mathcal{V}_{K,p}[[z]]$, la démonstration s'obtiendrait de façon similaire.
- (ii) Le théorème 1.4.6 nous dit que pour montrer le premier point de la conjecture 4 il suffit de voir que f annule un opérateur différentiel à coefficients dans $\overline{\mathbb{Q}}(z)$ muni d'une structure de Frobenius forte.

6. Voir aussi la discussion p. 351 de [54] et les références associées.

- (iii) Le lien entre algébricité modulo p et structure de Frobenius forte a d'abord été observé par Christol [20, 26]. Chez Christol, ce lien est donné à travers la notion de suite p -automatique⁷. En effet, soit $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Z}[[z]]$. Dans [20], il est montré que la suite $\{a(n) \bmod p\}_{n \geq 0}$ est p -automatique si et seulement si la série $f|_p(z)$ est algébrique sur $\mathbb{F}_p(z)$ et il suit de [26, Théorème 7.2 et Corollaire 8.3] que si $f(z) \in \mathbb{Z}_{(p)}[[z]]$ annule un opérateur différentiel à coefficients dans $\mathbb{Q}(z)$ muni d'une structure de Frobenius forte pour p alors la suite $\{a(n) \bmod p\}_{n \geq 0}$ est p -automatique.
- (iv) La preuve que nous présentons du théorème 1.4.6 n'utilise pas de la notion de suite p -automatique, mais la nouveauté du théorème 1.4.6 vient avant tout de la majoration explicite que nous obtenons du degré d'algébricité de la série $f|_p(z)$.

À présent expliquons la stratégie employée dans la démonstration du théorème 1.4.6. Soient $L \in \mathbb{Q}(z)[d/dz]$ un opérateur différentiel d'ordre n , $f(z) \in \mathbb{Q}[[z]]$ solution de L , et p un nombre premier pour lequel l'opérateur L possède une structure de Frobenius forte de période h et $f \in \mathbb{Z}_{(p)}[[z]]$. Nous construisons un E_p -espace vectoriel V_f contenu dans l'anneau d'Amice \mathcal{W}_p tel que :

- la série $f \in V_f$;
- le E_p -espace vectoriel V_f est stable sous l'application $z \mapsto z^p$;
- le E_p -espace vectoriel V_f a dimension au plus n^2h .

Ainsi, nous obtenons qu'il existe $a_0(z), \dots, a_{n^2h}(z) \in E_p$ non nuls tels que

$$a_0(z)f(z) + a_1(z)f(z^p) + \dots + a_{n^2h}(z)f(z^{p^{n^2h}}) = 0. \quad (1.8)$$

Autrement dit, la série $f(z)$ est solution d'une équation p -mahlérienne à coefficients dans E_p d'ordre inférieur ou égal à n^2h . Le théorème 1.4.6 découle en étudiant la réduction de l'égalité (1.8) modulo l'idéal maximal de \mathfrak{v}_{E_p} . L'hypothèse que $f(z)$ est solution d'un opérateur muni d'une structure de Frobenius forte est évidemment utilisée dans la construction du E_p -espace vectoriel V_f .

Une conséquence remarquable de cet argument est la suivante : soient \mathcal{S} un ensemble infini de nombres premiers et $f(z) \in \mathbb{Q}[[z]]$ solution d'un opérateur différentiel L d'ordre n à coefficients dans $\mathbb{Q}(z)$ et muni d'une structure de Frobenius forte pour tout $p \in \mathcal{S}$. Alors, pour tout $p \in \mathcal{S}$, la série $f(z)$ est solution d'une équation p -mahlérienne non nulle à coefficients dans E_p d'ordre inférieur ou égal à n^2h , où h est la période qui correspond au nombre premier p .

Remarquons qu'il y a une similitude entre la stratégie utilisée dans [1] pour démontrer le théorème C (rappelons que cette stratégie a été décrite à la fin de la partie 1.3) et celle employée pour démontrer le théorème 1.4.6. Dans [1], l'hypothèse que $f(z)$ est la diagonale d'une série algébrique est utilisée pour construire un \mathbb{F}_p -espace vectoriel de dimension finie contenant $f(z)$ et stable sous l'action des opérateurs de Cartier, tandis que nous utilisons l'hypothèse que $f(z)$ est solution d'un opérateur différentiel muni d'une structure de Frobenius forte pour construire un E_p -espace vectoriel de dimension finie contenant $f(z)$ et stable sous l'action du morphisme de Frobenius $z \mapsto z^p$.

1.4.5 Structure de Frobenius forte et rigidité

Commençons par observer comment le théorème 1.4.6 peut être utilisé pour apporter une réponse positive aux questions 1 et 2 pour certaines séries formelles holonomes. En

7. Le lecteur trouvera la définition de suite p -automatique dans la partie 1.6.1

effet, supposons que $f(z) \in \mathbb{Q}[[z]]$ annule un opérateur différentiel L d'ordre n à coefficients dans $\mathbb{Q}(z)$ muni d'une structure de Frobenius forte de période h pour presque tout nombre premier p , où h est indépendant de p . Alors, d'après le théorème 1.4.6, si p est tel que $f(z) \in \mathbb{Z}_{(p)}[[z]]$, la série $f|_p(z)$ est algébrique sur $\mathbb{F}_p(z)$ de degré d'algébricité inférieur ou égal à p^{n^2h} . Comme l'entier n^2h est indépendant de p , les questions 1 et 2 ont une réponse positive pour la série $f(z)$.

Dans cette partie, nous allons voir que les *opérateurs rigides*, dont la définition est donnée dans la partie 2.2, possèdent, pour presque tout nombre premier p , une structure de Frobenius forte de période h , où h est majorée explicitement et indépendamment de p . Avant d'énoncer ce résultat, nous rappelons quelques notions classiques concernant les opérateurs différentiels.

Opérateur fuchsien

Dans cette partie, K désigne un corps quelconque. Un opérateur différentiel à coefficients dans $K(z)$ est un opérateur de la forme

$$L := \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} + a_n(z), \quad (1.9)$$

où les $a_i(z)$ appartiennent à $K(z)$. L'entier n est l'*ordre* de l'opérateur L . Un point α dans la clôture algébrique de K est un point *singulier* de L s'il existe $i \in \{1, \dots, n\}$ tel que α est un pôle pour $a_i(z)$. Nous disons que α est un point *singulier régulier* de L si α est un point singulier de L et, pour tout $i \in \{1, \dots, n\}$, $\tilde{a}_i(z) := (z - \alpha)^i a_i(z)$ n'a pas de pôle en α . Soit L_∞ l'opérateur différentiel obtenu après avoir appliqué le changement de variable $z \mapsto 1/z$ à L . Nous disons que l'infini est un point *singulier régulier* de L si zéro est un point singulier régulier de L_∞ . Remarquons que si, pour chaque $i \in \{1, \dots, n\}$, nous écrivons $a_i(z) = \frac{b_{i,1}(z)}{b_{i,2}(z)}$, où $b_{i,1}(z)$ et $b_{i,2}(z)$ appartiennent à $K[z]$ et sont premiers entre eux, alors l'infini est un point singulier régulier de L si et seulement si, pour tout $i \in \{1, \dots, n\}$, $\deg(b_{i,1}(z)) \leq \deg(b_{i,2}(z)) - i$.

Nous dirons que α est une *singularité à distance finie* de L si α est un point singulier de L et α n'est pas l'infini.

Définition 1.4.7 (Opérateur fuchsien). Soient K un corps quelconque et L défini comme en (1.9). L'opérateur L est *fuchsien* si l'infini est un point singulier régulier de L et si toutes les singularités à distance finie de L sont des points singuliers réguliers de L . Soit $\delta = z \frac{d}{dz}$. Par abus de langage, si $L_\delta \in K(z)[\delta]$ est d'ordre n , nous dirons que L_δ est fuchsien si l'opérateur obtenu après avoir réécrit l'opérateur $\frac{1}{z^n} L_\delta$ en fonction de d/dz est fuchsien.

Définition 1.4.8 (Exposants). Soient L défini comme en (1.9) un opérateur fuchsien et α une singularité à distance finie de L . Les exposants de L en α sont les racines du polynôme

$$X(X-1) \cdots (X-n+1) + \tilde{a}_1(\alpha) X(X-1) \cdots (X-n+2) + \cdots + \tilde{a}_{n-1}(\alpha) X + \tilde{a}_n(\alpha).$$

Si l'infini est un point singulier de L , les exposants de L en l'infini sont les exposants de L_∞ en zéro.

Rappelons maintenant la définition des matrices de monodromie locale d'un opérateur à coefficients dans $\mathbb{C}(z)$. Soient $L \in \mathbb{C}(z)[d/dz]$ un opérateur différentiel d'ordre n et $x \in \mathbb{C}$ un point non singulier de L , d'après la théorie classique de Cauchy,

$$\text{Sol}(L)_x = \{f \text{ holomorphe au voisinage de } x \text{ et } L(f) = 0\}$$

est un \mathbb{C} -espace vectoriel de dimension n . Soient $F = \{f_1, \dots, f_n\}$ une base de $Sol(L)_x$, $S = \{\gamma_1, \dots, \gamma_r\} \in \mathbb{C} \cup \{\infty\}$ l'ensemble des points singuliers de L et $\gamma \in S$. Les fonctions f_1, \dots, f_n peuvent être prolongées le long d'un lacet τ tel que $\langle [\tau] \rangle = \Pi_1(\mathbb{C} \setminus S, x)$. Ainsi, on obtient un nouvel ensemble \tilde{F} qui sera encore une base de $Sol(L)_x$. Alors la matrice de *monodromie locale*, notée $M(A, \gamma) \in GL_n(\mathbb{C})$, est la matrice de changement de base de F vers \tilde{F} . Le *groupe de monodromie* de L est le groupe engendré par les matrices $M(A, \gamma_1), \dots, M(A, \gamma_r)$ qui satisfont à la relation $M(A, \gamma_1) \cdots M(A, \gamma_r) = Id$.

Définition 1.4.9. (Rigidité) Soient L un opérateur fuchsien à coefficients dans $\mathbb{C}(z)$ d'ordre n et $M_1, \dots, M_r \in GL_n(\mathbb{C})$ les matrices qui engendrent le groupe de monodromie de L telles que $M_1 \cdots M_r = Id$. On dit que le groupe de monodromie de L est rigide si pour tout $N_1, \dots, N_r \in GL_n(\mathbb{C})$ telles que $N_1 \cdots N_r = Id$ et N_i est conjuguée à M_i , il existe $U \in GL_n(\mathbb{C})$ telle que, pour tout $i \in \{1, \dots, r\}$, $U^{-1}M_iU = N_i$.

Structure de Frobenius forte et rigidité

Soit L défini comme en (1.6) et supposons que les exposants aux points singuliers réguliers sont des nombres rationnels. Soit s la valuation de $a_0(z)$, c'est-à-dire s est l'entier positif tel que $a_0(z)$ appartient à l'idéal $z^s\mathbb{Q}[z]$ et $a_0(z)$ n'appartient pas à $z^{s+1}\mathbb{Q}[z]$. Considérons les ensembles suivants : \mathfrak{A}_1 est formé du terme constant du polynôme $\frac{a_0(z)}{z^s}$, du coefficient dominant de $a_0(z)$ et du discriminant de $a_0(z)$, \mathfrak{A}_2 est formé des dénominateurs des exposants aux points singuliers réguliers de L et $\mathfrak{A}_3 = \left\{ \frac{a_i(z)}{a_0(z)} \right\}_{1 \leq i \leq n}$. Soit d le plus petit commun multiple des dénominateurs des exposants de L en les points singuliers réguliers. On pose $h_1 = \phi(d)$, où ϕ est la fonction indicatrice d'Euler, h_2 la dimension du corps de décomposition du polynôme $a_0(z)$ sur \mathbb{Q} , et finalement $h = h_1h_2$. Voici un deuxième résultat obtenu dans cette thèse.

Théorème 1.4.10. Soit $L \in \mathbb{Q}[z][d/dz]$ un opérateur différentiel défini comme en (1.6). Supposons que les conditions suivantes sont vérifiées.

1. Les points singuliers de L sont réguliers, c'est-à-dire que L est fuchsien.
2. Les exposants aux points singuliers réguliers sont des nombres rationnels.
3. Le groupe de monodromie de L est rigide.

Soit \mathcal{S} l'ensemble des nombres premiers tels que $a_0(z) \in \mathbb{Z}_{(p)}[z]$, tout élément de \mathfrak{A}_1 et \mathfrak{A}_2 ait une norme p -adique égale à 1 et tout élément de \mathfrak{A}_3 ait une norme de Gauss inférieure ou égale à 1. Alors pour tout $p \in \mathcal{S}$, l'opérateur différentiel a une structure de Frobenius forte de période h .

Les exemples les plus célèbres d'opérateurs satisfaisant aux trois conditions du théorème 1.4.10 sont les opérateurs hypergéométrique de Gauss

$$z(z-1)\frac{d}{dz^2} + ((a+b)z-c)\frac{d}{dz} + ab,$$

où $a, b, c \in \mathbb{Q} \cap (0, 1]$. Dans [62], Salinier a montré que ces opérateurs possèdent une structure de Frobenius forte pour presque tout nombre premier p dont la période est indépendante du nombre premier p . Notons qu'avant le travail de Salinier, Dwork avait déjà montré par une approche différente que, sous ces hypothèses, l'opérateur hypergéométrique de Gauss est muni d'une structure de Frobenius forte pour presque tout p (voir [41, Chap. 7, 7.2.2]). Le théorème 1.4.10 montre de façon plus générale que les systèmes différentiels rigides sont munis d'une structure de Frobenius forte pour presque tout p

dont la période peut être majorée explicitement et indépendamment du nombre premier p . Notre démonstration de ce résultat généralise l’approche de Salinier au cas des systèmes différentiels rigides ou, de façon équivalente, au cas des équations différentielles sans paramètre accessoire (cf. [52]). Notons par ailleurs que Crew [32] a également obtenu récemment un résultat similaire en suivant une approche différente fondée sur la cohomologie p -adique. Nous précisons que nous n’avons pris connaissance de l’article [32] qu’après avoir démontré le théorème 1.4.10. Crew montre que, sous les hypothèses 1, 2 et 3 du théorème 1.4.10, si p est un nombre premier tel que L définit un isocrystal *surconvergent*⁸ et vérifiant certaines autres hypothèses (les conditions C_1 et C_3 dans [32]), alors L a une structure de Frobenius forte pour p . Sa preuve repose sur des outils de cohomologie p -adique et le fait que la surconvergence lui permet (Theorem 1 et Theorem 2 de [32]) de définir la rigidité p -adique en termes de cohomologie p -adique. Il montre aussi que la période h obtenue ne dépend pas de p . L’intérêt de notre approche est son aspect plus élémentaire puisqu’elle repose sur les aspects classiques de la théorie des équations différentielles (à la fois sur $\mathbb{C}(z)$ et $\mathbb{C}_p(z)$) et que nous donnons une description précise de l’ensemble des nombres premiers p qui munissent L d’une structure de Frobenius forte. Pour davantage de précisions, notamment sur le lien entre le théorème 1.4.10 et les résultats de Katz [52], Esnault et Groechenig [44] nous renvoyons le lecteur à la partie 2.2.1.

Comme nous l’avons déjà mentionné, les opérateurs hypergéométriques de Gauss à paramètres rationnels sont des exemples d’opérateurs rigides. Considérons l’opérateur hypergéométrique de Gauss

$$L := z(z-1)\frac{d}{dz^2} + (2z-1)\frac{d}{dz} + \frac{1}{4}$$

qui est aussi un opérateur de Picard–Fuchs. L’opérateur L satisfait aux conditions du théorème 1.4.10. Notons que l’ensemble des exposants de L aux points singulier réguliers est $\{0, 1/2\}$ et que $a_0(z) = z(1-z)$. Donc, dans ce cas $\mathfrak{A}_1 = \{-1, 1\}$, $\mathfrak{A}_2 = \{2\}$, $\mathfrak{A}_3 = \{\frac{2z-1}{z(z-1)}, \frac{1}{4z(z-1)}\}$. On en déduit que \mathcal{S} est l’ensemble des nombres premiers différents de 2. De plus, $d = 2$, $\phi(d) = 1$, $h_2 = 1$ et ainsi $h = 1$. D’après le théorème 1.4.10, l’opérateur L est donc muni d’une structure de Frobenius forte de période 1 pour tout nombre premier différent de 2.

1.4.6 Structure de Frobenius forte et équations hypergéométriques

L’application principale que nous obtenons des théorèmes 1.4.6 et 1.4.10 est de montrer que la conjecture 4 est vraie pour la plupart des séries hypergéométriques généralisées. Rappelons que les séries hypergéométriques généralisées sont définies comme suit

$${}_nF_{n-1}(\underline{\alpha}; \underline{\beta}, z) = \sum_{j \geq 0} \frac{(\alpha_1)_j \cdots (\alpha_n)_j}{(\beta_1)_j \cdots (\beta_{n-1})_j j!} z^j$$

où $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Q} \setminus \mathbb{Z}_{\leq 0})^n$, et $\underline{\beta} = (\beta_1, \dots, \beta_{n-1}) \in (\mathbb{Q} \setminus \mathbb{Z}_{\leq 0})^{n-1}$ et, pour $x \in \mathbb{R}$, $(x)_n = x(x+1) \cdots (x+n-1)$ et $(x)_0 = 1$.

La série hypergéométrique ${}_nF_{n-1}(\underline{\alpha}; \underline{\beta}, z)$ annule l’opérateur différentiel

$$\mathcal{H}(\underline{\alpha}, \underline{\beta}) : -z(\delta + \alpha_1) \cdots (\delta + \alpha_n)y + \delta(\delta + \beta_1 - 1) \cdots (\delta + \beta_{n-1} - 1), \quad (1.10)$$

8. Un opérateur $L \in \mathbb{Q}(z)[d/dz]$ est surconvergent pour un nombre premier p , si le rayon de convergence de L au point générique associé à p est égal à 1. Dans la partie 1.5, le lecteur trouvera la définition de point générique associé à p d’un opérateur différentiel.

où $\delta = z \frac{d}{dz}$. Cet opérateur est appelé *opérateur différentiel hypergéométrique*. L'observation clé est que sous certaines hypothèses cet opérateur satisfait aux trois conditions du théorème 1.4.10.

1. Il est facile de voir que cet opérateur est fuchsien et que ses singularités sont $0, 1$ et ∞ .
2. Les exposants de $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ en zéro sont $1 - \beta_1, \dots, 1 - \beta_{n-1}, 0$, les exposants de $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ en 1 sont $0, 1, \dots, n - 2, -1 + \sum(\beta_j - \alpha_i)$ et les exposants de $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ en l'infini sont $\alpha_1, \dots, \alpha_n$. Puisque $\alpha_i, \beta_j \in \mathbb{Q}$ pour tout $i, j \in \{1, \dots, n\}$, les exposants de $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ aux points singuliers sont des nombres rationnels.
3. Enfin, si $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$, alors l'opérateur $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ est rigide. Il s'agit d'un résultat dû à Levelt (voir le Theorem 3.5 de [14]).

Donc, si $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$, le théorème 1.4.10 implique que l'opérateur $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ possède, pour presque tout p , une structure de Frobenius forte de période h , où h ne dépend pas de p . Plus précisément, nous obtenons le résultat suivant :

Théorème 1.4.11. *Soient $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{n-1}, \beta_n = 1 \in \mathbb{Q} \setminus \mathbb{Z}_{\leq 0}$ tels que pour tout i, j , $\alpha_i - \beta_j \notin \mathbb{Z}$ et \mathcal{S}' l'ensemble des nombre premiers p tel que $|\alpha_i|_p, |\beta_j|_p \leq 1$ pour tout $i, j \in \{1, \dots, n\}$. Alors, pour tout $p \in \mathcal{S}'$, l'opérateur $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ possède une structure de Frobenius forte pour p de période $\varphi(d_{\alpha, \beta})$, où φ est l'indicatrice d'Euler et $d_{\alpha, \beta}$ est le plus petit commun multiple des dénominateurs des nombres rationnels $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$.*

Finalement, avec les notations du théorème 1.4.11, il est clair que $\mathcal{S} \subset \mathcal{S}'$, où \mathcal{S} est l'ensemble des nombres premiers p tels que p ne divise pas $d_{\alpha, \beta}$ et ${}_nF_{n-1}(\underline{\alpha}, \underline{\beta}, z) \in \mathbb{Z}_{(p)}[[z]]$. Ainsi, le théorème suivant découle des théorèmes 1.4.6 et 1.4.11.

Théorème 1.4.12. *Soient $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_{n-1}, \beta_n = 1 \in \mathbb{Q} \setminus \mathbb{Z}_{\leq 0}$ tels que pour tout i, j , $\alpha_i - \beta_j \notin \mathbb{Z}$. Soit $d_{\alpha, \beta}$ le plus petit commun multiple des dénominateurs des nombres rationnels $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ et soit \mathcal{S} l'ensemble des nombres premiers p tels que p ne divise pas $d_{\alpha, \beta}$ et ${}_nF_{n-1}(\underline{\alpha}, \underline{\beta}, z) \in \mathbb{Z}_{(p)}[[z]]$. Alors, pour tout $p \in \mathcal{S}$, ${}_nF_{n-1}(\underline{\alpha}, \underline{\beta}, z)$ est algébrique modulo p de degré majoré par $p^{n^2 \phi(d_{\alpha, \beta})}$, où ϕ désigne l'indicatrice d'Euler.*

Rappelons que la conjecture 4 est vraie pour les G -fonctions qui sont dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ et pour la classe de G -fonctions étudiées dans [5]. Les séries ${}_nF_{n-1}(\underline{\alpha}, \underline{\beta}, z)$ du théorème 1.4.12 sont également des G -fonctions, mais elles ne sont pas forcément dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ ou dans la classe de G -fonctions étudiées dans [5]. Le théorème 1.4.12 fournit ainsi de nouveaux exemples de G -fonctions qui vérifient la conjecture 4. Illustrons cela à l'aide des exemples suivants.

Exemple 1.4.13. *Considérons les séries hypergéométriques*

$$f_2(z) := {}_3F_2 \left(\frac{1}{9}, \frac{4}{9}, \frac{5}{9}; \frac{1}{3}, 1, z \right) \quad \text{et} \quad f_3(z) := {}_2F_1 \left(\frac{1}{3}, \frac{1}{2}; \frac{5}{12}, z \right).$$

La série $f_2(z)$ est globalement bornée car $f_2(27^2 z) \in \mathbb{Z}[[z]]$ par contre, à ce jour, nous ne savons toujours pas si $f_2(z)$ est dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$. D'autre part, d'après [5, Example 8.6], la série $f_2(z)$ n'est pas dans la famille étudiée dans [5]. Puisque $f_2(27^2 z) \in \mathbb{Z}[[z]]$, on a $f_2(z) \in \mathbb{Z}_{(p)}[[z]]$ pour tout $p \neq 3$. Notons que dans ce cas $d_{\alpha, \beta} = 9$, avec $\underline{\alpha} = (\frac{1}{9}, \frac{4}{9}, \frac{5}{9})$ et $\underline{\beta} = (\frac{1}{3}, 1)$. Le théorème 1.4.12 garantit donc que, pour tout nombre premier $p \neq 3$, $f_2|_p$ est algébrique sur $\mathbb{F}_p(z)$ de degré majoré par p^{54} .

Nous savons que la série $f_3(z)$ n'est pas dans $\mathbf{Diag}_{\mathbb{Q}}^{alg}$ car elle n'est pas globalement bornée (voir proposition 1 de [27]). D'autre part, d'après la section 8 de [5], elle n'appartient pas à la classe de G -fonctions considérée dans [5]. Par contre, le théorème 1.4.12 s'applique. En effet, soit \mathcal{S} l'ensemble des nombres premiers tels que $f_3(z) \in \mathbb{Z}_{(p)}[[z]]$. Cet ensemble est infini car si p est un nombre premier congruent à 1 modulo 12, alors $p \in \mathcal{S}$. Dans ce cas, on vérifie que $d_{\underline{\alpha}, \underline{\beta}} = 12$, $\underline{\alpha} = (\frac{1}{3}, \frac{1}{2})$ et $\underline{\beta} = (\frac{5}{12})$. D'après le théorème 1.4.12, si $p > 3$ appartient à \mathcal{S} , alors $f_{3|p}$ est algébrique sur $\mathbb{F}_p(z)$ de degré majoré par p^{16} .

1.5 Algébricité modulo p de G -fonctions et conjecture de Bombieri-Dwork.

Le but de cette partie est d'énoncer la conjecture de Bombieri–Dwork et de montrer qu'elle implique le premier point de la conjecture 4.

La notion de convergence au point générique est fondamentale dans l'énoncé de la conjecture de Bombieri–Dwork. Étant donné un nombre premier p et $G = (g_{i,j}(z))_{1 \leq i,j \leq n} \in \mathcal{M}_n(E_p)$, nous posons $\|G\|_{\mathcal{G},p} = \max\{|h_{i,j}(z)|_{\mathcal{G}}\}$. Soient $L \in \overline{\mathbb{Q}}[z][d/dz]$ et A la matrice compagnon de L . Considérons la suite de matrices A_s définie par la formule suivante : A_0 la matrice identité, $A_1 = A$ et $A_{s+1} = \frac{d}{dz}A_s + A_s A$. Étant donné un nombre premier p , le rayon de convergence de L au point générique associé à p est le nombre réel positif $r_p(L)$ défini par

$$\frac{1}{r_p(L)} = \lim_{s \rightarrow \infty} \left\| \frac{A_s}{s!} \right\|_{\mathcal{G},p}^{1/s}.$$

Il suit de [10, chapter IV 2.5] que $r_p(L) > 0$ pour tout nombre premier p . Nous disons que l'opérateur différentiel L est de *type arithmétique* (voir Bombieri [15]), si

$$\sum_{p \text{ premier}} \text{Log}^+(1/r_p(L)) < \infty,$$

où $\text{Log}^+(1/r_p(L)) = \max\{0, \text{Log}(1/r_p(L))\}$.

La conjecture de Bombieri–Dwork, donnée pour la première fois dans [40, p.2], provient d'une question traitée par Dwork dans [39] : si $f(z) = \sum_{j \geq 0} a(j)z^j \in \mathbb{Q}[[z]]$ alors, pour chaque nombre premier p , on peut voir $f(z)$ comme une série formelle à coefficients dans l'anneau \mathbb{C}_p et ainsi calculer son rayon de convergence p -adique, $r_p(f)$; la question est de déterminer la valeur de $r_p(f)$ et notamment de comprendre la variation de $r_p(f)$ en fonction de p .

Supposons que $f(z)$ est solution d'un opérateur différentiel $L \in \mathbb{Q}(z)[d/dz]$ d'ordre n tel que zéro est un point singulier régulier. D'après le Theorem 3 de [29], $r_p(f) > 0$. Supposons de plus que les exposants de L en zéro appartiennent à $\mathbb{Q} \cap \mathbb{Z}_p$, alors L admet une base de solution de la forme

$$(F_1, \dots, F_n) \exp(\theta \text{Log} z)$$

où $F_1, \dots, F_n \in \mathbb{Q}[[z]]$ et θ est une matrice à coefficients dans \mathbb{Q} . Dwork montre dans [37, Theorem 6] que si L est une équation de Picard–Fuchs alors, pour tout $i \in \{1, \dots, n\}$, $r_p(F_i) \geq 1$ pour presque tout nombre premier p ; en particulier $r_p(f) \geq 1$ pour presque tout nombre premier p . D'autre part, Christol a montré dans [24, théorème 2] le fait suivant : pour tout $i \in \{1, \dots, n\}$, $r_p(F_i) \geq 1$ si et seulement si $r_p(L) = 1$. Par conséquent, si L est une équation de Picard–Fuchs, alors $r_p(L) = 1$ pour presque tout nombre premier p .

On dit qu'un opérateur différentiel à coefficients dans $\overline{\mathbb{Q}}(z)$ provient de la géométrie s'il peut se factoriser sous la forme $L_1 \circ \cdots \circ L_t$, où les L_i sont des facteurs d'équations de Picard–Fuchs.

Comme nous l'avons vu, pour presque tout nombre premier p , le rayon de convergence au point générique des équations de Picard–Fuchs est égal à 1 et, d'après la proposition 1 de [10, IV 2.5], le rayon de convergence au point générique des équations qui proviennent de la géométrie est égal à 1 pour presque tout nombre premier p . Ainsi, si L provient de la géométrie, L est de type arithmétique. La conjecture de Bombieri–Dwork affirme que les uniques opérateurs différentiels de type arithmétique sont les opérateurs qui proviennent de la géométrie :

Conjecture 5 (Bombieri–Dwork). *Soit $L \in \overline{\mathbb{Q}}(z)[d/dz]$. Si L est de type arithmétique, alors L provient de la géométrie.*

Suivant la terminologie d'André [10, p.76], les opérateurs de type arithmétique sont appelés G -opérateurs. Sous cette terminologie la conjecture de Bombieri–Dwork prédit que tout G -opérateur provient de la géométrie.

Affirmation 1.5.1. *Si la conjecture de Bombieri–Dwork est vraie alors le point 1 de la conjecture 4 l'est également.*

Voici une esquisse de justification pour cette affirmation. Soient $f(z) \in K[[z]]$ une G -fonction, où K est une extension finie de \mathbb{Q} et \mathcal{S} un ensemble infini d'idéaux premiers \mathfrak{p} de ϑ_K tel que $f \in \vartheta_{K,\mathfrak{p}}[[z]]$ pour tout $\mathfrak{p} \in \mathcal{S}$. Soit $\mathcal{M}_f \in \overline{\mathbb{Q}}(z)[d/dz]$ l'opérateur d'ordre minimal annulé par f . Il suit du théorème de Chudnosvky (Theorem 1.5 de [42, Chap. VIII]) et du théorème de Bombieri–André (Theorem 2.1 de [42, Chap. VII]) que \mathcal{M}_f est de type arithmétique; d'après la conjecture de Bombieri–Dwork, \mathcal{M}_f provient de la géométrie.

Soit M le module différentiel associé à l'opérateur \mathcal{M}_f . Comme \mathcal{M}_f provient de la géométrie, le module M peut être obtenu au moyen des constructions algébriques \otimes , \wedge , \oplus et Ext des modules M_i , où M_i est un module différentiel associé à une équation de Picard–Fuchs. Ainsi, les modules M_i sont munis d'une structure de Frobenius forte pour presque tout p et puisque la structure de Frobenius forte est préservée par les foncteurs \otimes , \wedge , \oplus et Ext, on obtient que le module M est muni d'une structure de Frobenius forte pour presque tout nombre premier p . Par conséquent, \mathcal{M}_f possède une structure de Frobenius forte pour presque tout nombre premier p .

Considérons maintenant l'ensemble \mathcal{S}' des idéaux premiers \mathfrak{p} de ϑ_K qui sont dans \mathcal{S} et qui sont au-dessus des nombres premiers p pour lesquels \mathcal{M}_f est muni d'une structure de Frobenius forte. Donc, \mathcal{S}' est infini et $\mathcal{S} \setminus \mathcal{S}'$ est fini. Comme nous l'avons mentionné, le théorème 1.4.6 reste valide pour les opérateurs différentiels à coefficients dans $\overline{\mathbb{Q}}(z)$ et $f \in \vartheta_{K,\mathfrak{p}}[[z]]$. Cela entraîne que, pour tout $\mathfrak{p} \in \mathcal{S}'$, $f|_{\mathfrak{p}}(z)$ est algébrique sur $(\vartheta_{K,\mathfrak{p}}/\mathfrak{p})(z)$ de degré majoré par $p^{n^2 h_p}$, où n est l'ordre de \mathcal{M}_f et h_p est la période de la structure de Frobenius forte qui correspond au nombre premier p . Par conséquent, nous aurions que la conjecture de Bombieri–Dwork impliquerait le point 1 de la conjecture 4.

Notons qu'avec cette approche nous ne pouvons pas conclure que le point 2 de la conjecture 4 est également vérifié. En effet, nous ne savons pas a priori comment varie la période h_p en fonction de p . D'où l'importance du théorème 1.4.10. En effet, celui-ci nous garantit que, pour les opérateurs rigides, il existe un entier c telle que $h_p \leq c$ pour tout nombre premier p pour lequel l'opérateur possède une structure de Frobenius forte.

1.6 Applications combinatoires et arithmétiques

Dans cette partie, nous passons en revue quelques applications combinatoires et arithmétiques de l'algébricité modulo p .

1.6.1 Ensembles p -automatiques et congruences à la Lucas

Dans cette partie, nous rappelons un résultat de Christol [20] qui établit une équivalence entre la notion de *suite p -automatique* et l'algébricité modulo p , où p est un nombre premier. Ce résultat montre qu'une suite dans un corps fini de caractéristique p est p -automatique si et seulement si la série génératrice de cette suite est algébrique sur le corps des fractions rationnelles à coefficients dans ce corps. Le théorème de Christol est à l'origine d'une interaction très riche entre la théorie d'automates, la combinatoire, l'algèbre et la théorie de nombres.

La notion de *suite k -automatique*, où k est un entier supérieur ou égal à 2, a été introduite par Cobham en 1972 [31] :

Définition 1.6.1. Soient k un entier supérieur ou égal à 2 et A_k l'alphabet $\{0, 1, \dots, k-1\}$. Un k -*automate* est un 6-uplet $\mathcal{A} = (Q, A_k, \lambda, q_0, Y, \phi)$, où Q est un ensemble fini appelé ensemble d'états, $\lambda : Q \times A_k \rightarrow Q$ est la fonction de transition, q_0 est l'état initial, Y est un ensemble fini appelé alphabet de sortie et $\phi : Q \rightarrow Y$ est la fonction de sortie. Étant donné un état $q \in Q$ et un mot $w = w_1 w_2 \cdots w_n$ de l'alphabet A_k , nous définissons $\lambda(q, w)$ récursivement en posant $\lambda(q, w) = \lambda(\lambda(q, w_1 w_2 \cdots w_{n-1}), w_n)$. Si $n \in \mathbb{N}$ et $n = \sum_{i=0}^r w_i k^i$ est le développement de n en base k , on note $\langle n \rangle_k = w_r w_{r-1} \cdots w_0$.

On dit qu'une suite $(a_n)_{n \geq 0}$ à valeurs dans l'ensemble Y est k -*automatique* s'il existe un k -automate \mathcal{A} tel que, pour tout $n \geq 0$, $a_n = \phi(\lambda(q_0, \langle n \rangle_k))$.

Un exemple célèbre de suite automatique est la suite de Thue-Morse $(t_n)_{n \geq 0}$. Cette suite est définie de la façon suivante : $t_n = 0$ si la somme des chiffres binaires de n est paire et $t_n = 1$ dans le cas contraire. Cette suite est 2-automatique car elle est engendrée par le 2-automate $\mathcal{A} = (\{0, 1\}, A_2, \lambda, 0, \{0, 1\}, \phi)$, où $\lambda((0, 0)) = \lambda((1, 1)) = 0$, $\lambda((0, 1), (1, 0)) = 1$ et $\phi(0) = 0$, $\phi(1) = 1$.

Montrons maintenant que la série génératrice de la suite de Thue-Morse est algébrique sur $\mathbb{F}_2(z)$. Soit $F(z) = \sum_{n \geq 0} t_n z^n \in \mathbb{F}_2[[z]]$, où $(t_n)_{n \geq 0}$ est la suite de Thue-Morse (vue dans \mathbb{F}_2). La définition de la suite de Thue-Morse implique que $t_{2n} = t_n$ et $t_{2n+1} = 1 + t_n$, pour tout $n \geq 0$. On obtient alors

$$\begin{aligned} F(z) &= \sum_{n \geq 0} t_n z^{2n} + \sum_{n \geq 0} t_{2n+1} z^{2n+1} \\ &= \sum_{n \geq 0} t_n z^{2n} + \sum_{n \geq 0} (1 + t_n) z^{2n+1} \\ &= \left(\sum_{n \geq 0} t_n z^n \right)^2 + z \left(\sum_{n \geq 0} t_n z^n \right)^2 + z \left(\sum_{n \geq 0} z^n \right)^2 \\ &= (1 + z)F(z)^2 + z \frac{1}{(1 + z)^2}. \end{aligned}$$

Ainsi, $F(z)$ annule le polynôme $(1 + z)^3 Y^2 + (1 + z)^2 Y + z$ et par conséquent, $F(z)$ est algébrique sur $\mathbb{F}_2(z)$, de degré 2. Le théorème de Christol est le suivant :

Théorème D (Christol [20]). Soient p un nombre premier et $(a(n))_{n \geq 0}$ une suite à coefficients dans \mathbb{F}_p . La suite $(a(n))_{n \geq 0}$ est p -automatique si et seulement si la série $\sum_{n \geq 0} a(n)z^n$ est algébrique sur $\mathbb{F}_p(z)$.

Congruences automatiques. Commençons par rappeler la notion de k -noyau d'une suite.

Définition 1.6.2. Étant donnée une suite $\mathbf{a} = (a(n))_{n \geq 0}$, le k -noyau de \mathbf{a} est l'ensemble $\mathcal{N}(\mathbf{a})$ défini par

$$\mathcal{N}(\mathbf{a}) := \{(a(nk^h + r))_{n \geq 0} : h \geq 0, 0 \leq r \leq k^h - 1\}.$$

Étant donné $j \in \{0, 1, \dots, k-1\}$, on définit l'opérateur Λ_j (appelé à nouveau opérateur de Cartier, ou encore opérateur de section) qui associe à une suite $\mathbf{a} = (a(n))_{n \geq 0}$ la suite $\Lambda_j(\mathbf{a}) = (a(nk + j))_{n \geq 0}$. Soit Ω_k le semi-groupe engendré par l'identité et les Λ_j pour la loi de composition. On a alors

$$\mathcal{N}(\mathbf{a}) = \{\Lambda(\mathbf{a}) : \Lambda \in \Omega_k\}.$$

On obtient alors la caractérisation suivante d'une suite k -automatique.

Théorème E (Eilenberg [43]). Une suite est k -automatique si et seulement si son k -noyau est fini.

Il découle donc des théorèmes B, D et E que si $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Z}[[z]]$ est la diagonale d'une série algébrique et p est un nombre premier alors la suite $(a(n))_{n \geq 0}$ vérifie de nombreuses congruences modulo p , appelées « congruences automatiques ». Par exemple, si $j \in \{0, \dots, p-1\}$, alors il existe des entiers h, e, j' tels que $h \geq 0, e \geq 1, 0 \leq j' \leq p^e - 1$ et, pour tout entier $n \geq 0$,

$$a(np^h + p^{h-1}j + \dots + pj + j) \equiv a(np^e + j') \pmod{p}.$$

Dans la plupart des exemples que nous allons traiter, nous retrouverons la congruence suivante :

$$a(pn) \equiv a(n) \pmod{p}$$

pour tout entier $n > 0$ et tout nombre premier p . Par exemple, nous avons déjà vu que la série $\mathbf{g}(z) = \sum_{n \geq 0} \binom{2n}{n} z^n$ est la diagonale d'une série algébrique et, d'après l'égalité (1.1), on a

$$\binom{2np}{np} \equiv \binom{2n}{n} \pmod{p}$$

pour tout entier $n > 0$ et tout nombre premier p .

Les coefficients binomiaux et le théorème de Lucas. Le coefficient binomial $\binom{n}{m}$ est défini par

$$\binom{n}{m} = \begin{cases} \frac{n!}{m!(n-m)!} & \text{si } n \geq m \\ 0 & \text{si } n < m. \end{cases}$$

Rappelons que $\binom{n}{m}$ représente le nombre de choix d'un sous-ensemble à m éléments dans un ensemble à n éléments. Considérons la série

$$F(X, Y) = \sum_{(n, m) \in \mathbb{N}^2} \binom{n}{m} X^m Y^n$$

et remarquons que $F(X, Y) = \frac{1}{1-(1+X)Y}$ est une fraction rationnelle de deux variables. Ainsi, pour tout nombre premier p , la série $F(X, Y) \pmod p$ appartient à $\mathbb{F}_p(X, Y)$. D'autre part, Salon [63, 64] a donné une généralisation du théorème D pour les séries formelles de plusieurs variables. On obtient donc que la suite $\{\binom{n}{m} \pmod p\}_{n, m \geq 0}$ est p -automatique pour tout nombre premier p . Cela implique l'existence de congruences automatiques pour les coefficients binomiaux. On peut en fait obtenir un résultat bien plus précis ; il s'agit du théorème de Lucas :

Théorème F (Théorème de Lucas [55]). *Soient n et m des entiers et p un nombre premier. Notons $n = \sum_{i=0}^s n_i p^i$ et $m = \sum_{i=0}^s m_i p^i$ les développements respectifs de n et m en base p . Alors, on a*

$$\binom{n}{m} \equiv \prod_{i=0}^s \binom{n_i}{m_i} \pmod p.$$

Le théorème de Lucas se démontre très simplement à l'aide du théorème du binôme, comme l'a noté Fine [45].

Démonstration. Soit p un nombre premier. Alors, pour tout $i \geq 0$, $(1+X)^{p^i} \equiv 1+X^{p^i} \pmod p$ et d'après le théorème du binôme $\sum_{m=0}^n \binom{n}{m} X^m = (1+x)^n$. Ainsi, sous les hypothèses du théorème de Lucas on a

$$\begin{aligned} \sum_{m=0}^n \binom{n}{m} X^m &= (1+x)^n = \prod_{i=0}^s (1+X)^{n_i p^i} \equiv \prod_{i=0}^s (1+X^{p^i})^{n_i} \pmod p \\ &= \prod_{i=0}^s \left(\sum_{m_i=0}^{n_i} \binom{n_i}{m_i} X^{m_i p^i} \right) \pmod p \\ &= \sum_{m=0}^n \left(\prod_{i=0}^s \binom{n_i}{m_i} \right) X^m \pmod p. \end{aligned}$$

On conclut en comparant les coefficients en X^m dans cette congruence. \square

Le théorème de Lucas s'avère être un outil pertinent pour obtenir l'algébricité modulo p de certaines séries. C'est le cas dans l'exemple suivant :

Exemple 1.6.3. *Montrons que la série*

$$\mathfrak{g}_r(z) = \sum_{n \geq 0} \binom{2n}{n}^r z^n$$

est algébrique modulo p pour tout nombre premier p et tout entier $r \geq 1$.

D'après le théorème de Lucas, pour tout couple d'entiers (n, k) et pour tous $l, s \in \{0, 1, \dots, p-1\}$, on a

$$\binom{np+l}{kp+s} \equiv \binom{n}{k} \binom{l}{s} \pmod p.$$

Ainsi, pour tout $r \geq 1$, tout nombre premier p , tout entier n et tout $m \in \{0, 1, \dots, p-1\}$, on a

$$\binom{2(np+m)}{np+m}^r \equiv \begin{cases} \binom{2n}{n}^r \binom{2m}{m}^r \pmod p & \text{si } m \in \{0, 1, \dots, (p-1)/2\} \\ \binom{2n+1}{n}^r \binom{2m-p}{m}^r \pmod p & \text{si } m \in \{(p+1)/2, \dots, p-1\}. \end{cases}$$

Mais $\binom{2m-p}{m} = 0$ puisque $2m - p < m$. On obtient donc

$$\begin{aligned} \mathfrak{g}_{r|p} &= \sum_{m=0}^{(p-1)/2} \sum_{n=0}^{\infty} \left(\binom{2n}{n}^r \binom{2m}{m}^r \pmod{p} \right) z^{np+m} \\ &= \left(\sum_{m=0}^{(p-1)/2} \left(\binom{2m}{m}^r \pmod{p} \right) z^m \right) \left(\sum_{n=0}^{\infty} \left(\binom{2n}{n}^r \pmod{p} \right) z^{np} \right) \\ &= \left(\sum_{m=0}^{(p-1)/2} \left(\binom{2m}{m}^r \pmod{p} \right) z^m \right) \mathfrak{g}_{r|p}(z^p). \end{aligned}$$

Puisque $\mathfrak{g}_{r|p}(z) \in \mathbb{F}_p[[z]]$, on a $\mathfrak{g}_{r|p}(z^p) = \mathfrak{g}_{r|p}(z)^p$. Notamment, pour tout $r \geq 1$ et pour tout nombre premier p , on a

$$\mathfrak{g}_{r|p}(z) = \left(\sum_{m=0}^{(p-1)/2} \left(\binom{2m}{m}^r \pmod{p} \right) z^m \right) \mathfrak{g}_{r|p}(z)^p.$$

Ainsi, pour tout $r \geq 1$ et pour tout nombre premier p , la série $\mathfrak{g}_{r|p}$ est algébrique sur $\mathbb{F}_p(z)$. De plus, son degré d'algébricité est majoré par $p - 1$.

La série \mathfrak{g}_r est un exemple de ce qu'on appelle une série p -Lucas.

Congruences « à la Lucas ». De nombreuses suites, étudiées notamment en combinatoire énumérative, ont la propriété de satisfaire des congruences de type « p -Lucas » pour une infinité de nombres premiers p .

Définition 1.6.4. Soient $(a(n))_{n \geq 0}$ une suite à coefficients dans \mathbb{Q} et p un nombre premier. On dit que la suite est p -Lucas si :

1. $a(0) = 1$;
2. pour tout $n \geq 0$, $a(n) \in \mathbb{Z}_{(p)}$, c'est-à-dire, pour tout entier $n \geq 0$, p ne divise pas le dénominateur de $a(n)$;
3. pour tout $k \geq 0$ et tout $r \in \{0, 1, \dots, p-1\}$, $a(kp+r) \equiv a(k)a(r) \pmod{p}$.

Par abus de langage on dit que la série $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Q}[[z]]$ est p -Lucas si la suite $(a(n))_{n \geq 0}$ est p -Lucas. Une remarque très simple mais fondamentale pour la suite est la suivante :

Remarque 1.6.5. Soient $f(z) = 1 + \sum_{n \geq 1} a(n)z^n \in \mathbb{Q}[[z]]$ et p un nombre premier tels que $f(z) \in \mathbb{Z}_{(p)}[[z]]$. Alors, la série f est p -Lucas si et seulement si

$$f_{|p}(z) = \left(\sum_{n=0}^{p-1} (a(n) \pmod{p}) z^n \right) f_{|p}(z^p). \quad (1.11)$$

Comme $f_{|p}(z)$ est à coefficients dans \mathbb{F}_p , on a $f_{|p}(z^p) = f_{|p}(z)^p$. De plus, l'égalité (1.11) entraîne que, pour tout entier $n \geq 0$,

$$a(pn) \equiv a(n) \pmod{p}.$$

La remarque 1.6.5 implique que si $f(z) \in \mathbb{Q}[[z]]$ est p -Lucas, alors $f|_p$ est algébrique sur $\mathbb{F}_p(z)$ et le degré d'algébricité de $f|_p$ est au plus $p - 1$. Au vu des questions 1 et 2, il est naturel de chercher à savoir quand une série est p -Lucas pour une infinité de nombres premiers p . Dans [5] les auteurs ont montré qu'il y a une grande classe de G -fonctions qui sont p -Lucas pour un infinité de nombres premiers p . Cette classe de G -fonctions contient certaines séries hypergéométriques généralisées et de certaines séries obtenues par spécialisation de séries de plusieurs variables dont les coefficients sont des quotients de factorielles de plusieurs variables. L'approche utilisée dans [5] pour démontrer que ces séries sont p -Lucas repose sur un étude détaillé de la valuation p -adique de leurs coefficients. À présent nous allons décrire ces deux familles de séries formelles.

Séries hypergéométriques généralisées. Soient $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Q}^n \cap (0, 1]^n$, $\underline{\beta} = (\beta_1, \dots, \beta_{n-1}) \in \mathbb{Q}^n \cap (0, 1]^{n-1}$ et $d_{\alpha, \beta}$ le plus petit commun multiple des dénominateurs des α_i et les β_j . On pose $\Delta_{\underline{\alpha}, \underline{\beta}} : \mathbb{R} \rightarrow \mathbb{Z}$ défini par

$$\Delta_{\underline{\alpha}, \underline{\beta}}(x) = \sum_{i=1}^n [x - \alpha_i] - \sum_{j=1}^{n-1} [x - \beta_j] - [x - 1]$$

et $m_{\underline{\alpha}, \underline{\beta}} = \min\{\alpha_1, \dots, \alpha_n, \beta_1, \beta_{n-1}, 1\}$.

Théorème G (Proposition 8.5 de [5]). *Si $\Delta_{\underline{\alpha}, \underline{\beta}}(x) \geq 1$ pour tout $x \in [m_{\underline{\alpha}, \underline{\beta}}, 1)$, alors la série hypergéométrique ${}_nF_{n-1}(\underline{\alpha}, \underline{\beta})$ est p -Lucas pour tout nombre premier p tel que $p \equiv 1 \pmod{d_{\alpha, \beta}}$.*

Il suit donc de ce théorème que la série $f_1(z) = {}_2F_1(1/2, 1/2; 2/3, z)$ est p -Lucas pour tout nombre premier p congru à 1 modulo 6, tandis que ce critère ne s'applique pas à la série $f_3(z) := {}_2F_1(\frac{1}{3}, \frac{1}{2}; \frac{5}{12}, z)$ car $\Delta_{(1/3, 1/2), (5/12)}(5/12) = 0$ et $5/12 \in [1/3, 1)$ et $1/3 = m_{(1/3, 1/2), (5/12, 1)}$.

Quotients de factorielles et spécialisations. Soient $e = (\mathbf{e}_1, \dots, \mathbf{e}_u)$ et $f = (\mathbf{f}_1, \dots, \mathbf{f}_v)$ deux vecteurs à coefficients dans \mathbb{N}^d . Notons $|e| = \sum_{i=1}^u \mathbf{e}_i$ et $|f| = \sum_{j=1}^v \mathbf{f}_j$. Etant donné $\mathbf{n} \in \mathbb{N}^d$, on pose

$$\mathcal{Q}_{e, f}(\mathbf{n}) = \frac{\prod_{i=1}^u (\mathbf{e}_i \cdot \mathbf{n})!}{\prod_{j=1}^v (\mathbf{f}_j \cdot \mathbf{n})!}$$

et

$$F_{e, f}(\mathbf{x}) = \sum_{\mathbf{n} \in \mathbb{N}^d} \mathcal{Q}_{e, f}(\mathbf{n}) \mathbf{x}^{\mathbf{n}}.$$

Considérons la fonction de Landau $\Delta_{e, f} : \mathbb{R}^d \rightarrow \mathbb{Z}$ définie par

$$\Delta_{e, f}(\mathbf{x}) = \sum_{i=1}^u [\mathbf{x} \cdot \mathbf{e}_i] - \sum_{j=1}^v [\mathbf{x} \cdot \mathbf{f}_j].$$

Considérons aussi l'ensemble

$$\mathcal{D}_{e, f} = \{\mathbf{x} \in [0, 1)^d : \exists \mathbf{d} \in \{\mathbf{e}_1, \dots, \mathbf{e}_u, \mathbf{f}_1, \dots, \mathbf{f}_v\} \text{ tel que } \mathbf{x} \cdot \mathbf{d} \geq 1\}.$$

Soit \mathfrak{F} l'ensemble constitué des séries $F_{e, f}(\mathbf{x})$ telles que $|e| = |f|$ et $\Delta_{e, f}(\mathbf{x}) \geq 1$ pour tout $x \in \mathcal{D}_{e, f}$. On pose également

$$\mathcal{N}_{e, f} = \{\mathbf{n} \in \mathbb{N}^d \text{ tel que pour tout } \mathbf{z} \in [0, 1)^d \text{ avec } \mathbf{z} \cdot \mathbf{n} \geq 1 \text{ on a } \Delta_{e, f}(\mathbf{z}) \geq 1\}.$$

Théorème H (Proposition 8.10 de [5]). Soit $f(z) = F_{e,f}(b_1 z^{n_1}, \dots, b_d z^{n_d})$, où $F_{e,f}(\mathbf{x})$ appartient à \mathfrak{F} , (n_1, \dots, n_d) appartient à $\mathcal{N}_{e,f}$ et (b_1, \dots, b_d) appartient à \mathbb{Q}^d . Alors, la série $f(z)$ est p -Lucas pour tout nombre premier p tel que $(b_1, \dots, b_d) \in \mathbb{Z}_{(p)}^d$.

Les auteurs de [5] observent que de nombreuses séries génératrices provenant de la combinatoire et de la théorie de nombres peuvent s'obtenir par spécialisation de séries qui appartiennent à \mathfrak{F} . Illustrons cette affirmation en montrant que la série génératrice des nombres d'Apéry

$$\mathbf{a}_1(z) = \sum_{n \geq 0} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \right) z^n$$

peut être obtenue par spécialisation d'un élément de \mathfrak{F} .

Considérons la suite $a(n) = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2$. Cette suite a été introduite par Apéry [12] dans sa démonstration de l'irrationalité de $\zeta(3)$. Remarquons d'abord que la série $\mathbf{a}_1(z)$ est une G -fonction. En effet, $\mathbf{a}_1(z)$ est la diagonale de la fraction rationnelle

$$\frac{1}{[1 - z_1 z_2 z_3 z_4][(1 - z_3)(1 - z_4) - z_0(1 + z_1)(1 + z_2)]}.$$

Considérons $e = ((2, 1), (2, 1))$ et $f = ((1, 0), (1, 0), (1, 0), (1, 0), (0, 1), (0, 1))$, alors $|e| = |f|$ et $\mathcal{D}_{e,f} = \{(x_1, x_2) \in (0, 1]^2 : 2x_1 + x_2 \geq 1\}$. Par conséquent, $\Delta_{e,f}(x) \geq 1$ pour tout $x \in \mathcal{D}_{e,f}$ et ainsi la série

$$F_{e,f}(x_1, x_2) = \sum_{(n_1, n_2) \in \mathbb{N}^2} \frac{(2n_1 + n_2)!^2}{n_1!^4 n_2!^2} x_1^{n_1} x_2^{n_2}$$

appartient à \mathfrak{F} . Finalement notons que $\mathbf{a}_1(z) = F_{e,f}(z, z)$ et il suit du théorème H que la série $\mathbf{a}_1(z)$ est p -Lucas pour tout nombre premier p puisque $(1, 1) \in \mathcal{N}_{e,f}$. Ce résultat a été d'abord démontré en 1982 par Gessel [49] à l'aide du théorème de Lucas. Par contre, la stratégie utilisée dans [5] permet d'obtenir de nombreux autres exemples de G -fonctions qui sont p -Lucas pour une infinité de nombres premiers p . Dans [5, Section 8.4], le lecteur trouvera la mise en place de cette stratégie.

Voici un second exemple. Considérons la série

$$\mathbf{a}_2(z) = \sum_{n \geq 0} \left(\sum_{n=0}^k \binom{n}{k}^2 \binom{n+k}{k} \right) z^n.$$

La suite $a(n) = \sum_{n=0}^k \binom{n}{k}^2 \binom{n+k}{k}$ a été aussi introduite par Apéry [12] pour redémontrer l'irrationalité de $\zeta(2)$. Posons $e = ((2, 1), (1, 1))$ et $f = ((1, 0), (1, 0), (1, 0), (0, 1), (0, 1))$, alors $|e| = |f|$ et $\mathcal{D}_{e,f} = \{(x_1, x_2) \in (0, 1]^2 : 2x_1 + x_2 \geq 1 \text{ ou } x_1 + x_2 \geq 1\}$. Par conséquent, $\Delta_{e,f}(x) \geq 1$ pour tout $x \in \mathcal{D}_{e,f}$ et ainsi la série

$$F_{e,f}(x_1, x_2) = \sum_{(n_1, n_2) \in \mathbb{N}^2} \frac{(2n_1 + n_2)!(n_1 + n_2)!}{n_1!^3 n_2!^2} x_1^{n_1} x_2^{n_2}$$

appartient à \mathfrak{F} . Finalement, $\mathbf{a}_2(z) = F_{e,f}(z, z)$ et le théorème H entraîne à nouveau que la série $\mathbf{a}_2(z)$ est p -Lucas pour tout nombre premier p .

Diagonales, structure de Frobenius forte, G -fonctions et automates. Notons $\mathbf{SF}_{\overline{\mathbb{Q}}}$ l'ensemble des séries formelles à coefficients dans $\overline{\mathbb{Q}}$ qui annulent un opérateur différentiel

à coefficients dans $\overline{\mathbb{Q}}(z)$ muni d'une structure de Frobenius forte pour presque tout nombre premier p . Soit $\mathbf{G}_{\overline{\mathbb{Q}}}$ l'ensemble des G -fonctions. Nous avons alors la classification suivante :

$$\mathbf{Diag}_{\overline{\mathbb{Q}}} \subset \mathbf{SF}_{\overline{\mathbb{Q}}} \subset \mathbf{G}_{\overline{\mathbb{Q}}}. \quad (1.12)$$

En effet, si $f(z) \in \mathbf{Diag}_{\overline{\mathbb{Q}}}$, alors $f(z)$ annule un opérateur différentiel de Picard-Fuchs (voir [25]) et donc $f(z) \in \mathbf{SF}_{\overline{\mathbb{Q}}}$. Ainsi $\mathbf{Diag}_{\overline{\mathbb{Q}}} \subset \mathbf{SF}_{\overline{\mathbb{Q}}}$. Maintenant montrons que $\mathbf{SF}_{\overline{\mathbb{Q}}} \subset \mathbf{G}_{\overline{\mathbb{Q}}}$. Soit $f(z) \in \mathbf{SF}_{\overline{\mathbb{Q}}}$, alors $f(z)$ annule un opérateur différentiel L muni d'une structure de Frobenius forte pour presque tout p . Comme L est muni d'une structure de Frobenius forte pour p alors, d'après les propositions 4.1.2, 4.6.4 et 4.7.2 de [23], on a $r_p(L) = 1$. Ainsi, $r_p(L) = 1$ pour presque tout nombre premier p . D'après la proposition 5.1 et le théorème 6.1 de [42, Chap. III], on obtient que les singularités de L sont régulières à exposants rationnels. Enfin, en combinant cette propriété avec le théorème 4.2 [42, Chap. VII] et la proposition 1.1 de [42, Chap. VIII], on obtient que $f(z)$ est une G -fonction.

Considérons $\mathbf{Diag}_{\mathbb{Z}}$ l'ensemble formé par les séries de $\mathbf{Diag}_{\overline{\mathbb{Q}}}$ qui sont à coefficients dans \mathbb{Z} , et de la même façon $\mathbf{SF}_{\mathbb{Z}}$ et $\mathbf{G}_{\mathbb{Z}}$. Désignons par $\mathbf{Aut}_{\mathbb{Z}}$ l'ensemble formé des séries $\sum_{n \geq 0} a(n)z^n \in \mathbb{Z}[[z]]$ telles que, pour presque tout nombre premier p , la suite $(a(n) \bmod p)_{n \geq 0}$ est p -automatique. D'après l'argument précédent, il est clair que

$$\mathbf{Diag}_{\mathbb{Z}} \subset \mathbf{SF}_{\mathbb{Z}} \subset \mathbf{G}_{\mathbb{Z}}.$$

Si le premier point de la conjecture 4 s'avérait vrai, alors le théorème D impliquerait que

$$\mathbf{Diag}_{\mathbb{Z}} \subset \mathbf{SF}_{\mathbb{Z}} \subset \mathbf{G}_{\mathbb{Z}} \subset \mathbf{Aut}_{\mathbb{Z}}.$$

Remarquons d'autre part que l'on a $\mathbf{SF}_{\mathbb{Z}} \subset \mathbf{Aut}_{\mathbb{Z}}$ d'après les théorèmes 1.4.6 et D.

1.6.2 Transcendance de séries formelles

Dans cette partie, nous rappelons que le fait qu'une série $f(z)$ soit p -Lucas pour une infinité de nombres premiers p peut être utilisé pour démontrer la transcendance de $f(z)$ sur $\mathbb{Q}(z)$.

Une source de motivation pour étudier la transcendance de séries formelles sur $\mathbb{Q}(z)$ vient de l'étude des séries génératrices traitées par la combinatoire énumérative. En effet, le fait qu'une série génératrice soit rationnelle ou algébrique reflète, dans une certaine mesure, la structure sous-jacente des objets comptés par ses coefficients (voir [18]). Par exemple, d'après [18, Section 2.4], la structure associée aux coefficients d'une série rationnelle est généralement liée aux marches dans un digraphe ou aux langages réguliers. En outre, savoir qu'une série est rationnelle, algébrique, ou holonome permet d'obtenir des asymptotiques plus ou moins précis, ou des relations de récurrence plus ou moins simples, pour les coefficients de la série en question.

À présent, nous listons quelques approches pour montrer la transcendance sur $\mathbb{Q}(z)$ de séries formelles à coefficients rationnels.

a) Approche analytique. Une première remarque est qu'une série algébrique sur $\mathbb{Q}(z)$ a un rayon de convergence non nul. On obtient ainsi la transcendance de la série $f(z) = \sum_{n > 0} n!z^n$. De plus, le rayon de convergence d'une série algébrique sur $\mathbb{Q}(z)$ est fini, sauf s'il s'agit d'un polynôme. On en déduit la transcendance de la série $\exp(z) = \sum_{n \geq 0} \frac{1}{n!}z^n$. Par contre, ces deux arguments ne s'appliquent jamais aux G -fonctions car elles ont un rayon de convergence non nul et fini (sauf pour les polynômes). Établir la transcendance de G -fonctions nécessite donc des critères plus fins. Dans [46], Flajolet

énonce plusieurs résultats concernant l'asymptotique des coefficients de séries holonomes à coefficients dans \mathbb{Q} . Parmi eux, nous citons le résultat suivant qui est très efficace pour démontrer la transcendance de séries formelles :

Théorème I (Flajolet [46]). *Soit $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Q}[[z]]$. Si $f(z)$ est algébrique sur $\mathbb{Q}(z)$ alors, pour tout $n \geq 0$, on a*

$$a(n) = \frac{\beta^n n^s}{\Gamma(s+1)} \sum_{i=0}^m C_i \omega_i^n + O(\beta^n n^t),$$

où $s \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$, $t < s$, β est un nombre algébrique strictement positif et C_i et ω_i sont des nombres algébriques avec $|\omega_i| = 1$.

En 1980, Stanley [68] a conjecturé que, pour tout $r \geq 2$, la série $\mathfrak{g}_r(z) = \sum_{n \geq 0} \binom{2n}{n}^r z^n$ est transcendante sur $\mathbb{Q}(z)$. Il a démontré que c'est bien le cas lorsque r est pair en utilisant une asymptotique moins précise que celle du théorème I. Cette conjecture a ensuite été résolue indépendamment par Flajolet [46] en 1987 et par Sharif et Woodcock [65] en 1989. La preuve de Flajolet repose sur le théorème I. Elle utilise la formule de Stirling qui implique que

$$\binom{2n}{n}^r \sim \frac{2^{(2n+1/2)r}}{(2\pi n)^{r/2}}, \quad (1.13)$$

pour tout $r \geq 1$, ainsi que la transcendance du nombre π .

b) Approche galoisienne. La théorie de Galois différentielle permet d'associer à une équation différentielle linéaire un groupe, appelé *groupe de Galois* de l'équation. Il s'agit d'un groupe algébrique linéaire, c'est-à-dire qu'il peut être représenté comme un groupe de matrice à coefficients dans le corps des constantes associé à l'équation considérée (le corps \mathbb{C} dans le cas qui nous intéresse ici). Si ce groupe est fini, alors toutes les solutions de l'équations sont algébriques ; les solutions étant choisies dans un espace adapté, appelé extension de Picard-Vessiot. Plus généralement, les relations algébriques entre les solutions de l'équations sont encodées par son groupe de Galois. C'est pourquoi cette théorie est très utile pour démontrer des résultats de transcendance et d'indépendance algébrique de séries holonomes. Nous revoyons le lecteur à [72] pour une introduction complète à cette théorie.

Le théorème suivant est un cas particulier d'un théorème du à Kolchin.

Théorème J (Kolchin [53]). *Soient $a(z) \in \mathbb{Q}(z)$ et $f(z) \in \mathbb{Q}[[z]]$ solution de l'opérateur différentiel $\frac{d}{dz} - a(z)$. Si $f(z)$ est algébrique sur $\mathbb{Q}(z)$ alors il existe un entier n , non nul, tel que $f(z)^n \in \mathbb{Q}(z)$.*

La démonstration donnée par Kolchin de ce théorème repose sur la théorie de Galois différentielle, mais ce résultat peut aussi s'obtenir de façon élémentaire. Illustrons ce théorème avec la série

$$\mathfrak{g}_1(z) = (1 - 4z)^{-1/2} = \sum_{n \geq 0} \binom{2n}{n} z^n.$$

Cette série est algébrique et solution de l'opérateur différentiel $\frac{d}{dz} - \frac{2}{1-4z}$. Le théorème J implique donc qu'il existe un entier n non nul tel que $\mathfrak{g}_1(z)^n \in \mathbb{Q}(z)$. En effet, on a $\mathfrak{g}_1(z)^2 = \frac{1}{1-4z} \in \mathbb{Q}(z)$.

Lorsque l'on veut étudier le groupe de Galois d'un opérateur différentiel fuchsien, le groupe de monodromie joue un rôle central. En effet, ce groupe est alors dense (pour

la topologie de Zariski) dans le groupe de Galois différentiel. En particulier, si la série $f(z) \in \mathbb{Q}[[z]]$ annule un opérateur différentiel fuchsien L à coefficients dans $\mathbb{C}(z)$ et que le groupe de monodromie associé à L est fini, alors $f(z)$ est algébrique sur $\mathbb{Q}(z)$. Dans [14], Beukers et Heckman utilisent cette approche pour caractériser les séries hypergéométriques généralisées qui sont algébriques. Avant d'énoncer leur résultat, nous rappelons la définition d'ensembles entrelacés sur le cercle unité. Soient $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ des nombres rationnels. On dit que les ensembles

$$\{\exp(2\pi i\alpha_1), \dots, \exp(2\pi i\alpha_n)\} \quad \text{et} \quad \{\exp(2\pi i\beta_1), \dots, \exp(2\pi i\beta_n)\}$$

sont *entrelacés sur le cercle unité* si

$$\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \dots < \alpha_n < \beta_n \quad \text{ou} \quad \beta_1 < \alpha_1 < \beta_2 < \alpha_2 < \dots < \beta_n < \alpha_n.$$

Théorème K (Beukers et Heckman [14]). *Soient $\underline{\alpha} = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Q} \setminus \mathbb{Z}_{\leq 0})^n$, $\underline{\beta} = (\beta_1, \dots, \beta_{n-1}) \in (\mathbb{Q} \setminus \mathbb{Z}_{\leq 0})^{n-1}$ et $d_{\alpha, \beta}$ le plus petit commun multiple des dénominateurs des α_i et β_j . Supposons que pour tout $i, j \in \{1, \dots, n\}$, $\alpha_i - \beta_j \notin \mathbb{Z}$. Alors, la série hypergéométrique généralisée ${}_nF_{n-1}(\underline{\alpha}, \underline{\beta}, z)$ est algébrique sur $\mathbb{Q}(z)$ si et seulement si, pour tout entier positif k premier à $d_{\alpha, \beta}$, les ensembles $\{\exp(2\pi i k \alpha_1), \dots, \exp(2\pi i k \alpha_n)\}$ et $\{\exp(2\pi i k \beta_1), \dots, \exp(2\pi i k \beta_n)\}$ sont entrelacés sur le cercle unité.*

La conjecture de Stanley [68] peut être aussi résolue en appliquant le théorème K. En effet, remarquons que, pour tout $r \geq 1$, on a

$$\mathfrak{g}_r(z) = {}_rF_{r-1}((1/2, \dots, 1/2); (1, \dots, 1), 4^r z).$$

A l'aide du théorème K, on vérifie alors facilement que, pour tout $r \geq 2$, la série $\mathfrak{g}_r(z)$ est transcendante, tandis que la série $\mathfrak{g}_1(z)$ est algébrique.

c) Approche utilisant l'algébricité modulo p . Dans cette partie nous allons illustrer comment utiliser l'algébricité modulo p pour déterminer la transcendance sur $\mathbb{Q}(z)$ de certaines séries formelles. Nous rappelons la stratégie de preuve utilisée par Sharif et Woodcock [65] pour démontrer la conjecture de Stanley [68]. Celle-ci repose sur le fait que la série \mathfrak{g}_r est p -Lucas pour tout nombre premier p .

Rappelons que si une série $f(z) \in \mathbb{Z}[[z]]$ est algébrique modulo p pour un ensemble infini de nombres premiers \mathcal{S} et que la suite $\{\deg(f|_p(z))\}_{p \in \mathcal{S}}$ n'est pas bornée, alors $f(z)$ est transcendante. Soit $r \geq 2$. On sait que pour tout nombre premier p , la série \mathfrak{g}_r est p -Lucas. Par conséquent, pour tout nombre premier p ,

$$\mathfrak{g}_{r|p}(z) = \left(\sum_{n=0}^{p-1} \left(\binom{2n}{n} \pmod{p} \right) z^n \right) \mathfrak{g}_{r|p}(z)^p. \quad (1.14)$$

Cela montre que \mathfrak{g} est algébrique modulo p pour tout nombre premier p et que le degré d'algébricité de $\mathfrak{g}_{r|p}$ divise $p - 1$. Sharif et Woodcock montrent que si A est un entier positif, il existe un ensemble \mathcal{S}_A infini de nombres premiers tel que si $p \in \mathcal{S}_A$ et l divise $p - 1$, alors $l = 1, 2$ ou $l > A$. Ils parviennent à en déduire que pour tout nombre premier p dans \mathcal{S}_A tel que $p > 3^{r-1}$ on a $\deg(\mathfrak{g}_{r|p}) > A$. Ainsi, la suite $(\deg(\mathfrak{g}_{r|p}))_{p \in \mathcal{P}}$, où \mathcal{P} désigne l'ensemble des nombres premiers, n'est pas bornée et par conséquent, \mathfrak{g}_r est transcendante pour $r \geq 2$.

Allouche, Gouyou-Beauchamps et Skordev ont généralisé cette approche dans [8].

Théorème L (Allouche, Gouyou-Beauchamps et Skordev [8]). *Soit s un entier supérieur ou égal à 2. On pose $s' = s$ si s est pair et $s' = 2s$ si s est impair. Soient $f(z) \in 1 + z\mathbb{Q}[[z]]$ et \mathcal{S} l'ensemble des nombres premiers p tels que p est congru à 1 modulo s' . Les affirmations suivantes sont équivalentes :*

- (i) *la série $f(z)$ est algébrique et pour presque tout nombre premier $p \in \mathcal{S}$, la série $f(z)$ est p -Lucas ;*
- (ii) *il existe un polynôme $P(z) \in \mathbb{Q}[z]$ de degré inférieur ou égal à s' , avec $P(0) = 1$, tel que $f(z) = P(z)^{-1/s'}$.*

Ce résultat implique que si $f(z)$ est p -Lucas pour presque tout nombre premier p , alors la série $f(z)$ est algébrique si, et seulement si, il existe un polynôme de degré inférieur ou égal à 2 tel que $P(0) = 1$ et $f(z) = P(z)^{-1/2}$. Il est par exemple montré dans [8], à l'aide du théorème L, que la série génératrice des nombre d'Apéry

$$\mathfrak{a}_1(z) = \sum_{n \geq 0} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \right) z^n$$

est transcendante .

Plus récemment, Adamczewski et Bell [1] ont montré comment utiliser les équations (1.11) pour obtenir l'indépendance algébrique sur $\mathbb{Q}(z)$ de certaines séries p -Lucas. Cette approche a ensuite été développée par Adamczewski, Bell et Delaygue dans [2]. Ces auteurs ont introduit de nouveaux ensembles de séries formelles, les ensembles $\mathcal{L}(\mathcal{S})$, qui généralisent les ensembles de séries p -Lucas. Ils ont donné un critère d'indépendance algébrique pour les éléments de $\mathcal{L}(\mathcal{S})$ qui permet par exemple de démontrer que les séries $\mathfrak{g}_r(z)$, $r \geq 2$, et $\mathfrak{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. Ces résultats sont décrits dans la partie suivante. Notons qu'ils ont également généralisé le théorème L aux cas de séries de plusieurs variables.

1.6.3 Indépendance algébrique de G -fonctions

Nous nous intéressons à présent à l'indépendance algébrique de G -fonctions.

Définition 1.6.6. Soient K un corps et $f_1(z), \dots, f_r(z)$ des séries formelles à coefficients dans K . Les séries $f_1(z), \dots, f_r(z)$ sont *algébriquement dépendantes* sur $K(z)$ s'il existe un polynôme non nul $P(z, Y_1, \dots, Y_r)$ à coefficients dans K tel que $P(z, f_1(z), \dots, f_r(z)) = 0$. Dans le cas contraire, on dit que les séries formelles $f_1(z), \dots, f_r(z)$ sont *algébriquement indépendantes* sur $K(z)$.

Pour chaque entier $r \geq 1$, considérons à nouveau la série

$$\mathfrak{g}_r(z) = \sum_{n \geq 0} \binom{2n}{n}^r z^n.$$

Puisque pour tout nombre premier p , la série $\mathfrak{g}_r(z)$ est p -Lucas, il existe un polynôme $A_p(z)$ à coefficients dans \mathbb{F}_p de degré strictement inférieur à p tel que

$$\mathfrak{g}_{r|p} = A_p(z)\mathfrak{g}_r(z^p). \tag{1.15}$$

Dans la partie 1.6.2, nous avons observé, en suivant les arguments de Sharif et Woocock [65], que les relations (1.15) permettent d'obtenir la transcendance des séries $\mathfrak{g}_r(z)$ pour tout $r \geq 2$. Adamczewski, Bell et Delaygue ont montré que ces relations, en prenant en

compte que le degré de $A_p(z)$ est au plus $p-1$, permettent en fait d'établir l'indépendance algébrique de la famille $\{\mathbf{g}_r(z)\}_{r \geq 2}$. Cette observation a conduit les auteurs de [5] à définir les ensembles $\mathcal{L}(\mathcal{S})$.

Définition 1.6.7. Soit \mathcal{S} un ensemble infini de nombres premiers. $\mathcal{L}(\mathcal{S})$ est l'ensemble des séries formelles $f(z) \in 1 + z\mathbb{Q}[[z]]$ telles que pour tout $p \in \mathcal{S}$:

- (a) $f(z) \in \mathbb{Z}_{(p)}[[z]]$;
- (b) il existe un entier l_p strictement positif et une fraction rationnelle $A_p(z)$ dans $\mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ tels que

$$f|_p(z) = A_p(z)f|_p(z^{p^{l_p}}); \quad (1.16)$$

- (c) la hauteur⁹ de $A_p(z)$ est inférieure ou égale à Cp^{l_p} , où C est une constante qui ne dépend pas de p .

Il est clair que si $f(z) \in \mathbb{Q}[[z]]$ est p -Lucas pour tout nombre premier $p \in \mathcal{S}$ alors $f(z) \in \mathcal{L}(\mathcal{S})$. Voici le résultat principal de [5] :

Théorème M (Adamczewski, Bell et Delaygue [5]). *Soit \mathcal{S} un ensemble infini de nombres premiers. Des séries formelles $f_1(z), \dots, f_r(z) \in \mathcal{L}(\mathcal{S})$ sont algébriquement dépendantes sur $\mathbb{Q}(z)$ si et seulement si il existe $m_1, \dots, m_r \in \mathbb{Z}$, non tous nuls, tels que*

$$f_1(z)^{m_1} \dots f_r(z)^{m_r} \in \mathbb{Q}(z).$$

Ce résultat est à rapprocher d'un théorème de Kolchin (et aussi du théorème J qui en est un cas particulier). Les auteurs de [5] ont montré que ce critère est très efficace pour démontrer l'indépendance algébrique de certaines familles de G -fonctions. Nous illustrons leur approche avec deux exemples.

Définition 1.6.8. L'ensemble \mathfrak{M} est l'ensemble des séries formelles f à coefficients dans \mathbb{C} dont le rayon de convergence ρ_f est fini et non nul et telles qu'il existe $z_0 \in \mathbb{C}$, avec $|z_0| = \rho_f$, vérifiant que pour tout entier $n > 0$, la série f^n n'admet pas une prolongation méromorphe au voisinage de z_0 .

Voici une conséquence remarquable du théorème M : soient \mathcal{S} un ensemble infini de nombres premiers et $f_1, \dots, f_n \in \mathcal{L}(\mathcal{S}) \cap \mathfrak{M}$. Si les nombres réels $\rho_{f_1}, \dots, \rho_{f_n}$ sont distincts, alors les séries f_1, \dots, f_n sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Pour démontrer ce résultat à partir du théorème M, nous raisonnons par l'absurde et supposons que les séries sont algébriquement dépendantes sur $\mathbb{Q}(z)$. D'après le théorème M, il existe des entiers $m_1, \dots, m_n \in \mathbb{Z}$, non tous nuls, et $r(z) \in \mathbb{Q}(z)$ tels que

$$f_1^{m_1} \dots f_n^{m_n} = r(z).$$

Sans perte de généralité, on peut supposer que $\rho_{f_1} < \rho_{f_2} < \dots < \rho_{f_n}$. Soit $j \in \{1, \dots, n\}$ le plus petit indice tel que $m_j \neq 0$. Ainsi, $f_j^{m_j} = r(z)f_{j+1}^{-m_j} \dots f_n^{-m_n}$. Puisque $f_j \in \mathfrak{M}$, $f_j^{m_j}$ n'admet pas de prolongation méromorphe au voisinage de z_0 . D'autre part, il est clair que $r(z)f_{j+1}^{-m_j} \dots f_n^{-m_n}$ est méromorphe au voisinage de z_0 , ce qui fournit une contradiction. On en déduit donc que les séries f_1, \dots, f_n sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Donnons deux applications de ce résultat. La première est que la famille $\{\mathbf{g}_r(z)\}_{r \geq 2}$ est algébriquement indépendante sur $\mathbb{Q}(z)$. En effet, pour tout entier $r \geq 2$ et tout nombre

9. Si nous écrivons $A_p(z) = P(z)/Q(z)$, où $P(z), Q(z)$ sont des polynômes premiers entre eux, la hauteur de $A_p(z)$ est le maximum des degrés de $P(z)$ et $Q(z)$.

premier p , la série $\mathbf{g}_r(z)$ est p -Lucas. Ainsi, pour tout entier $r \geq 2$, la série $\mathbf{g}_r(z)$ appartient à $\mathcal{L}(\mathcal{P})$, où \mathcal{P} est l'ensemble des nombres premiers. D'autre part, en utilisant (1.13), on peut montrer que pour tout $r \geq 2$, $\mathbf{g}_r(z) \in \mathfrak{M}$ et que $\rho_{\mathbf{g}_r} = 1/4^r$. On obtient donc que, pour tout $r \geq 2$, les séries $\mathbf{g}_2(z), \dots, \mathbf{g}_r(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Voici un deuxième exemple. Considérons les séries,

$$\mathbf{g}_2(z) = \sum_{n \geq 0} \binom{2n}{n}^2 z^n \quad \text{et} \quad \mathbf{a}_1(z) = \sum_{n \geq 0} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \right) z^n.$$

Les séries $\mathbf{g}_2(z)$ et $\mathbf{a}_1(z)$ sont p -Lucas pour tout nombre premier p et, à nouveau, on peut utiliser l'asymptotique de leurs coefficients pour montrer que ces deux séries appartiennent à \mathfrak{M} . De plus, $\rho_{\mathbf{g}_2} = 1/16$ et $\rho_{\mathbf{a}_1} = 17 - 12\sqrt{2}$. Il suit donc que les séries $\mathbf{g}_2(z)$ et $\mathbf{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Ces résultats d'indépendance algébrique conduisent naturellement à se poser la question suivante :

Question 4. Soient $f(z) \in \mathbb{Q}[[z]]$ holonome et \mathcal{S} un ensemble infini de nombres premiers. A quelles conditions la série $f(z)$ appartient-elle à $\mathcal{L}(\mathcal{S})$?

Rappelons que les résultats obtenus dans [5], et énoncés dans cette thèse comme les théorèmes G et H, fournissent de nombreux exemples de G -fonctions qui sont dans des ensembles de type $\mathcal{L}(\mathcal{S})$. L'approche utilisée dans [5] repose sur un étude détaillé de la valuation p -adique des coefficients des séries hypergéométriques généralisées et de séries obtenues par spécialisation à partir de séries de plusieurs variables dont les coefficients sont des quotients de factorielles. Dans cette thèse, nous allons suivre une autre approche pour aborder la question 4. Celle-ci met en avant les équations différentielles. Notre étude fournira une nouvelle méthode qui s'avère efficace pour montrer que certaines série holonomes sont dans des ensembles de type $\mathcal{L}(\mathcal{S})$.

1.7 Résultats principaux, deuxième partie

Le but de cette partie est d'étudier la question 4. En outre, nous obtenons l'indépendance algébrique de certaines G -fonctions pour lesquelles le théorème M ne s'applique pas.

1.7.1 Structure de Frobenius forte et congruences « à la Lucas »

Une première observation est la suivante : parmi les exemples connus de séries appartenant à des ensembles de type $\mathcal{L}(\mathcal{S})$, un grand nombre sont des séries holonomes (plus précisément des G -fonctions) qui sont solutions d'opérateurs différentiels à coefficients dans $\mathbb{Q}(z)$ possédant une structure de Frobenius forte pour presque tout nombre premier p . Par exemple, pour tout entier $r \geq 1$, la série $\mathbf{g}_r(z) = \sum_{n \geq 0} \binom{2n}{n}^r z^n$ appartient à $\mathcal{L}(\mathcal{P})$, où \mathcal{P} est l'ensemble de nombres premiers et la série $\mathbf{g}_r(z)$ annule l'opérateur différentiel

$$\mathcal{L}_r := \delta^r - 4^r(\delta + 1/2)^r.$$

Il découle du théorème 1.4.11 que, pour tout $r \geq 1$, l'opérateur différentiel \mathcal{L}_r possède une structure de Frobenius forte pour tout nombre premier différent de 2.

Un autre exemple de cette situation est donné par la série $\mathbf{a}_1(z)$. En effet, comme nous avons dans la partie 1.6.1, la série $\mathbf{a}_1(z)$ est p -Lucas pour tout nombre premier p . De plus, $\mathbf{a}_1(z)$ est la diagonale d'une fraction rationnelle. D'après [25], cela implique que $\mathbf{a}_1(z)$ annule un opérateur différentiel à coefficients dans $\mathbb{Q}(z)$ muni d'une structure de Frobenius forte pour presque tout p .

Cela n'est pas vraiment surprenant, car conjecturalement toutes les G -fonctions devraient annuler des opérateurs différentiels dans $\overline{\mathbb{Q}}(z)$ qui viennent de la géométrie et de tels opérateurs sont munis de structure de Frobenius forte pour presque tout nombre premier p . Ainsi, si $f(z)$ est une telle G -fonction et que $f(z) \in \mathbb{Z}_{(p)}[[z]]$, on obtient que $f(z)$ est algébrique modulo p . L'existence de structure de Frobenius est donc un premier pas vers l'appartenance à un ensemble de type $\mathcal{L}(\mathcal{S})$. Cette remarque motive la définition suivante :

Définition 1.7.1. Etant donné un ensemble infini \mathcal{S} de nombres premiers, $\mathcal{F}(\mathcal{S})$ est l'ensemble des séries $f(z) \in 1 + z\mathbb{Q}[[z]]$ telles que :

- pour tout $p \in \mathcal{S}$, $f(z) \in \mathbb{Z}_{(p)}[[z]]$;
- $f(z)$ annule un opérateur différentiel $\mathcal{H} \in \mathbb{Q}(z)[d/dz]$ muni d'une structure de Frobenius forte pour tout $p \in \mathcal{S}$.

Il découle donc du théorème 1.4.6 que si $f(z) \in \mathcal{F}(\mathcal{S})$ alors, pour tout $p \in \mathcal{S}$, la série $f_{|p}(z)$ est algébrique sur $\mathbb{F}_p(z)$. Pour que $f(z)$ appartienne à $\mathcal{L}(\mathcal{S})$, il reste à obtenir que, pour tout nombre premier $p \in \mathcal{S}$, $f(z)$ vérifie une relation algébrique de la forme

$$f_{|p}(z) = A_p(z)f_{|p}(z)^{l_p}$$

où la hauteur de A_p est en $O(p^{l_p})$. Notons que cette relation est équivalente à l'égalité (1.16) car $f_{|p}(z^{l_p}) = f_{|p}(z)^{l_p}$. Nous cherchons donc une condition supplémentaire à ajouter aux éléments de $\mathcal{F}(\mathcal{S})$ afin de garantir leur appartenance à $\mathcal{L}(\mathcal{S})$. Dans cette direction, le théorème 1.7.6 établit que si $f(z) \in \mathcal{F}(\mathcal{S})$ annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MUM en zéro, alors la série $f(z)$ vérifie une équation du type (1.16) pour presque tout $p \in \mathcal{S}$. Avant d'énoncer ce théorème, nous rappelons la définition d'opérateur MUM en zéro et introduisons les ensemble $\mathcal{L}^2(\mathcal{S})$, ainsi que les opérateurs Λ_p .

Définition 1.7.2. Soit \mathcal{D} un opérateur différentiel à coefficients dans $\mathbb{Q}(z)$. Nous disons que \mathcal{D} est MUM en zéro si \mathcal{D} est fuchsien, zéro est un point singulier régulier de \mathcal{D} et la matrice de monodromie locale de \mathcal{D} en zéro est unipotente.

Remarque 1.7.3. Soient \mathcal{D} un opérateur différentiel à coefficients dans $\mathbb{Q}(z)$, $f(z) \in \mathbb{Q}[[z]]$ solution de \mathcal{D} et p un nombre premier tel que $f(z) \in \mathbb{Z}_{(p)}[[z]]$ et \mathcal{D}_p est bien défini. Rappelons que \mathcal{D}_p est la réduction de \mathcal{D} modulo p . Il est connu que si \mathcal{D} est MUM en zéro alors le \mathbb{Q} -espace vectoriel formé des solutions de \mathcal{D} qui sont dans $\mathbb{Q}[[z]]$ est de dimension 1. Une observation importante, démontrée dans le chapitre 3, est que l'hypothèse de MUM en zéro implique aussi que le $\mathbb{F}_p((z^p))$ -espace vectoriel formé des solutions de \mathcal{D}_p qui sont dans $\mathbb{F}_p((z))$ est de dimension 1. Cette observation est cruciale pour démontrer le théorème 1.7.6.

De plus, la notion d'opérateur MUM en zéro a une caractérisation algébrique qui est la suivante : \mathcal{D} est MUM en zéro si et seulement si \mathcal{D} est fuchsien, zéro est un point singulier régulier de \mathcal{D} et les exposants en zéro de \mathcal{D} sont tous égaux à zéro. En effet, d'après la proposition 3.12 de [72] et le théorème 5.1 de [72], tous les exposants en zéro de \mathcal{D} sont égaux à zéro si et seulement si toutes les valeurs propres de la matrice de monodromie locale de \mathcal{D} en zéro sont égales à 1, c'est-à-dire que la matrice de monodromie locale de \mathcal{D} en zéro est unipotente.

Définition 1.7.4. Soit \mathcal{S} un ensemble infini de nombres premiers. On définit $\mathcal{L}^2(\mathcal{S})$ comme l'ensemble des séries $f(z) \in 1 + z\mathbb{Q}[[z]]$ telles que pour tout $p \in \mathcal{S}$:

(a') $f(z) \in \mathbb{Z}_{(p)}[[z]]$;

(b') il existe un entier l_p strictement positif et une fraction rationnelle $A_p(z)$ dans $\mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ tels que

$$f|_p(z) = A_p(z)f|_p(z^{p^{l_p}}) ;$$

(c') la hauteur de $A_p(z)$ est inférieure ou égale à Cp^{2l_p} , où C est une constante qui ne dépend pas de p

Remarquons que les conditions (a') et (b') de la définition 1.7.4 sont les mêmes conditions (a) et (b) de la définition 1.6.7. Par contre, à la différence de la condition (c) de la définition 1.6.7, où il est demandé que la hauteur de A_p soit dans $O(p^{l_p})$, nous demandons dans la condition (c') que la hauteur de A_p soit dans $O(p^{2l_p})$. Il est donc clair que $\mathcal{L}(\mathcal{S}) \subset \mathcal{L}^2(\mathcal{S})$.

Définition 1.7.5. Soient p un nombre premier, K un corps quelconque. Nous notons Λ_p l'opérateur de $K[[z]]$ dans lui-même défini par : $\Lambda_p(\sum_{n \geq 0} a(n)z^n) = \sum_{n \geq 0} a(np)z^n$.

Par abus de langage, les opérateurs Λ_p seront appelés opérateurs de Cartier dans la suite¹⁰. Notre résultat principal concernant la question 4 est le suivant :

Théorème 1.7.6. Soient \mathcal{S} un ensemble infini de nombres premiers et $f(z)$ une série qui appartient à $\mathcal{F}(\mathcal{S})$ et qui annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MUM en zéro. Alors, on a :

1. $f(z) \in \mathcal{L}^2(\mathcal{S}')$, où $\mathcal{S}' \subset \mathcal{S}$ et $\mathcal{S} \setminus \mathcal{S}'$ est fini.
2. Si de plus, pour tout $p \in \mathcal{S}$, il existe un entier l strictement positif tel que $\Lambda_p^l(f(z))|_p = f|_p(z)$ alors $f(z) \in \mathcal{L}(\mathcal{S}')$, où $\mathcal{S}' \subset \mathcal{S}$ et $\mathcal{S} \setminus \mathcal{S}'$ est fini.

Malgré son apparente complexité, ce théorème fournit un moyen très efficace pour montrer que des séries holonomes appartiennent à des ensembles de type $\mathcal{L}(\mathcal{S})$. On peut par exemple l'utiliser pour montrer que les séries formelles $\mathfrak{g}_r(z)$, $r \geq 1$, et $\mathfrak{a}_1(z)$ sont dans $\mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{P} est l'ensemble des nombres premiers et \mathcal{J} est un ensemble fini de nombres premiers. De façon plus remarquable, ce résultat permet d'étudier les solutions d'opérateurs de type Calabi-Yau. Dans [9], les auteurs dressent une liste de plus de 400 opérateurs de type Calabi-Yau. Ces opérateurs vérifient certaines conditions algébriques dont : zéro est un point singulier régulier et les exposants en zéro sont tous égaux à zéro et chaque opérateur admet une solution dans $\mathbb{Z}[[z]]$ dont le terme constant est égal à 1. Notamment, tous ces opérateurs sont MUM en zéro. Comme nous le verrons dans la partie 3.7, le théorème 1.7.6 permet de montrer que 242 de ces séries appartiennent à $\mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{J} est un ensemble fini de nombres premiers.

Dans la partie 3.6 nous montrerons que, pour $f(z) \in \mathcal{F}(\mathcal{S})$, le fait d'annuler un opérateur différentiel MUM en zéro n'est pas une condition suffisante pour appartenir à $\mathcal{L}(\mathcal{S})$. Plus précisément, nous montrerons que la série hypergéométrique

$$\mathfrak{h}_2(z) = \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n}^2 z^n$$

10. Voir la discussion dans [7, Section 2] concernant cet abus de langage.

n'appartient pas à aucun ensemble de type $\mathcal{L}(\mathcal{S})$, alors que $\mathfrak{h}_2(z)$ annule un opérateur différentiel MUM en zéro. On a toutefois que $\mathfrak{h}_2(z) \in \mathcal{L}^2(\mathcal{P} \setminus \{2\})$ comme le garantit le théorème 1.7.6. Cela montre que le point 1 du théorème 1.7.6 est optimal.

Soit $f(z) = \sum_{n \geq 0} a(n)z^n \in 1 + z\mathbb{Q}[[z]]$. Dans le point 2 du théorème 1.7.6, la condition $\Lambda_p^l(f(z)|_p) = f|_p(z)$ revient à dire que pour tout entier $n \geq 0$,

$$a(np^l) \equiv a(n) \pmod{p}.$$

Remarquons que si $f(z)$ est p -Lucas alors, pour tout entier $n \geq 0$, $a(np) \equiv a(n) \pmod{p}$. Notons que dans beaucoup d'exemples il est plus facile de vérifier que $a(np) \equiv a(n) \pmod{p}$ pour tout entier $n \geq 0$, que de vérifier que la série $f(z)$ est p -Lucas.

Voici un exemple qui illustre cette situation. Considérons la série

$$f_4(z) = \sum_{j \geq 0} \left(\binom{2j}{j} \left(\sum_{k=0}^{2j} (-1)^k \binom{2j}{k}^4 \right) \right) z^j \in 1 + z\mathbb{Z}[[z]].$$

Nous allons voir qu'en utilisant le théorème de Lucas, on obtient sans difficulté que $\Lambda_p(f_4(z)|_p) = f_4|_p(z)$, pour tout $p \in \mathcal{P} \setminus \{2\}$. Nous devons donc montrer que pour tout $p \in \mathcal{P} \setminus \{2\}$ et tout entier j on a

$$\binom{2jp}{jp} \left(\sum_{k=0}^{2jp} (-1)^k \binom{2jp}{k}^4 \right) \equiv \binom{2j}{j} \left(\sum_{k=0}^{2j} (-1)^k \binom{2j}{k}^4 \right) \pmod{p}.$$

Soit $k \in \{0, \dots, 2jp\}$. Alors $k = lp + s$, où $0 \leq s \leq p-1$ et $0 \leq l \leq 2j$. D'après le théorème de Lucas, on a que

$$\binom{2jp}{k}^4 = \binom{2jp}{lp+s}^4 \equiv \binom{2j}{l}^4 \binom{0}{s}^4 \pmod{p}.$$

Ainsi, si $s > 0$ alors $\binom{2jp}{k}^4 \equiv 0 \pmod{p}$ et si $s = 0$ alors $k = lp$ et $\binom{2jp}{lp}^4 \equiv \binom{2j}{l}^4 \pmod{p}$. Par conséquent,

$$\sum_{k=0}^{2jp} (-1)^k \binom{2jp}{k}^4 \equiv \sum_{l=0}^{2j} (-1)^{lp} \binom{2j}{l}^4 = \sum_{l=0}^{2j} (-1)^l \binom{2j}{l}^4 \pmod{p},$$

car $p \neq 2$. Finalement, d'après le théorème de Lucas, $\binom{2jp}{jp} \equiv \binom{2j}{j} \pmod{p}$ et il vient

$$\binom{2jp}{jp} \left(\sum_{k=0}^{2jp} (-1)^k \binom{2jp}{k}^4 \right) \equiv \binom{2j}{j} \left(\sum_{k=0}^{2j} (-1)^k \binom{2j}{k}^4 \right) \pmod{p},$$

pour tout nombre premier $p \neq 2$ et tout entier j . Ainsi, pour tout nombre premier $p \neq 2$, $\Lambda_p(f_4(z)|_p) = f_4|_p(z)$. Par contre, cette approche directe ne permet pas de montrer que la série $f_4(z)$ appartient à $\mathcal{L}(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers. Pour montrer cela nous devons appliquer le théorème 1.7.6. En effet, d'après le théorème 3.5 de [17], la série $f_4(z)$ est une diagonale de fraction rationnelle et, d'après [25], $f_4(z)$ annule donc un opérateur différentiel $\mathcal{H} \in \mathbb{Q}(z)[d/dz]$ muni d'une structure de Frobenius forte pour presque tout nombre premier p . D'autre part, $f_4(z)$ annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ qui est MUM en zéro car elle est la série 210 de la liste donnée dans [9]. Le point 2 du théorème 1.7.6 entraîne finalement que $f_4(z) \in \mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{J} est un ensemble fini de nombres premiers.

1.7.2 Application à indépendance algébrique de G -fonctions

Comme nous l'avons déjà mentionné la série $\mathfrak{h}_2(z)$ n'appartient à aucun ensemble de type $\mathcal{L}(\mathcal{S})$. Par contre, cette série annule un opérateur MUM en zéro ainsi qu'un opérateur différentiel muni d'une structure de Frobenius forte pour presque tout nombre premier p . D'après le premier point du théorème 1.7.6, cette série appartient donc à $\mathcal{L}^2(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers. Il est donc naturel d'essayer d'étendre le critère d'indépendance algébrique d'Adamczewski, Bell et Delaygue aux éléments de $\mathcal{L}^2(\mathcal{S})$. Bien que nous ne donnions pas une réponse générale à ce problème, nous établissons un premier résultat dans cette direction.

Théorème 1.7.7. *Soient $f_1(z), \dots, f_r(z)$ des éléments de $\mathcal{F}(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers, annulant chacun un opérateur différentiel MUM en zéro à coefficients dans $\mathbb{Q}(z)$. Supposons qu'il existe $g_1(z), \dots, g_r(z) \in 1 + z\mathbb{Q}[[z]]$ telles que, pour tout $p \in \mathcal{S}$ et tout $i \in \{1, \dots, r\}$, $g_i(z) \in \mathbb{Z}_{(p)}[[z]]$ et il existe un entier $l_{i,p} \geq 1$ tel que $\Lambda_p^{l_{i,p}}(f_i(z))|_p = g_{i|p}(z) = \Lambda_p^{2l_{i,p}}(f_i(z))|_p$. Si $g_1(z), \dots, g_r(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$, alors $f_1(z), \dots, f_r(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$.*

Nous faisons la remarque suivante : sous les hypothèses du théorème, nous montrons dans le lemme 3.8.1 qu'il existe un ensemble $\mathcal{S}' \subset \mathcal{S}$ infini tel que les séries g_1, \dots, g_r appartiennent à $\mathcal{L}(\mathcal{S}')$. L'importance de cette observation vient du fait de que nous avons déjà décrit une méthode pour démontrer l'indépendance algébrique des séries qui appartiennent à $\mathcal{L}(\mathcal{S}')$. Le théorème 1.7.7 dit que pour obtenir l'indépendance algébrique des séries f_1, \dots, f_r il suffit de démontrer celles de séries qui sont dans $\mathcal{L}(\mathcal{S}')$, ce que nous pouvons généralement faire grâce au théorème M.

Nous illustrons la pertinence de ce théorème grâce aux deux exemples suivants qui en découlent.

Théorème 1.7.8. *Soit r un entier strictement positif et*

$$\mathfrak{h}_r(z) = \sum_{n \geq 0} \frac{-1}{(2n-1)} \binom{2n}{n}^r z^n.$$

Les séries hypergéométriques $\{\mathfrak{h}_r(z)\}_{r \geq 2}$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Théorème 1.7.9. *Les séries*

$$\mathfrak{h}_2(z) = \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n}^2 z^n \quad \text{et} \quad \mathfrak{a}_1(z) = \sum_{n \geq 0} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \right) z^n$$

sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Il est important de souligner que ces deux résultats ne peuvent être obtenus à l'aide du théorème M puisque, comme nous l'avons déjà signalé, la série $\mathfrak{h}_2(z)$ n'appartient à aucun ensemble de type $\mathcal{L}(\mathcal{S})$. En revanche, ils découlent tous les deux du théorème 1.7.7. En effet, d'après le théorème de Lucas, pour tout nombre premier p et tout $r \geq 1$, $\Lambda_p(\mathfrak{h}_r(z))|_p = \mathfrak{g}_{r|p}(z) = \Lambda_p^2(\mathfrak{h}_r(z))|_p$. Et comme nous avons déjà vu, la famille $\{\mathfrak{g}_r(z)\}_{r \geq 1}$ est algébriquement indépendante sur $\mathbb{Q}(z)$. D'après le théorème 1.7.7, on obtient que la famille $\{\mathfrak{h}_r(z)\}_{r \geq 1}$ est algébriquement indépendante sur $\mathbb{Q}(z)$. Finalement, d'après le théorème de Lucas, on a pour tout nombre premier p que $\Lambda_p(\mathfrak{a}_1(z))|_p = \mathfrak{a}_{1|p}(z) = \Lambda_p^2(\mathfrak{a}_1(z))|_p$. De plus, nous avons déjà observé que les séries $\mathfrak{g}_1(z)$ et $\mathfrak{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. A nouveau, on peut appliquer le théorème 1.7.7 et en déduire que les séries $\mathfrak{h}_2(z)$ et $\mathfrak{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Chapitre 2

Algébricité modulo p , structure de Frobenius forte et rigidité

Dans ce chapitre nous allons démontrer les théorèmes 1.4.6, 1.4.10, 1.4.12 et 1.4.11. Il est organisé de la façon suivante. Le théorème 1.4.6 est démontré dans la partie 2.1 Dans la partie 2.2, nous rappelons la notion d'opérateur différentiel rigide et dans la partie 2.3 nous démontrons le théorème 1.4.10. Enfin, dans la section 2.4, nous prouvons les théorèmes 1.4.12 et 1.4.11.

2.1 Démonstration du théorème 1.4.6

Cette partie est consacrée à l'algebricité modulo p des solutions des équations p -différentielles possédant une structure de Frobenius forte pour le nombre premier p . Nous démontrons le théorème 1.4.6.

Rappelons tout d'abord que l'ensemble \mathcal{W}_p est composé des séries de la forme

$$f(z) = \sum_{n \in \mathbb{Z}} a_n z^n,$$

dont les coefficients appartiennent à \mathbb{C}_p et telles que la famille $\{|a_n|\}_{n \in \mathbb{Z}}$ est bornée et tend vers 0 lorsque n tend négativement vers l'infini. L'anneau \mathcal{W}_p est complet pour la norme

$$|f| = \sup_{n \in \mathbb{Z}} |a_n|.$$

Par construction, E_p est un sous-corps de \mathcal{W}_p et on note ϑ_{E_p} les éléments de E_p dont la norme est inférieure ou égale à 1.

Nous commençons par montrer les deux lemmes suivants.

Lemme 2.1.1. *Soit \mathfrak{m} l'idéal maximal de ϑ_{E_p} . Il existe un isomorphisme de corps*

$$\phi : \vartheta_{E_p}/\mathfrak{m} \rightarrow \overline{\mathbb{F}_p}(z).$$

Démonstration. Soient $\vartheta_{\mathbb{C}_p}$ l'anneau des entiers de \mathbb{C}_p et \mathfrak{M} son idéal maximal. Soit $x \in \vartheta_{\mathbb{C}_p}$, comme x est la limite d'éléments dans la clôture algébrique de \mathbb{Q}_p , il existe une extension finie K de \mathbb{Q}_p et $y \in K$ tels que $|x - y| < 1$. Ainsi, $|y| \leq 1$ et dans $\vartheta_{\mathbb{C}_p}/\mathfrak{M}$, $\bar{x} = \bar{y}$. Comme le corps résiduel de K est une extension finie de \mathbb{F}_p , on a $\bar{y} \in \overline{\mathbb{F}_p}$. On définit

$$\omega : \vartheta_{\mathbb{C}_p} \rightarrow \overline{\mathbb{F}_p}$$

par $\omega(x) = \bar{y}$. Notons que $\omega(x)$ ne dépend pas de y et est un homomorphisme d'anneaux. D'après le lemme de Hensel, ω est surjectif et si $x \in \mathfrak{M}$, alors $\omega(x) = 0$. Ainsi,

$$\omega : \vartheta_{\mathbb{C}_p}/\mathfrak{M} \rightarrow \overline{\mathbb{F}_p}$$

est un isomorphisme tel que $\omega(\bar{x}) = \bar{x}$ pour tout $x \in \mathbb{Z}_p$. Soit $\vartheta_{\mathcal{W}_p}$ l'ensemble des éléments de \mathcal{W}_p dont la norme est inférieure ou égale à 1. Comme la norme est ultramétrique, $\vartheta_{\mathcal{W}_p}$ est un anneau et, si J désigne l'ensemble des éléments de \mathcal{W}_p dont la norme est strictement inférieure à 1, alors J est un idéal de $\vartheta_{\mathcal{W}_p}$ et le quotient de $\vartheta_{\mathcal{W}_p}$ par J est isomorphe à $\overline{\mathbb{F}_p}((z))$. En effet, soit $f(z) = \sum_{n \in \mathbb{Z}} a_n z^n \in \vartheta_{\mathcal{W}_p}$. Alors, pour tout entier n , $|a_n| \leq 1$ et par définition de l'anneau \mathcal{W}_p il existe un nombre naturel N tel que, pour tout $n < -N$, $|a_n| < 1$. Ainsi, on a

$$\overline{f(z)} := \sum_{n \geq -N} \overline{a_n} z^n \in (\vartheta_{\mathbb{C}_p}/\mathfrak{M})((z)).$$

Considérons l'application $\tilde{\omega} : \vartheta_{\mathcal{W}_p}/J \rightarrow \overline{\mathbb{F}_p}((z))$ définie par $\tilde{\omega}(\bar{f}) = \sum_{n \geq -N} \omega(\overline{a_n}) z^n$. Si $f \in \mathbb{Z}_p[[z]]$, alors $\tilde{\omega}(\bar{f}) = \bar{f}$. Comme ω est un isomorphisme il en est de même pour $\tilde{\omega}$. Construisons à présent l'isomorphisme ϕ . Comme ϑ_{E_p} est un anneau local et un sous-anneau de $\vartheta_{\mathcal{W}_p}$, si \mathfrak{m} désigne l'idéal maximal de ϑ_{E_p} , alors $\mathfrak{m} \subset J$. Ainsi, $\tilde{\omega}$ peut se restreindre à $\vartheta_{E_p}/\mathfrak{m}$.

Par construction, si $h \in \vartheta_{E_p}$, $\bar{h} \in (\vartheta_{\mathbb{C}_p}/\mathfrak{M})(z)$, d'où $\bar{h}s = t$, où $s, t \in (\vartheta_{\mathbb{C}_p}/\mathfrak{M})[z]$ sont différents du polynôme nul. Nous pouvons donc définir, $\phi(\bar{h}) = \tilde{\omega}(t)/\tilde{\omega}(s) \in \overline{\mathbb{F}_p}(z)$. \square

Le lemme suivant est démontré dans [2, Proposition 6.2] dans le cas où $L = \mathbb{C}$. En utilisant le même argument, on obtient le lemme suivant.

Lemme 2.1.2. *Soit K un corps, L une extension de K et $f_1, \dots, f_n \in K[[z]]$. S'il existe des polynômes $a_1(z), \dots, a_n(z) \in L[z]$, non tous nuls, tels que*

$$a_1(z)f_1 + \dots + a_n(z)f_n = 0,$$

alors il existe des polynômes $c_1(z), \dots, c_n(z) \in K[z]$, non tous nuls, tels que

$$c_1(z)f_1 + \dots + c_n(z)f_n = 0.$$

Nous pouvons maintenant démontrer le théorème 1.4.6.

Démonstration du théorème 1.4.6. Fixons un nombre premier p . Supposons que A est la matrice compagnon de l'opérateur différentiel

$$L := \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \dots + a_{n-1}(z) \frac{d}{dz} + a_n(z), \quad (2.1)$$

où les $a_i(z)$ sont des fractions rationnelles à coefficients dans \mathbb{Q} . Comme A a une structure de Frobenius forte de période h , il existe $H \in \mathrm{GL}_n(E_p)$ telle que

$$\frac{d}{dz} H = AH - H(p^h z^{p^h - 1} A(z^{p^h})).$$

Soit $g \in \mathcal{W}_p$ tel que $Lg = 0$, alors le vecteur $\vec{y} = (g, g', \dots, g^{(n-1)})^T$ est solution du système

$$\frac{d}{dz} Y = AY. \quad (2.2)$$

Ainsi, le vecteur $\vec{y}(z^{p^h})$ est solution du système

$$\frac{d}{dz}Y = p^h z^{p^h-1} A(z^{p^h})Y.$$

Par conséquent, le vecteur $H\vec{y}(z^{p^h})$ est solution du système (2.2). Comme $E_p \subset \mathcal{W}_p$, on trouve que $H\vec{y}(z^{p^h})$ est un vecteur à coefficients dans \mathcal{W}_p , dont le premier coefficient est une solution de l'équation associée à l'opérateur (2.1). Soit $V := \{(g, g', \dots, g^{n-1}) : g \in \mathcal{W}_p, Lg = 0\}$. Il s'agit d'un \mathbb{C}_p -espace vectoriel. Nous avons donc construit un endomorphisme

$$\begin{aligned} \psi : V &\rightarrow V \\ \vec{y} &\mapsto H\vec{y}(z^{p^h}). \end{aligned}$$

Comme $\dim_{\mathbb{C}_p} V = r \leq n$, le théorème de Cayley-Hamilton assure l'existence de c_0, \dots, c_{r-1} appartenant à \mathbb{C}_p tels que

$$\psi^r + c_{r-1}\psi^{r-1} + \dots + c_1\psi + c_0 = 0. \quad (2.3)$$

Comme par hypothèse $f(z) \in \mathbb{Z}_{(p)}[[z]]$ et L est annulée par $f(z)$, alors le vecteur $\vec{w} = (f, f', \dots, f^{(n-1)})$ est dans V . Considérons à présent V_f , le E_p -espace vectoriel engendré par les éléments de l'ensemble $\{f^{(j)}(z^{p^{jh}}) : j \in \{0, \dots, n-1\}, i \in \mathbb{N}\}$. L'égalité (2.3) montre que V_f a pour dimension au plus nr . Comme $f(z), \dots, f(z^{p^{nrh}}) \in V_f$, il existe $j \leq nr$ et $b_0, \dots, b_j \in E_p$ tels que

$$b_j f(z^{p^{jh}}) + b_{j-1} f(z^{p^{(j-1)h}}) + \dots + b_0 f(z) = 0.$$

Soit b_l tel que $|b_l| = \max\{|b_0(z)|, \dots, |b_j(z)|\}$ et soit $c_i(z) = b_i(z)/b_l(z)$. Alors, pour tout $i \in \{0, \dots, j\}$, $|c_i| \leq 1$ et

$$c_j f(z^{p^{jh}}) + c_{j-1} f(z^{p^{(j-1)h}}) + \dots + c_0 f(z) = 0.$$

On pose $d_i(z) = \overline{c_i(z)}$, alors on a

$$d_j(z)(f|_p(z^{p^{jh}})) + d_{j-1}(z)(f|_p(z)^{p^{(j-1)h}}) + \dots + d_0(z)f|_p(z) = 0. \quad (2.4)$$

et $d_0(z), \dots, d_j(z)$ ne sont toutes nulles car $1 = \max\{|c_0(z)|, \dots, |c_j(z)|\}$.

Soient $\tilde{\omega}$ l'homomorphisme construit dans le lemme 2.1.1 et $t_i(z) = \tilde{\omega}(d_i(z))$. Puisque $\tilde{\omega}$ est un isomorphisme alors $t_0(z), \dots, t_j(z)$ ne sont pas toutes nulles. Comme $\tilde{\omega}(f|_p) = f|_p$ car $f \in \mathbb{Z}_{(p)}[[z]]$, alors (2.4) implique que

$$t_j(z)(f|_p(z^{p^{jh}})) + t_{j-1}(z)(f|_p(z)^{p^{(j-1)h}}) + \dots + t_0(z)f|_p(z) = 0.$$

Finalement, le lemme 2.1.2 assure l'existence des polynômes $r_0(z), \dots, r_j(z) \in \mathbb{F}_p(z)$, non tous nuls, tels que

$$r_j(z)(f|_p(z)^{p^{jh}}) + r_{j-1}(z)(f|_p(z)^{p^{(j-1)h}}) + \dots + r_0(z)f|_p(z) = 0.$$

Comme les coefficients de $f|_p(z)$ sont dans \mathbb{F}_p , la dernière expression devient

$$r_j(z)(f|_p(z))^{p^{jh}} + r_{j-1}(z)(f|_p(z))^{p^{(j-1)h}} + \dots + r_0(z)f|_p(z) = 0.$$

Et puisque $j \leq nr \leq n^2$, nous obtenons que le degré de $f|_p$ sur $\mathbb{F}_p(z)$ est majoré par p^{n^2h} , comme souhaité. \square

Remarque 2.1.3. La démonstration montre plus précisément que le degré d'algébricité de $f|_p(z)$ est borné par p^{nrh} , où r désigne la dimension du \mathbb{C}_p -espace vectoriel V .

2.2 Structure de Frobenius forte et rigidité

Le théorème 1.4.10 concerne les opérateurs différentiels à coefficients dans $\mathbb{Q}[z]$ dont le groupe de monodromie est rigide. Dans la partie 1.4.5 nous avons rappelé la notion de point singulier, de point singulier régulier, d'exposant et de groupe de monodromie pour un opérateur différentiel. Dans cette partie nous commençons par rappeler ces mêmes notions mais dans le cas d'un système différentiel. Étant donné le système différentiel

$$\frac{d}{dz}y = Ay, \quad A \in \mathcal{M}_n(\mathbb{C}(z)), \quad (2.5)$$

nous disons que $\gamma \in \mathbb{C}$ est un point *singulier* du système différentiel (2.5) si γ est un pôle de A . L'infini est un point singulier de (2.5) si zéro est un point singulier du système différentiel obtenu après avoir appliqué le changement de variable $z \mapsto 1/z$ au système (2.5). Nous disons que $\gamma \in \mathbb{C}$ est un point *singulier régulier* du système différentiel (2.5) si γ est un point singulier et s'il existe une matrice $A_\gamma \in \mathcal{M}_n(\mathbb{C}(z))$ telle que la matrice $(z - \gamma)A_\gamma$ n'a pas de pôle en γ et qu'il existe une matrice $P \in \text{GL}_n(\mathbb{C}(\{z - \gamma\}))$ telle que $\frac{d}{dz}P = AP - PA_\gamma$, où $\mathbb{C}(\{z - \gamma\})$ est le corps des séries de Laurent convergentes au voisinage de γ . L'infini est un point singulier régulier de (2.5) si zéro est un point singulier régulier du système différentiel obtenu après avoir appliqué le changement de variable $z \mapsto 1/z$ au système (2.5). Le système différentiel (2.5) est *fuchsien* si tous ses points singuliers sont singuliers réguliers. Soit x un point non singulier du système différentiel (2.5), d'après la théorie classique de Cauchy

$$\text{Sol}(A)_x = \{y \in \mathbb{C}(\{z - x\})^n \text{ et } \frac{d}{dz}y = Ay\}$$

est un \mathbb{C} -espace vectoriel de dimension n . Soient $F = \{y_1, \dots, y_n\}$ une base de $\text{Sol}(A)_x$, S l'ensemble de points singuliers de (2.5) et $\gamma \in S$. Les coordonnées des vecteurs y_1, \dots, y_n peuvent être prolongées analytiquement le long du lacet τ , où $[\tau] \in \Pi_1(\mathbb{C} \setminus S, x)$ et τ est un lacet autour de γ tel que le groupe engendré par $[\tau]$ est \mathbb{Z} . Ainsi, on obtient un nouvel ensemble \tilde{F} qui sera encore une base de $\text{Sol}(A)_x$. Alors la matrice de *monodromie locale en γ* , notée $M(A, \gamma) \in \text{GL}_n(\mathbb{C})$, est la matrice de changement de base de F vers \tilde{F} . Le théorème de monodromie complexe nous garanti que si $[\tau] = [\alpha]$, on obtient encore l'ensemble \tilde{F} en prolongeant les coordonnées des vecteurs y_1, \dots, y_n le long du lacet α . Écrivons $S = \{\gamma_1, \dots, \gamma_r\} \subset \mathbb{C} \cup \{\infty\}$. Le *groupe de monodromie* de (2.5) est le groupe engendré par les matrices $M(A, \gamma_1), \dots, M(A, \gamma_r)$ qui satisfont à la relation $M(A, \gamma_1) \cdots M(A, \gamma_r) = \text{Id}$. D'après la construction, le groupe de monodromie dépend de la base F . Si nous prenons une autre base F_1 de $\text{Sol}(A)_x$ alors ces deux groupes de monodromie sont conjugués. Ainsi le groupe de monodromie est unique à conjugaison près.

Soit

$$\frac{d}{dz}y = A'y, \quad A' \in \mathcal{M}_n(\mathbb{C}(z)) \quad (2.6)$$

un système différentiel. Supposons que les systèmes (2.5) et (2.6) sont fuchsien et que zéro est un point singulier régulier de (2.5) et de (2.6). On dit que A et A' sont *localement équivalentes en zéro* si les matrices de monodromie locale en zéro de (2.5) et (2.6) sont conjuguées. D'après le théorème 5.1 de [72], cela revient à dire qu'il existe P une matrice inversible à coefficients dans $\mathbb{C}(\{z\})$ telle que

$$\frac{d}{dz}P = AP - PA',$$

où $\mathbb{C}(\{z\})$ est le corps des séries de Laurent qui convergent. Soit x_0 un point singulier régulier de (2.5) et de (2.6) On dit que A et A' sont *localement équivalentes en x_0* si, après application du changement de variable $z \mapsto z - x_0$ à (2.5) et (2.6), les nouveaux systèmes sont localement équivalents en zéro. On dit que A et A' sont *localement équivalentes*, si elles sont localement équivalentes en tous points.

Définition 2.2.1 (Système rigide). Soient $A \in \mathcal{M}_n(\mathbb{C}(z))$ et $\frac{d}{dz}y = Ay$ un système différentiel fuchsien. Un tel système est dit *rigide* si, pour tout système $\frac{d}{dz}y = A'y$ fuchsien tel que A et A' sont localement équivalentes, il existe $P \in \text{GL}_n(\mathbb{C}(z))$ telle que

$$\frac{d}{dz}P = AP - PA'.$$

Autrement dit, les matrices A et A' sont $\mathbb{C}(z)$ -équivalentes.

En général pour un corps quelconque K , nous disons que deux matrices $A, A' \in \mathcal{M}_n(K(z))$ sont $K(z)$ -équivalentes s'il existe $P \in \text{GL}_n(K(z))$ telle que $\frac{d}{dz}P = AP - PA'$.

Définition 2.2.2 (Groupe rigide). Soient $g_1, \dots, g_r \in \text{GL}_n(\mathbb{C})$ et G le groupe engendré par ces matrices. Le r-uplet g_1, \dots, g_r est dit irréductible si G agit de manière irréductible sur \mathbb{C}^n . Le groupe G est dit rigide si les conditions suivantes sont vérifiées :

1. le r-uplet g_1, \dots, g_r est irréductible ;
2. on a $g_1 \cdots g_r = Id$;
3. pour tout r-uplet $\tilde{g}_1, \dots, \tilde{g}_r$ tel que $\tilde{g}_1 \cdots \tilde{g}_r = Id$, où \tilde{g}_i est conjugué à g_i , il existe une matrice $U \in \text{GL}_n(\mathbb{C})$ telle que $\tilde{g}_i = U g_i U^{-1}$ pour tout $i \in \{1, \dots, r\}$.

Proposition 2.2.3. Soient $A \in \mathcal{M}_n(\mathbb{C}(z))$ et $\frac{d}{dz}y = Ay$ fuchsien. Si le groupe de monodromie de $\frac{d}{dz}y = Ay$ est rigide alors le système $\frac{d}{dz}y = Ay$ est rigide.

En effet, cette proposition découle de la proposition suivante qui est un cas particulier du théorème 6.15 de [72].

Proposition 2.2.4. Soient $A, A' \in \mathcal{M}_n(\mathbb{C}(z))$. Si $\frac{d}{dz}y = Ay$ et $\frac{d}{dz}y = A'y$ sont deux systèmes fuchsien dont les groupes de monodromie sont conjugués, alors les matrices A et A' sont $\mathbb{C}(z)$ -équivalentes.

Soient $L \in \mathbb{C}(z)[d/dz]$ et A sa matrice compagnon. Si L est un opérateur fuchsien, alors le système différentiel $\frac{d}{dz}y = Ay$ est fuchsien (cf. remarque 2.3.4).

Définition 2.2.5 (Opérateur rigide). Soient $L \in \mathbb{C}(z)[d/dz]$ fuchsien et A sa matrice compagnon. L'opérateur L est rigide si le système différentiel $\frac{d}{dz}y = Ay$ est dit rigide.

Le calcul de la matrice de monodromie locale n'est pas facile. Par contre, dans le cas où γ est un point singulier régulier nous pouvons la calculer à conjugaison près. Nous ferons cela dans le lemme suivant. Avant, nous rappelons la notion d'exposants en γ . Soit $\gamma \in \mathbb{C}$ un point singulier régulier du système (2.5). Cela veut dire qu'il existe une matrice $A_\gamma \in \mathcal{M}_n(\mathbb{C}(z))$ telle que les matrices A et A_γ sont localement équivalentes en γ et la matrice $(z - \gamma)A_\gamma$ n'a pas de pôle en γ . Les exposants en γ sont les valeurs propres de la matrice $[(z - \gamma)A_\gamma](\gamma)$. Dans le cas que $\gamma = \infty$, γ est un point singulier régulier s'il existe une matrice $A_\infty \in \mathcal{M}_n(\mathbb{C}(z))$ telle que les matrices A et A_∞ sont localement équivalentes en γ et la matrice zA_∞ n'a pas de pôle en γ . Les exposants en l'infini sont les valeurs propres de la matrice $[zA_\infty](\gamma)$. Notons que cette définition dépend de la matrice A_γ . Par contre, d'après le lemme 2.4 de [42, Chap V], si A'_γ est telle que A et A'_γ sont localement équivalentes en γ et $(z - \gamma)A'_\gamma$ n'a pas de pôle en γ , alors les valeurs propres de $[(z - \gamma)A_\gamma](\gamma)$ et les valeurs propres de $[(z - \gamma)A'_\gamma](\gamma)$ sont égales modulo \mathbb{Z} .

Lemme 2.2.6. Soient $A \in \mathcal{M}_n(\mathbb{C}(z))$ et $\gamma \in \mathbb{C} \cup \{\infty\}$ un point singulier régulier du système différentiel $\frac{d}{dz}y = Ay$. Alors il existe une matrice $C \in \mathcal{M}_n(\mathbb{C})$ telle que $\exp(2\pi iC)$ est conjuguée à la matrice de monodromie locale de A en γ et satisfaisant aux deux propriétés suivantes :

(a) si λ, β sont deux valeurs propres différentes de C , alors $\lambda - \beta \notin \mathbb{Z}$,

(b) l'ensemble des exposants de A en γ et l'ensemble des valeurs propres de C sont égaux modulo \mathbb{Z} .

Démonstration. Sans perdre de généralité supposons que $\gamma = 0$. Soit $A_0(z) \in \mathcal{M}_n(\mathbb{C}(z))$ telle que les matrices $A(z)$ et $\frac{1}{z}A_0(z)$ sont localement équivalentes en zéro et A_0 n'a pas de pôle en zéro. Comme $A_0(z) \in \mathcal{M}_n(\mathbb{C}[[z]])$, le lemme 8.2 et le corollaire 8.3 de [42, chap. III] nous assure l'existence d'une matrice $W_0(z) \in \mathcal{M}_n(\mathbb{C}[[z]])$ telle que les matrices $\frac{1}{z}A_0(z)$ et $\frac{1}{z}W_0(z)$ sont localement équivalentes en zéro et les valeurs propres de $C := W_0(0)$ satisfont aux conditions (a) et (b) de l'énoncé. D'après le théorème 5.1 de [72], on obtient que la matrice de monodromie locale du système $\frac{d}{dz}y = \frac{1}{z}W_0(z)y$ en 0 est conjuguée à $\exp(2\pi iC)$. Puisque $\frac{1}{z}A_0(z)$ et $\frac{1}{z}W_0(z)$ sont localement équivalentes en zéro, alors toujours par le théorème 5.1 de [72], la matrice de monodromie locale en zéro du système $\frac{d}{dz}y = \frac{1}{z}A_0(z)y$ est conjuguée à $\exp(2\pi iC)$. Finalement, comme $A(z)$ et $\frac{1}{z}A_0(z)$ sont localement équivalentes en zéro alors, d'après le théorème 5.1 de [72], la matrice de monodromie locale en zéro de $\frac{d}{dz}y = A(z)y$ est conjuguée à $\exp(2\pi iC)$ et comme nous l'avons déjà écrit, C satisfait aux conditions (a) et (b). \square

Remarque 2.2.7. Soit K un corps algébriquement clos. Il suit de la démonstration du lemme 8.2 et du corollaire 8.3 de [42, Chap.III] que, si $A_0 \in \mathcal{M}_n(K(z))$, alors $W_0 \in \mathcal{M}_n(K(z))$ et les matrices $\frac{1}{z}A_0(z)$ et $\frac{1}{z}W_0(z)$ sont $K(z)$ -équivalentes. De plus, la matrice $C := W_0(0)$ vérifie les conditions du lemme 2.2.6.

2.2.1 Opérateurs rigides et équations qui proviennent de la géométrie.

D'après Katz [52, Theorem 9.4], si L est un opérateur rigide alors le module différentiel défini par L est un sous-module différentiel d'un module différentiel associé à une équation de *Picard-Fuchs*. Or les équations de Picard-Fuchs sont munies d'une structure de Frobenius forte pour presque tout p (voir par exemple [54, Theorem 22.2.1]). Ainsi, on peut s'attendre à ce qu'un opérateur rigide soit muni d'une structure de Frobenius forte pour presque tout p . Le théorème 1.4.10 montre que c'est bien le cas et que, de plus, la période h des structures de Frobenius fortes peut être majorée explicitement et indépendamment du nombre premier p . Comme nous l'avons déjà mentionné, ce dernier point est essentiel au vu de la conjecture 4 et du théorème 1.4.6. Il semble que l'on puisse obtenir l'existence d'une structure de Frobenius forte pour n'importe quel sous module N d'un module différentiel M associé à une équation de Picard-Fuchs. En effet, d'après le théorème 4.2.6 [33], M est semi-simple et donc N est semi-simple et on peut le décomposer comme somme directe finie de sous-modules simples N_i . Rappelons que d'après le Theorem 22.2.1 de [54], M a une structure de Frobenius forte pour presque tout p . Soit p l'un de ces nombres premiers et h la période de la structure de Frobenius forte correspondante. En notant ϕ le Frobenius, on a donc que $\phi^h(M)$ et M sont isomorphes. Donc, pour tout $m \geq 1$, $\phi^{mh}(N_i)$ est sous module simple de $\phi^h(M)$ et on obtient l'existence de deux entiers m et m' tels que $\phi^{mh}(N_i) = \phi^{m'h}(N_i)$. Autrement dit, N_i est muni d'une structure de Frobenius forte pour p . On en déduit que N est muni d'une structure de Frobenius forte pour p car l'application ϕ respecte les sommes directes. Malheureusement, cet argument ne permet pas de majorer précisément la période h de cette structure de Frobenius forte,

ni même de la majorer indépendamment de p . L'intérêt principal du théorème 1.4.10 est qu'il permet justement de majorer la période des structures de Frobenius fortes des opérateurs rigides indépendamment de p . Le théorème 1.4.10 a également été obtenu sous une forme légèrement différente, mais essentiellement équivalente, par Crew [32]. Il nous semble néanmoins utile de présenter la démonstration proposée ici qui est écrite dans un langage différent et plus élémentaire, notamment exempt de toute considération cohomologique. Notons qu'un cas particulier du théorème 1.5 de [44] implique aussi qu'un opérateur différentiel satisfaisant aux conditions du théorème 1.4.10 a une structure de Frobenius forte pour presque tout p . Mais ce dernier résultat ne donne pas explicitement de renseignement sur la période des structures de Frobenius associées et ne permet donc pas d'utiliser le théorème 1.4.6 comme nous le faisons.

2.3 Démonstration du théorème 1.4.10

Nous rappelons que $Frob : \mathbb{C}_p \rightarrow \mathbb{C}_p$ est l'automorphisme de Frobenius de \mathbb{C}_p choisi dans la remarque 1.4.1. À présent, nous présentons les différentes étapes de la preuve du théorème 1.4.10. Celles-ci seront démontrées dans la partie 2.3.3.

Premier pas. Le premier pas est consacré au calcul des groupes de monodromie locale de L à conjugaison près. Plus précisément, soit A la matrice compagnon de L et soient $\gamma_1 = 0, \dots, \gamma_r = \infty$ les points singuliers réguliers de L . Pour tout $j \in \{1, \dots, r\}$, soit $M(A, \gamma_j)$ la matrice de monodromie locale de A en γ_j . À l'aide du lemme 2.2.6 nous allons montrer qu'elle est conjuguée à une matrice de la forme $\exp(2\pi i C_j)$, où $C_j \in \mathcal{M}_n(\mathbb{C})$ satisfait aux conditions suivantes :

- (a) Si λ, β sont deux valeurs propres différentes de C_j , alors $\lambda - \beta \notin \mathbb{Z}$.
- (b) L'ensemble des exposants de L en γ_j et l'ensemble des valeurs propres de C_j sont égaux modulo \mathbb{Z} .

Deuxième pas. Nous montrerons que pour $p \in \mathcal{S}$ et tout $j \in \{1, \dots, r\}$, les matrices $\exp(2\pi i C_j)$ et $\exp(2\pi i p^h C_j)$ sont conjuguées. Nous rappelons que l'ensemble de nombres premiers \mathcal{S} et l'entier h sont définis comme dans le théorème 1.4.10.

Troisième pas. Nous montrerons que pour tout $p \in \mathcal{S}$, la matrice $B = p^h z^{p^h - 1} A(z^{p^h})$ est E_p -équivalente à la matrice A . La matrice B est dans $\mathcal{M}_n(E_p)$. La démonstration de ce troisième pas se décompose selon les 3 étapes suivantes :

- (i) Soit m entier strictement positif tel que $-m$ n'est pas une singularité de L . Nous montrerons que B est E_p -équivalente à

$$G = \frac{\gamma_1 + m}{(z + m)(z - \gamma_1)} F_1 + \dots + \frac{\gamma_{r-1} + m}{(z + m)(z - \gamma_{r-1})} F_{r-1} - \frac{1}{z + m} F_r,$$

où $F_j \in \mathcal{M}_n(\mathbb{C}_p)$ pour $j \in \{1, \dots, r\}$.

Dans la démonstration de (ii) nous utiliserons un isomorphisme de corps $\kappa : \mathbb{C}_p \rightarrow \mathbb{C}$. L'isomorphisme κ s'étend naturellement en un isomorphisme de corps entre $\mathbb{C}_p(z)$ et $\mathbb{C}(z)$, que nous notons encore $\kappa : \mathbb{C}_p(z) \rightarrow \mathbb{C}(z)$. La matrice $M^\kappa \in \mathcal{M}_n(\mathbb{C}(z))$ désigne la matrice que l'on obtient en appliquant κ à chaque entrée de $M \in \mathcal{M}_n(\mathbb{C}_p(z))$.

- (ii) Nous montrerons d'une part que la matrice de monodromie locale de G^κ en $\kappa(\gamma_j)$, $M(G^\kappa, \kappa(\gamma_j))$, est conjuguée à la matrice $\exp(2\pi i p^h C_j)$. D'autre part, nous prouvons que la matrice de monodromie locale en $-m$ est l'identité.

D'après le deuxième pas, les matrices $\exp(2\pi i C_j)$ et $\exp(2\pi i p^h C_j)$ sont conjuguées. Ainsi, il découle du premier pas que pour $j \in \{1, \dots, r\}$, la matrice $M(A, \gamma_j)$ et la matrice $M(G^\kappa, \kappa(\gamma_j))$ sont conjuguées.

(iii) Comme la monodromie de $\frac{d}{dz}y = Ay$ est rigide, les conjugaisons des matrices $M(A, \gamma_j)$ et $M(G^\kappa, \kappa(\gamma_j))$ entraînent qu'il existe $U \in \mathrm{GL}_n(\mathbb{C})$ telle que $M(A, \gamma_j) = UM(G^\kappa, \kappa(\gamma_j))U^{-1}$ pour $1 \leq j \leq r$. Il suit donc que les groupes de monodromie des systèmes $Ay = \frac{d}{dz}y$ et $G^\kappa y = \frac{d}{dz}y$ sont isomorphes. D'après la correspondance de Riemann Hilbert, théorème 6.15 de [72], on obtient qu'il existe $H_1 \in \mathrm{GL}_n(\mathbb{C}(z))$ telle que

$$\frac{d}{dz}H_1 = AH_1 - H_1G^\kappa.$$

On pose $H = H_1^{\kappa^{-1}}$, ainsi $H \in \mathrm{GL}_n(\mathbb{C}_p(z)) \subset \mathrm{GL}_n(E_p)$ et

$$\frac{d}{dz}H = A^{\kappa^{-1}}H - HG.$$

Remarquons que $A^{\kappa^{-1}} = A$ car A est une matrice à coefficients dans $\mathbb{Q}(z)$. Par conséquent, A et G sont E_p -équivalentes. Or, d'après (i), on sait que G est E_p -équivalente à B . Par transitivité on conclut que A et B sont E_p -équivalentes.

2.3.1 Disque non singulier et singulier régulier

Dans cette partie nous énonçons et démontrons le théorème 2.3.1 ci-dessous. Ce résultat nous permettra dans la démonstration du théorème 1.4.10 de passer de la théorie des équations différentielles p-adiques à la théorie des équations différentielles classiques.

Pour tout $\gamma \in \mathbb{C}_p$, nous désignons par D_γ le disque ouvert de centre γ et de rayon 1 et par D_∞ l'ensemble des éléments de \mathbb{C}_p dont la norme est strictement supérieure à 1 et $\infty \in D_\infty$. Nous notons $\vartheta_{\mathbb{C}_p}$ l'ensemble des éléments de \mathbb{C}_p dont la norme est inférieure ou égale à 1 et si $\alpha, \gamma \in \vartheta_{\mathbb{C}_p}$ alors $D_\alpha = D_\gamma$ si, et seulement si $|\alpha - \gamma| < 1$. Et, $D_\alpha \cap D_\gamma = \emptyset$ si, et seulement si $|\alpha - \gamma| = 1$. Nous notons $E(D_\gamma)$ le complété pour la norme de Gauss des fractions rationnelles qui n'ont pas de pôle dans la boule D_γ .

Pour énoncer le théorème 2.3.1 nous aurons besoin de rappeler quelques notions de la théorie des équations différentielles p-adiques. Pour cela nous reprenons l'exposition de [21].

Soient $A \in \mathcal{M}_n(E_p)$ et $\gamma \in \vartheta_{\mathbb{C}_p}$. Nous dirons que la matrice A est *non singulière dans le disque* D_γ , respectivement à l'infini, s'il existe une matrice A_γ , respectivement A_∞ , E_p -équivalente à A et qui appartient à $\mathcal{M}_n(E(D_\gamma))$, respectivement à $z^2\mathcal{M}_n(E(D_\infty))$. Nous dirons que la matrice A est *singulière régulière dans le disque* D_γ , respectivement à l'infini, s'il existe un point β de D_γ et une matrice A_γ , respectivement A_∞ , E_p -équivalente à A tels que $(z - \beta)A_\gamma$ appartient à $\mathcal{M}_n(E(D_\gamma))$, respectivement zA_∞ appartient à $\mathcal{M}_n(E(D_\infty))$.

Théorème 2.3.1. *Soient $B \in \mathcal{M}_n(E_p)$ et $S = \{\gamma_1, \dots, \gamma_{r-1}\} \subset \vartheta_{\mathbb{C}_p}$ tel que pour tout $i \neq j$, $|\gamma_i - \gamma_j|_p = 1$. Supposons que pour tout $\gamma \in S \cup \{\infty\}$, la matrice B est singulière régulière dans le disque D_γ et que pour tout $\gamma \notin S \cup \{\infty\}$ la matrice B est non singulière dans le disque D_γ . Soit m un entier strictement positif tel que $-m \notin S$. Pour tout $\gamma \in S$, soient β_γ un point de D_γ et B_γ une matrice E_p -équivalente à B tels que $(z - \beta_\gamma)B_\gamma$ appartient à $\mathcal{M}_n(E(D_\gamma))$. Soit B_∞ une matrice E_p -équivalente à B , telle que zB_∞ appartient à $\mathcal{M}_n(E(D_\infty))$. Alors B est E_p -équivalente à une matrice G de la forme*

$$G = \frac{\beta_{\gamma_1} + m}{(z + m)(z - \beta_{\gamma_1})}G_1 + \dots + \frac{\beta_{\gamma_{r-1}} + m}{(z + m)(z - \beta_{\gamma_{r-1}})}G_{r-1} - \frac{1}{z + m}G_r, \quad (2.7)$$

où, pour $j \in \{1, \dots, r-1\}$, G_j est une matrice à coefficients dans \mathbb{C}_p semblable à la matrice $[(z - \beta_\gamma)B_\gamma](\beta_\gamma)$, G_r est une matrice à coefficients dans \mathbb{C}_p semblable à $[-zB_\infty](\infty)$ et $\sum_{\gamma \in S \cup \{\infty\}} G_\gamma$ est une matrice diagonale à coefficients dans \mathbb{Z} .

Le théorème 2.3.1 est démontré dans [21, théorème 4.2] dans le cas où le disque D_∞ est non singulier.

Démonstration. Considérons la matrice

$$V = -\frac{1}{z^2}B\left(\frac{1-zm}{z}\right),$$

obtenue en appliquant le changement de variables $z \mapsto \frac{1-zm}{z}$ au système $By = \frac{d}{dz}y$. Le disque D_∞ est non singulier pour la matrice V car le disque D_{-m} est non singulier pour la matrice B . Ainsi nous ramenons toutes les singularités à distance finie. Posons pour $j \in \{1, \dots, r-1\}$, $\tau_j = 1/(\beta_{\gamma_j} + m)$ et $\tau_r = 0$. Notons que pour $j \in \{1, \dots, r-1\}$, $|\beta_{\gamma_j} + m|_p = 1$ car D_{-m} est un disque non singulier pour la matrice B . Considérons l'ensemble $S' = \{\tau_1, \dots, \tau_{r-1}, 0\}$. Nous allons appliquer le théorème 4.2 de [21] à la matrice V et à l'ensemble S' . Nous allons donc montrer que V et S' satisfont aux hypothèses du théorème 4.2 de [21]. D'après le changement de variables choisi, il nous reste à vérifier que :

1. $|\tau_i - \tau_j| = 1$ pour $i \neq j$;
2. Soit η tel que $|\eta| \leq 1$ et $|\tau_i - \eta| = 1$ pour $i \in \{1, \dots, r\}$. Alors V est non singulière dans le disque D_η ;
3. Les disques singuliers réguliers de V sont exactement les disques D_{τ_j} , $1 \leq j \leq r-1$, et D_0 .

Preuve du point 1. On a

$$\tau_i - \tau_j = \frac{1}{\beta_{\gamma_i} + m} - \frac{1}{\beta_{\gamma_j} + m} = \frac{\beta_{\gamma_j} - \beta_{\gamma_i}}{(\beta_{\gamma_i} + m)(\beta_{\gamma_j} + m)}.$$

Par hypothèse $|\gamma_j - \gamma_i| = 1$ alors $|\beta_{\gamma_i} - \beta_{\gamma_j}| = 1$ et on a déjà vu que $|(\beta_{\gamma_j} + m)| = 1$ pour $j \in \{1, \dots, r-1\}$, d'où $|(\beta_{\gamma_i} + m)(\beta_{\gamma_j} + m)| = 1$. Ainsi $|\tau_i - \tau_j| = 1$.

Preuve du point 2. Comme $|\tau_i - \eta| = 1$ pour tout $i \in \{1, \dots, r\}$, alors on a $|\eta| = 1$ car $\tau_r = 0$. Supposons que V est singulière dans le disque D_η , alors la matrice B est singulière dans le disque $D_{\frac{1-\eta m}{\eta}}$. Donc, il existe $i \in \{1, \dots, r-1\}$ tel que

$$\overline{\beta_{\gamma_i}} = \overline{\left(\frac{1-\eta m}{\eta}\right)}$$

et comme $\beta_{\gamma_i} = \frac{1-\tau_i m}{\tau_i}$ il suit que

$$\overline{\left(\frac{1-\eta m}{\eta}\right)} = \overline{\left(\frac{1-\tau_i m}{\tau_i}\right)}.$$

Ainsi, on a $\bar{\eta} = \bar{\tau}_i$. Autrement dit $|\tau_i - \eta| < 1$, ce qui est une contradiction.

Preuve du point 3. Par hypothèse pour chaque $j \in \{1, \dots, r-1\}$, la matrice B est E_p -équivalente à B_{γ_j} , où $(z - \beta_{\gamma_j})B_{\gamma_j}$ appartient à $\mathcal{M}_n(E(D_{\gamma_j}))$. Ainsi, $B_{\gamma_j} = \frac{1}{z - \beta_{\gamma_j}}H_{\gamma_j}$, où H_{γ_j} appartient à $\mathcal{M}_n(E(D_{\gamma_j}))$. Montrons que V est E_p -équivalente à

$$V_j = -\frac{1}{z} \cdot \frac{1}{1 - z(m + \beta_{\gamma_j})} H_{\gamma_j} \left(\frac{1 - zm}{z}\right).$$

En effet, on sait qu'il existe $G_j \in \mathrm{GL}_n(E_p)$ telle que

$$\frac{d}{dz}G_j = BG_j - G_jB_{\gamma_j}.$$

On pose $T_j := G_j \left(\frac{1-zm}{z} \right) \in \mathrm{GL}_n(E_p)$, donc en appliquant la dérivée d'une composition on obtient que

$$\begin{aligned} \frac{d}{dz}T_j &= \left[B \left(\frac{1-zm}{z} \right) G_j \left(\frac{1-zm}{z} \right) - G_j \left(\frac{1-zm}{z} \right) B_{\gamma_j} \left(\frac{1-zm}{z} \right) \right] \left(\frac{-1}{z^2} \right) \\ &= VT_j - T_j \cdot \left(\left(\frac{-1}{z^2} \right) B_{\gamma_j} \left(\frac{1-zm}{z} \right) \right). \end{aligned} \quad (2.8)$$

Mais $B_{\gamma_j} = \frac{1}{z-\beta_{\gamma_j}}H_{\gamma_j}$ entraîne que

$$B_{\gamma_j} \left(\frac{1-zm}{z} \right) = \frac{z}{1-z(m+\beta_{\gamma_j})}H_{\gamma_j} \left(\frac{1-zm}{z} \right),$$

d'où

$$\left(\frac{-1}{z^2} \right) B_{\gamma_j} \left(\frac{1-zm}{z} \right) = V_j$$

et ainsi

$$\frac{d}{dz}T_j = VT_j - T_jV_j.$$

Donc V et V_j sont E_p -équivalentes.

Comme $m + \beta_{\gamma_j} = 1/\tau_j$ pour $1 \leq i \leq j-1$, il vient que

$$V_j = -\frac{1}{z} \cdot \frac{\tau_j}{\tau_j - z} H_{\gamma_j} \left(\frac{1-zm}{z} \right). \quad (2.9)$$

Enfin, comme B est E_p -équivalente à B_∞ , où $B_\infty = \frac{1}{z}H_\infty$ avec H_∞ dans $\mathcal{M}_n(E(D_\infty))$ alors V est E_p -équivalente à

$$V_\infty := -\frac{1}{z} \cdot \frac{1}{1-zm} H_\infty \left(\left(\frac{1-zm}{z} \right) \right). \quad (2.10)$$

Pour finir, montrons que, pour tout $j \in \{1, \dots, r-1\}$, la matrice $(z - \tau_j)V_j$ est non singulière dans le disque D_{τ_j} . En effet, d'après (2.9), $(z - \tau_j)V_j = \frac{\tau_j}{z}H_{\gamma_j} \left(\frac{1-zm}{z} \right)$. Soit $y \in D_{\tau_j}$, alors $\frac{1-ym}{y} \in D_{\gamma_j}$ et par conséquent, la matrice $H_{\gamma_j} \left(\frac{1-zm}{z} \right)$ n'a pas de pôle en y car H_{γ_j} appartient à $M(E(D_{\gamma_j}))$. Donc la matrice $(z - \tau_j)V_j$ est non singulière dans le disque D_{τ_j} . De manière similaire, on montre que la matrice zV_∞ est non singulière dans le disque D_0 .

Par conséquent, le théorème 4.2 de [21] montre que V est E_p -équivalente à la matrice

$$F = \sum_{i=1}^r \frac{1}{z - \tau_j} G_j, \quad (2.11)$$

où, pour tout $j \in \{1, \dots, r-1\}$, G_j est une matrice carrée à coefficients dans \mathbb{C}_p semblable à $[(z - \tau_j)V_j](\tau_j)$, G_r est semblable à $(zV_r)(0)$ et $\sum_{i=1}^r G_j$ est une matrice diagonale à coefficients dans \mathbb{Z} . De (2.9) et (2.10) il suit que

$$[(z - \tau_j)V_j](\tau_j) = H_{\gamma_j}(\gamma_j) \quad \text{et} \quad (zV_\infty)(0) = -H_\infty(\infty). \quad (2.12)$$

En particulier, le théorème 4.2 de [21] montre qu'il existe $T \in \text{GL}_n(E_p)$ telle que

$$\frac{d}{dz}T = VT - TF.$$

En posant $H_2 = T \left(\frac{1}{z+m} \right)$, on a $H_2 \in \text{GL}_n(E_p)$ et

$$\begin{aligned} \frac{d}{dz}H_2 &= \left[V \left(\frac{1}{z+m} \right) T \left(\frac{1}{z+m} \right) - T \left(\frac{1}{z+m} \right) F \left(\frac{1}{z+m} \right) \right] \left(\frac{-1}{(z+m)^2} \right) \\ &= \left[-(z+m)^2 B H_2 - H_2 F \left(\frac{1}{z+m} \right) \right] \left(\frac{-1}{(z+m)^2} \right) \\ &= B H_2 - H_2 \cdot \left(\frac{-1}{(z+m)^2} F \left(\frac{1}{z+m} \right) \right). \end{aligned} \quad (2.13)$$

Ainsi, B est E_p -équivalente à $G := -\frac{1}{(z+m)^2} F \left(\frac{1}{z+m} \right)$. Comme $\tau_j = 1/(\beta_{\gamma_i} + m)$, l'égalité (2.11) donne que

$$G = \frac{\beta_{\gamma_1} + m}{(z+m)(z-\beta_{\gamma_1})} G_1 + \cdots + \frac{\beta_{\gamma_{r-1}} + m}{(z+m)(z-\beta_{\gamma_{r-1}})} G_{r-1} - \frac{1}{z+m} G_r.$$

Finalement, d'après (2.12), G_j est semblable à $H_{\gamma_j}(\gamma_j)$ mais, $H_{\gamma_j}(\gamma_j) = [(z-\beta_{\gamma_j})B_{\gamma_j}](\beta_{\gamma_j})$ donc, G_j est semblable à $[(z-\beta_{\gamma_j})B_{\gamma_j}](\beta_{\gamma_j})$. Encore par (2.12), la matrice G_r est semblable à $-H_\infty(\infty)$, mais $H_\infty(\infty) = [zB_\infty](\infty)$ alors $-H_\infty(\infty)$ est semblable $[zB_\infty](\infty)$. \square

Remarque 2.3.2. Il suit de la démonstration du théorème 4.2 de [21] que, l'infini est une singularité régulière apparente de F . Alors, $-m$ est une singularité régulière apparente de G et par conséquent, G a une base de solutions à coefficients dans $\mathbb{C}_p((z+m))$.

2.3.2 Lemmes préparatoires.

Afin de démontrer les trois pas précédents, nous aurons besoin des lemmes préparatoires suivants.

Le premier lemme est un résultat qui semble classique mais nous utiliserons les idées de la preuve dans la démonstration du théorème 1.4.10. On pose

$$L = \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} + a_n(z) \in \mathbb{Q}(z)[d/dz], \quad (2.14)$$

Lemme 2.3.3. *Considérons l'opérateur différentiel (2.14) et soit A la matrice compagnon associée à L . Si $\gamma \in \overline{\mathbb{Q}} \cup \{\infty\}$ est un point singulier régulier de L , alors il existe $A_\gamma \in \mathcal{M}_n(\overline{\mathbb{Q}}(z))$ telle que :*

1. Les matrices A et $\frac{1}{z-\gamma}A_\gamma$ sont $\mathbb{Q}(\gamma)(z)$ -équivalentes. Et si γ est l'infini alors A et $\frac{-1}{z}A_\infty$ sont $\mathbb{Q}(z)$ -équivalentes.
2. A_γ n'a pas de pôle en γ ;
3. Les valeurs propres de $A_\gamma(\gamma)$ sont les exposants de l'équation en γ .

Remarque 2.3.4. Ce lemme est encore valide quand $L \in \mathbb{C}(z)[d/dz]$, mais dans ce cas nous pouvons seulement affirmer que A et $\frac{1}{z-\gamma}A_\gamma$ sont $\mathbb{C}(z)$ -équivalentes et il en va de même pour l'infini. En particulier si L est fuchsien alors le système différentiel $\frac{d}{dz}y = Ay$ est fuchsien.

Démonstration. Notons que $z^n \frac{d^n}{dz^n} = \delta(\delta - 1) \cdots (\delta + n - 1)$, où $\delta = z \frac{d}{dz}$. Ainsi, il existe $a_{1j}, \dots, a_{jj} \in \mathbb{Z}$ tels que $\frac{d^j}{dz^j} = \frac{a_{1j}}{z^j} \delta + \cdots + \frac{a_{jj}}{z^j} \delta^j$. Soit

$$G_n = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & \frac{1}{z} & 0 & 0 & \cdots & 0 & 0 \\ 0 & -\frac{1}{z^2} & \frac{1}{z^2} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & \frac{a_{1,n-1}}{z^{n-1}} & \frac{a_{2,n-1}}{z^{n-1}} & \frac{a_{3,n-1}}{z^{n-1}} & \cdots & \frac{a_{n-2,n-1}}{z^{n-1}} & \frac{1}{z^{n-1}} \end{pmatrix} \in \text{GL}_n(\mathbb{Z}[1/z])$$

la matrice exprimant $\{1, \dots, \frac{d^{n-1}}{dz^{n-1}}\}$ en fonction de $\{1, \delta, \dots, \delta^{n-1}\}$.

Soit γ un point singulier régulier de L . Nous commençons par considérer un nouvel opérateur

$$L_\gamma := \frac{d^n}{dz^n} + a_1(z + \gamma) \frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z + \gamma) \frac{d}{dz} y + a_n(z + \gamma)$$

que l'on écrit sous la forme

$$\delta^n + q_1(z)\delta^{n-1} + \cdots + q_{n-1}(z)\delta + q_n(z), \quad (2.15)$$

où $\delta = z \frac{d}{dz}$ et

$$(q_n(z), \dots, q_1(z), 1) = (a_n(z + \gamma), \dots, a_1(z + \gamma), 1) z^n G_{n+1}. \quad (2.16)$$

On rappelle que les exposants de (2.14) en γ sont les zéros du polynôme

$$\lambda^n + q_1(0)\lambda^{n-1} + \cdots + q_{n-1}(0)\lambda + q_n(0),$$

où $q_n(z), \dots, q_1(z)$ sont définis dans (2.16).

Notons que $q_i(z) \in \mathbb{Q}(\gamma)(z)$ pour $1 \leq i \leq n$. Soit

$$B_\gamma = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ -q_n(z) & -q_{n-1}(z) & \cdots & -q_2(z) & -q_1(z) \end{pmatrix}.$$

D'après le théorème de Fuchs, B_γ n'a pas de pôle en zéro. Montrons que les valeurs propres de $B_\gamma(0)$ sont les exposants en γ . En effet, le polynôme caractéristique de $B_\gamma(0)$ est $(-1)^n(\lambda^n + q_1(0)\lambda^{n-1} + \cdots + q_{n-1}(0)\lambda + q_n(0))$. Posons

$$A_\gamma = B_\gamma(z - \gamma) \in \mathcal{M}_n(\mathbb{Q}(\gamma)(z)). \quad (2.17)$$

Alors, A_γ n'a pas de pôle en γ et les valeurs propres de $A_\gamma(\gamma)$ sont les exposants en γ . Ainsi, elle appartient à $\mathcal{M}_n(\mathbb{Q}\{z - \gamma\})$. Donc A_γ satisfait aux points 2 et 3 du lemme 2.3.3. Montrons qu'elle satisfait aussi le point 1.

Soit C_γ la matrice compagnon associée à l'équation L_γ . Montrons que

$$\frac{d}{dz} G_n = C_\gamma G_n - G_n \frac{1}{z} B_\gamma.$$

Soit f une solution quelconque de L_γ . On pose $(\mathbf{d}f) = (f, f', \dots, f^{(n-1)})^t$ et $(\delta f) = (f, \delta f, \dots, \delta^{(n-1)} f)^t$. Alors, $\frac{d}{dz}(\mathbf{d}f) = C_\gamma(\mathbf{d}f)$ et $\delta(\delta f) = B_\gamma(\delta f)$. D'après la construction

de la matrice G_n , nous avons que $(\mathbf{d}f) = G_n(\delta f)$. En appliquant d/dz à cette dernière égalité, on a que

$$C_\gamma(\mathbf{d}f) = \left(\frac{d}{dz} G_n \right) (\delta f) + G_n \frac{d}{dz} (\delta f) = \left(\frac{d}{dz} G_n \right) (\delta f) + G_n \frac{1}{z} \delta(\delta f).$$

Mais $(\mathbf{d}f) = G_n(\delta f)$ et $\delta(\delta f) = B_\gamma(\delta f)$. Donc,

$$C_\gamma G_n(\delta f) = \left(\frac{d}{dz} G_n \right) (\delta f) + G_n \frac{1}{z} B_\gamma(\delta f).$$

Finalement, comme f est une solution quelconque de L_γ et que l'espace des solutions de L_γ est de dimension n sur \mathbb{C} , on obtient que

$$C_\gamma G_n = \frac{d}{dz} G_n + G_n \frac{1}{z} B_\gamma.$$

Notons que $A = C_\gamma(z - \gamma)$, alors en posant $H_\gamma := G_n(z - \gamma) \in \mathrm{GL}_n(\mathbb{Q}(\gamma)(z))$, il vient

$$\frac{d}{dz} H_\gamma = A H_\gamma - H_\gamma \frac{1}{z - \gamma} A_\gamma.$$

Pour l'infini, considérons l'équation différentielle

$$\frac{d^n}{dz^n} y + b_1(z) \frac{d^{n-1}}{dz^{n-1}} y + \cdots + b_{n-1}(z) \frac{d}{dz} y + b_n(z) y = 0, \quad (2.18)$$

où $(b_n(z), \dots, b_1(z), 1) = (a_n(1/z), \dots, a_1(1/z), 1) \frac{(-1)^n}{z^{2n}} W_n$ et

$$W_n = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & -z^2 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 2z^3 & z^4 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & * & * & * & \cdots & * & (-z^2)^n \end{pmatrix}$$

qui est la matrice qui exprime le vecteur $(1, D, \dots, D^n)$ en fonction de $(1, \frac{d}{dz}, \dots, \frac{d^n}{dz^n})$, où $D = -z^2 \frac{d}{dz}$.

Comme l'infini est singulier régulier, alors zéro est un point singulier régulier de (2.18) et par définition les exposants à l'infini de (2.14) sont les exposants en zéro de (2.18). Notons \tilde{A} la matrice compagnon de (2.18). Il existe une matrice \tilde{A}_0 qui n'a pas de pôle en zéro, les valeurs propres de $\tilde{A}_0(0)$ sont les exposant en zéro de (2.18) et $\frac{1}{z} \tilde{A}_0$ et \tilde{A} sont $\mathbb{Q}(z)$ -équivalentes. Alors il existe $\tilde{H}_0 \in \mathrm{GL}_n(\mathbb{Q}(z))$ telle que

$$\frac{d}{dz} \tilde{H}_0 = \frac{1}{z} \tilde{A}_0 \tilde{H}_0 - \tilde{H}_0 \tilde{A}.$$

Ainsi, si $\tilde{G} = \tilde{H}_0(1/z) \in \mathbb{Q}(z)$ on a

$$\frac{d}{dz} \tilde{G} = -\frac{1}{z} \tilde{A}_0(1/z) \tilde{G} - \tilde{G} \cdot \left(\frac{-1}{z^2} \tilde{A}(1/z) \right).$$

Soit f un solution de L et soit $g = f(1/z)$, on pose $(\mathbf{d}f) = (f, f', \dots, f^{(n-1)})^t$, $(\mathbf{d}g) = (g, g', \dots, g^{(n-1)})^t$. À l'aide des égalités $\mathbf{d}f = (W_n \mathbf{d}g)(1/z)$, $\frac{d}{dz}(\mathbf{d}f) = A \mathbf{d}f$ et $\frac{d}{dz}(\mathbf{d}g) = \tilde{A} \mathbf{d}g$, on obtient que

$$\frac{d}{dz} W_n = -\left(\frac{1}{z^2} A(1/z) \right) W_n - W_n \tilde{A}.$$

Posons $T_\infty = W_n(1/z) \in \mathrm{GL}_n(\mathbb{Q}(z))$, il vient donc $\frac{d}{dz}T_\infty = A(z)T_\infty - T_\infty \left(\frac{-1}{z^2}\tilde{A}(1/z)\right)$.
Maintenant, en posant $H_\infty = \tilde{G}T_\infty^{-1} \in \mathrm{GL}_n(\mathbb{Q}(z))$, il vient

$$\frac{d}{dz}H_\infty = -\frac{1}{z}\tilde{A}_0(1/z)H_\infty - H_\infty A.$$

Par conséquent, les matrices A et $-\frac{1}{z}\tilde{A}_0(1/z)$ sont $\mathbb{Q}(z)$ -équivalentes. On pose $A_\infty = \tilde{A}_0(1/z)$, ainsi la matrice A_∞ satisfait aux conditions demandées. \square

Notons que pour tout nombre premier p , γ appartient à la clôture algébrique de \mathbb{Q}_p , car il annule un polynôme à coefficients dans $\mathbb{Q} \subset \mathbb{Q}_p$. La démonstration précédente montre que $A_\gamma, H_\gamma \in \mathrm{GL}_n(\mathbb{Q}(\gamma)(z))$ et $A_\infty, H_\infty \in \mathrm{GL}_n(\mathbb{Q}(z))$, notamment $A_\gamma, H_\gamma \in \mathrm{GL}_n(E_p)$ et ainsi les matrices $A, \frac{1}{z-\gamma}A_\gamma$ sont E_p -équivalentes. On obtient le corollaire suivant.

Corollaire 2.3.5. *Soient $L \in \mathbb{Q}(z)[d/dz]$, $A, A_\gamma \in \mathcal{M}_n(\overline{\mathbb{Q}}(z))$, $\gamma \in \overline{\mathbb{Q}} \in \{\infty\}$ comme dans le lemme 2.3.3.*

1. *Soit p un nombre premier tel que le disque $D_\gamma \subset \mathbb{C}_p$ ne contient pas d'autres points singulier de L . Alors le disque D_γ est non singulier pour A_γ .*
2. *Soit p un nombre premier tel que tous les points singuliers de L à distance finie ont norme p -adique égale à 1. Supposons que l'infini est un point singulier régulier de L . Alors le disque D_∞ est non singulier pour la matrice A_∞ .*
3. *Soit p un nombre premier tel que $\|A\|_p \leq 1$ et $|\gamma|_p = 1$, alors $\|A_\gamma\|_p \leq 1$ et $\|\frac{1}{z-\gamma}A_\gamma\|_{\mathcal{G},p} \leq 1$.*

Pour $A = (a_{ij}) \in \mathcal{M}_n(E_p)$, $\|A\|_{\mathcal{G},p} = \max(|a_{ij}|_{\mathcal{G},p})$.

Démonstration. Avec les notations de la preuve du lemme 2.3.3, l'équation (2.17) donne que

$$A_\gamma = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ -q_n(z-\gamma) & -q_{n-1}(z-\gamma) & \dots & -q_2(z-\gamma) & -q_1(z-\gamma) \end{pmatrix}.$$

et de (2.16) on a que

$$(q_n(z-\gamma), \dots, q_1(z-\gamma), 1) = (a_n(z), \dots, a_1(z), 1)(z-\gamma)^n G_{n+1}(z-\gamma). \quad (2.19)$$

Notons que $(z-\gamma)^n G_{n+1}(z-\gamma) \in \mathrm{GL}_n(\mathbb{Z}[z-\gamma])$.

1. Cela revient à montrer que $A_\gamma \in \mathcal{M}_n(E(D_\gamma))$, c'est-à-dire que A_γ n'a pas de pôle en D_γ . En effet, soit $\alpha \in \overline{\mathbb{Q}}$ une singularité de A_γ . D'après le lemme 2.3.3, on a $\alpha \neq \gamma$ car A_γ n'a pas de pôle en γ . L'équation (2.19) donne que α est une singularité de A et d'après l'hypothèse, $\alpha \notin D_\gamma$, ainsi $A_\gamma \in \mathcal{M}_n(D_\gamma)$.
2. Rappelons que $A_\infty = \tilde{A}_0(1/z)$. Notons que les singularités de (2.18) sont 0 et $1/\gamma$, avec γ une singularité de L . De l'hypothèse, $|1/\gamma|_p = 1$, ainsi D_0 ne contient pas d'autre point singulier de (2.18). Alors, du point 1 du corollaire, A_0 est non singulier dans le disque D_0 et ainsi A_∞ est non singulier dans le disque D_∞ .

3. D'après l'hypothèse, $\|(a_n(z), \dots, a_1(z), 1)\|_{\mathcal{G},p} \leq 1$, $\|(z - \gamma)\|_{\mathcal{G},p} = 1$ et notons que

$$G_{n+1}(z - \gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & \frac{1}{z-\gamma} & 0 & 0 & \dots & 0 & 0 \\ 0 & -\frac{1}{(z-\gamma)^2} & \frac{1}{(z-\gamma)^2} & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & \frac{a_{1,n}}{(z-\gamma)^n} & \frac{a_{2,n}}{(z-\gamma)^n} & \frac{a_{3,n}}{(z-\gamma)^n} & \dots & \frac{a_{n-1,n}}{(z-\gamma)^n} & \frac{1}{(z-\gamma)^n} \end{pmatrix}.$$

Comme les a_{ij} sont entiers, on a $\|G_{n+1}(z - \gamma)\|_{\mathcal{G},p} \leq 1$ et l'équation (2.19) donne

$$\|(q_n(z - \gamma), \dots, q_1(z - \gamma), 1)\|_{\mathcal{G},p} \leq 1.$$

Ainsi, $\|A_\gamma\|_{\mathcal{G},p} \leq 1$. Finalement, comme $\|\frac{1}{z-\gamma}\|_{\mathcal{G},p} = 1$, alors

$$\|\frac{1}{z-\gamma}A_\gamma\|_{\mathcal{G},p} = \|\frac{1}{z-\gamma}\|_{\mathcal{G},p}\|A_\gamma\|_{\mathcal{G},p} \leq 1.$$

□

Nous aurons besoin du lemme suivant pour la démonstration du deuxième pas du théorème 1.4.10.

Lemme 2.3.6. *Soient $a_0(z) \in \mathbb{Q}[z]$, K le corps de décomposition de $a_0(z)$ sur \mathbb{Q} , h_2 la dimension de K comme \mathbb{Q} -espace vectoriel et s la valuation de $a_0(z)$. Considérons l'ensemble \mathcal{S}' des nombres premiers tels que le coefficient dominant de $a_0(z)$ et le terme constant du polynôme $a_0(z)/z^s$ aient une norme p -adique égale à 1 et que $a_0(z) \in \mathbb{Z}_{(p)}[z]$. Alors pour tout $p \in \mathcal{S}'$, tout entier $m \geq 1$ et toute racine γ de $a_0(z)$, on a*

$$|\gamma^{p^{mh_2}} - \gamma|_p < \frac{1}{p} < |\pi_p|.$$

Remarque 2.3.7. Notons que l'ensemble $\mathcal{P} \setminus \mathcal{S}'$ est fini.

Démonstration. Si $\gamma = 0$ il n'a rien à prouver. Supposons donc que $\gamma \neq 0$. Soit $p \in \mathcal{S}'$, alors $a_0(z) \in \mathbb{Z}_{(p)}[z]$ car $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$. Soient K_p le corps de décomposition de $a_0(z)$ sur \mathbb{Q}_p et h_3 la dimension de K_p comme \mathbb{Q}_p -espace vectoriel. Il suit du théorème 6.1 de [42, Chap. I] que les racines non nulles de $a_0(z)$ ont une norme égale à 1. Soit $P(z) = a_0(z)/z^s$. Notons que $P_0(z) \in \mathbb{Z}_{(p)}[z]$. Comme $|P(0)|_p = 1$ et toutes les racines de $P(z)$ ont norme égale à 1 alors $P(z)$ est irréductible sur \mathbb{Q}_p . Soit $\bar{P}(z)$ le polynôme qui est obtenu après avoir réduit les coefficients de $P(z)$ modulo l'idéal maximal de $\mathbb{Z}_{(p)}$. Comme $P(z)$ est irréductible sur \mathbb{Q}_p et $P(z)$ est à coefficients dans $\mathbb{Z}_{(p)}$ alors le lemme de Hensel nous assure que $\bar{P}(z)$ est irréductible sur \mathbb{F}_p . Soient $L = \mathbb{Q}_p(\gamma)$ et $k = \mathbb{F}_p(\bar{\gamma})$. Comme $P(\gamma) = 0$ et $P(z)$ est irréductible sur \mathbb{Q}_p alors $[L : \mathbb{Q}_p] = \deg(P(z))$. De même, comme $\bar{P}(\bar{\gamma}) = 0$ et $\bar{P}(z)$ est irréductible sur \mathbb{F}_p alors $[k : \mathbb{F}_p] = \deg(\bar{P}(z))$. Mais, $\deg(P(z)) = \deg(\bar{P}(z))$ et ainsi, $[L : \mathbb{Q}_p] = \deg(P(z)) = [k : \mathbb{F}_p]$. Alors, d'après le petit théorème de Fermat, $\gamma^{p^{\deg(P(z))}} \equiv \gamma \pmod{p}$. Puisque L est un sous corps de K_p alors $\deg(P(z))$ divise h_3 et ainsi, $\gamma^{p^{h_3}} \equiv \gamma \pmod{p}$. Donc, pour tout entier $n \geq 1$, $\gamma^{p^{nh_3}} \equiv \gamma \pmod{p}$. Finalement, comme K est une extension galoisienne de \mathbb{Q} , on obtient que $h_2 = h_3r$, où r est un entier strictement positif. Ainsi, pour tout entier $m \geq 1$, $\gamma^{p^{mh_2}} \equiv \gamma \pmod{p}$. Finalement, on obtient que pour tout entier $m \geq 1$,

$$|\gamma^{p^{mh_2}} - \gamma|_p < \frac{1}{p} < |\pi_p|.$$

□

L'importance du troisième pas repose sur le fait que nous allons passer de la théorie des équations différentielles p -adiques à la théorie des équations différentielles classiques, et pour cela nous utiliserons le théorème 2.3.1. Dans un premier temps, nous étudions les disques singuliers réguliers de B . D'après le lemme 2.3.3, on obtient que B est E_p -équivalente à $\frac{pz^{p-1}}{z^p - \gamma_j} A_{\gamma_j}(z^p)$. De plus, d'après le choix de p , le corollaire 2.3.5 nous garantit que la matrice $A_{\gamma_j}(z^p)$ est non singulière dans le disque D_{γ_j} . Ainsi, la matrice $(z - \gamma_j) \left(\frac{1}{z^p - \gamma_j}\right) A_j(z^p)$ a comme singularités les racines p -ième de γ_j qui sont dans D_{γ_j} . Pour surmonter cette difficulté, nous considérerons la transformation $z \mapsto (z + \gamma_j)^p - \gamma_j$.

Dans l'étude de cette transformation nous devons reprendre la construction de $Frob_{z^p}$ faite dans la partie 1.4.3. De manière plus générale, pour $\omega \in E_p$ vérifiant

$$|\omega - z^{p^h}| < 1 \quad (2.20)$$

pour un certain h , nous construisons $Frob_\omega : E_p \rightarrow E_p$ comme suit. Nous définissons $Frob_\omega : \mathbb{C}_p(z) \rightarrow E_p$ donné par

$$Frob_\omega \left(\frac{\sum_i a_i z^i}{\sum_j b_j z^j} \right) = \frac{\sum_j Frob(a_j) \omega^j}{\sum_j Frob(b_j) \omega^j},$$

où $(\sum_i a_i z^i) / (\sum_j b_j z^j) \in \mathbb{C}_p(z)$. Remarquons que $\sum_j Frob(b_j) \omega^j \neq 0$ car d'après (2.20), ω est transcendant. Le Frobenius $Frob_\omega$ est continu car c'est une isométrie (voir lemme 2.3.9), il s'étend donc au corps des éléments analytiques E_p , noté encore $Frob_\omega : E_p \rightarrow E_p$. De plus, c'est à nouveau une isométrie. Soit A une matrice de taille n à coefficients E_p , on considère la matrice $F_\omega(A) := \frac{d}{dz}(\omega) A^{Frob_\omega}$, où A^{Frob_ω} est la matrice obtenue en appliquant $Frob_\omega$ à chaque entrée de A .

De la proposition 4.1.2 de [23] on sait que si $A \in \mathcal{M}_n(E_p)$ a norme inférieure ou égale à 1 alors le système $Ay = \frac{d}{dz}y$ a une base de solution dans l'anneau des séries à coefficients dans E_p qui convergent pour $|x| < |\pi_p|$, donc en analogie avec la proposition 4.7.3 de [23], nous obtenons la proposition suivante.

Proposition 2.3.8. *Soit $\omega \in E_p$ tel que $|\omega - z^{p^h}| < |\pi_p|$ et $A \in \mathcal{M}_n(E_p)$ de norme inférieure ou égale à 1. Alors $F_\omega(A)$ et $F_{z^{p^h}}(A)$ sont E_p -équivalentes.*

Nous allons utiliser la proposition 2.3.8 dans l'étape (i) du troisième pas afin de montrer que B est E_p -équivalente à $F_\omega\left(\frac{1}{z - \gamma_k} A_{\gamma_k}\right)$, avec $\omega = (z + \gamma_j)^{p^h} - \gamma_j$, où $Frob(\gamma_k) = \gamma_j$.

Un des points importants de la démonstration de la proposition 4.7.3 de [23] est que $Frob_{z^{p^h}}$ est une isométrie. Pour appliquer la proposition 2.3.8 nous devons montrer que $Frob_\omega$ est une isométrie. Nous démontrons cela dans le lemme suivant.

Lemme 2.3.9. *Soit h un entier strictement positif et $\omega \in E_p$ tels que $|\omega - z^{p^h}| < 1$. Alors, il existe un endomorphisme isométrique, $Frob_\omega : E_p \rightarrow E_p$ tel que $Frob_\omega(z) = \omega$. De plus, pour tout e dans E_p , on a*

$$\frac{d}{dz}(Frob_\omega(e)) = \frac{d}{dz}(\omega) Frob_\omega \left(\frac{d}{dz} e \right).$$

Démonstration. Soit $Frob : \mathbb{C}_p \rightarrow \mathbb{C}_p$ l'automorphisme de Frobenius choisi dans la remarque 1.4.1. On a $\bar{\omega} = \bar{z}^{p^h}$ et $|\omega| = 1$. Définissons $Frob_\omega : \mathbb{C}_p(z) \rightarrow E_p$ de la manière suivante. Étant donné $P(z) = \sum_{i=0}^n a_i z^i$ et $Q(z) = \sum_{j=0}^m b_j z^j \in \mathbb{C}_p[z]$, on pose

$$Frob_\omega \left(\frac{P}{Q} \right) = \frac{\sum_{i=0}^n Frob(a_i) \omega^i}{\sum_{j=0}^m Frob(b_j) \omega^j}.$$

Notons que $\sum_{j=0}^m \text{Frob}(b_j)\omega^j \neq 0$ car ω est transcendant sur K . Montrons que Frob_ω est une isométrie. Soient $l \in \{0, \dots, n\}$ et $k \in \{0, \dots, m\}$ tels que $|a_l| = |P|$ et $|b_k| = |Q|$. Alors $P = a_l P_1$ et $Q = b_k Q_1$ avec $P_1 = \sum_{i=0}^n c_i z^i$ où $c_i = \frac{a_i}{a_l}$, $Q_1 = \sum_{j=0}^m d_j z^j$ et $d_j = \frac{b_j}{b_k}$.

On pose $R = \frac{P_1}{Q_1}$.

Ainsi, on a $|P_1| = 1 = |Q_1|$, $|R| = 1$ et

$$\overline{\text{Frob}_\omega(R)} = \left(\frac{\sum_i c_i^p z^{ip^h}}{\sum_j d_j^p z^{jp^h}} \right) = \left(\frac{\sum_i c_i z^{ip^{h-1}}}{\sum_j d_j z^{jp^{h-1}}} \right)^p = \overline{R(z^{p^{h-1}})^p}. \quad (2.21)$$

On obtient que

$$|\text{Frob}_\omega(R) - (R(z^{p^{h-1}}))^p| < 1,$$

et comme $|R(z^{p^{h-1}})| = 1$, alors $|\text{Frob}_\omega(R)| = 1$ et $|\text{Frob}_\omega(P/Q)| = |P/Q|$.

Donc $\text{Frob}_\omega : \mathbb{C}_p(z) \rightarrow E_p$ est continue et isométrique. Elle peut se prolonger de manière unique au corps E_p en un endomorphisme isométrique. De la construction de Frob_ω et de la dérivation de la composée, il suit que pour toute fraction rationnelle $P/Q \in \mathbb{C}_p(z)$, on a

$$\frac{d}{dz}(\text{Frob}_\omega(P/Q)) = \frac{d}{dz}(\omega) \text{Frob}_\omega \left(\frac{d}{dz}(P/Q) \right).$$

Comme Frob_ω et $\frac{d}{dz}$ sont continues, on obtient que, pour tout $e \in E_p$, on a

$$\frac{d}{dz}(\text{Frob}_\omega(e)) = \frac{d}{dz}(\omega) \text{Frob}_\omega \left(\frac{d}{dz}e \right).$$

□

2.3.3 Démonstration des pas

Nous sommes maintenant prêts à démontrer le théorème 1.4.10.

Démonstration du premier pas. Soient $\gamma_1 = 0, \dots, \gamma_{r-1}, \gamma_r = \infty$ les points singuliers de L et A sa matrice compagnon. D'après le lemme 2.3.3, on a que γ_j est un point singulier régulier du système $\frac{d}{dz}y = Ay$. Ainsi, d'après le lemme 2.2.6, il existe $C_j \in \mathcal{M}_n(\mathbb{C})$ telle que $M(A, \gamma_j)$ est conjuguée à $\exp(2\pi i C_j)$, où, si λ, β sont deux valeurs propres différentes de C_j alors $\lambda - \beta \notin \mathbb{Z}$ et si α_{ij} est un exposant de $\frac{d}{dz}y = Ay$ en γ_j alors il existe un entier $m \in \mathbb{Z}$ tel que $\alpha + m$ est une valeur propre de C . Mais, toujours d'après le lemme 2.3.3, les exposants de $\frac{d}{dz}y = Ay$ en γ_j sont les exposants de L en γ_j . Ainsi, C_j satisfait aux conditions (a) et (b) du premier pas □

Remarque 2.3.10. D'après le lemme 2.3.3, nous pouvons réécrire le point (b) comme suit : l'ensemble des valeurs propres de $A_j(\gamma_j)$ et l'ensemble des valeurs propres de C_j sont égaux modulo \mathbb{Z} .

Soit \mathfrak{A} l'ensemble des nombres algébriques formé par les points $\gamma_2, \dots, \gamma_{r-1}$, les nombres algébriques $\gamma_i - \gamma_j$, $i \neq j$, et les dénominateurs des exposants des points $\gamma_1, \dots, \gamma_r$. Si $p \in \mathcal{S}$, alors les éléments de \mathfrak{A} ont tous une norme p -adique égale à 1. En effet, comme $p \in \mathcal{S}$ et $\gamma_2, \dots, \gamma_{r-1}$ sont les racines non nulles de $a_0(z)$ alors, d'après le théorème 6.1 de [42, Chap. I], leurs normes p -adique sont égales à 1. Le discriminant de $a_0(z)$ est donnée par $\prod_{i \neq j} (\gamma_i - \gamma_j)^2$. Si $p \in \mathcal{S}$, on a donc que $|\prod_{i \neq j} (\gamma_i - \gamma_j)^2|_p = 1$. De plus, comme la norme est ultramétrique, on obtient que $|\gamma_i - \gamma_j|_p \leq 1$ pour $i \neq j$. On en déduit donc que $|\gamma_i - \gamma_j|_p = 1$ pour $i \neq j$. Rappelons enfin que si $p \in \mathcal{S}$, alors $\|A\|_{\mathcal{G}, p} \leq 1$.

Désignons par $\alpha_{1,j}, \dots, \alpha_{n,j}$ les exposants de L en γ_j . Notons d le plus petit commun multiple des dénominateurs des $\alpha_{i,j}$ pour $1 \leq i \leq n$ et $1 \leq j \leq r$. Rappelons que $h_1 = \phi(d)$. On sait que si $p \in \mathcal{S}$, on a $|d|_p = 1$. Donc, p et d sont premiers entre eux et $p^{h_1} \equiv 1 \pmod{d}$. Ainsi, pour tout $p \in \mathcal{S}$, on obtient que

$$p^{h_1} \equiv 1 \pmod{d}.$$

Finalement, pour tout $i \in \{1, \dots, n\}$ et tout $j \in \{1, \dots, r\}$, il vient

$$p^{h_1} \alpha_{i,j} \equiv \alpha_{i,j} \pmod{\mathbb{Z}}.$$

D'après le lemme 2.3.6, on a

$$|\gamma_j^{p^h} - \gamma_j|_p < |\pi_p|, \quad (2.22)$$

pour tout $p \in \mathcal{S}$ et tout $j \in \{1, \dots, r-1\}$. Comme $h = h_1 h_2$, on obtient que

$$p^h \alpha_{i,j} \equiv \alpha_{i,j} \pmod{\mathbb{Z}}, \quad (2.23)$$

pour tout $i \in \{1, \dots, n\}$, tout $j \in \{1, \dots, r\}$ et tout $p \in \mathcal{S}$.

Démonstration du deuxième pas. Soit $p \in \mathcal{S}$ et montrons que les matrices $\exp(2\pi i C_j)$ et $\exp(2\pi i p^h C_j)$ sont conjuguées. Soit M la forme de Jordan de C_j , alors $C_j = U M U^{-1}$, où $U \in \mathrm{GL}_n(\mathbb{C})$. Soient $\lambda_{1,j}, \dots, \lambda_{r,j}$ les valeurs propres de C_j . Soit $J_{\lambda_{i,j}}$ un bloc de Jordan de M qui correspond à la valeur propre $\lambda_{i,j}$. Ainsi, $J_{\lambda_{i,j}} = \lambda_{i,j} I_{n_{\lambda_{i,j}}} + N_{\lambda_{i,j}}$, où $I_{n_{\lambda_{i,j}}}$ est la matrice identité de taille $n_{\lambda_{i,j}}$ et $N_{\lambda_{i,j}}$ est une matrice carrée nilpotente de taille $n_{\lambda_{i,j}}$. D'après le premier pas, $\lambda_{i,j} = \alpha + m$, où α est un exposant de L en γ_j et m un entier. Ainsi,

$$\exp(2\pi i J_{\lambda_{i,j}}) = \exp(2\pi i \alpha) \exp(2\pi i N_{\lambda_{i,j}}). \quad (2.24)$$

Les valeurs propres de $p^h C_j$ sont $p^h \lambda_{1,j}, \dots, p^h \lambda_{r,j}$. Puisque $p^h C_j = U(p^h M)U^{-1}$, alors $p^h M$ est constituée des blocs de Jordan de M multipliés par p^h . Ainsi, la matrice $p^h J_{\lambda_{i,j}} = p^h(\lambda_{i,j} I_{n_{\lambda_{i,j}}} + N_{\lambda_{i,j}})$ est un bloc de la matrice $p^h M$. Montrons que $p^h \lambda_{i,j} \equiv \alpha \pmod{\mathbb{Z}}$. Comme on l'a déjà dit $\lambda_{i,j} = \alpha + m$, où α est un exposant de L en γ_j et m un entier. Alors $p^h \lambda_{i,j} = p^h \alpha + p^h m$ et il suit de (2.23) que $p^h \alpha = \alpha + m'$, où m' est un entier. Donc, $p^h \lambda_{i,j} = \alpha + m' + p^h m$. Comme $m' + p^h m$ est un entier, on a $p^h \lambda_{i,j} \equiv \alpha \pmod{\mathbb{Z}}$. Par conséquent, on obtient que

$$\begin{aligned} \exp(p^h 2\pi i J_{\lambda_{i,j}}) &= \exp(2\pi i p^h \lambda_{i,j}) \exp(2\pi i p^h N_{\lambda_{i,j}}) \\ &= \exp(2\pi i \alpha) \exp(2\pi i N_{\lambda_{i,j}}). \end{aligned} \quad (2.25)$$

D'après (2.24) et (2.25), on a $\exp(2\pi i J_{\lambda_{i,j}}) = \exp(p^h 2\pi i J_{\lambda_{i,j}})$. Il suit donc que les matrices $\exp(2\pi i M)$ et $\exp(2\pi p^h M)$ sont conjuguées. Finalement, comme $\exp(2\pi i C_j) = U \exp(2\pi i M) U^{-1}$ et $\exp(2\pi i p^h C_j) = U \exp(2\pi i p^h M) U^{-1}$, la matrice $\exp(2\pi i C_j)$ et la matrice $\exp(2\pi i p^h C_j)$ sont conjuguées. \square

Démonstration du troisième pas.— Soit $p \in \mathcal{S}$ et soit $B = p^h z^{p^h-1} A(z^{p^h})$. Nous allons montrer que A et B sont E_p -équivalentes. Dans cette partie, nous verrons B comme une matrice à coefficients dans E_p . Pour chaque point singulier $\gamma_1 = 0, \dots, \gamma_{r-1}, \gamma_r = \infty$ de L , nous notons A_i la matrice construite dans le lemme 2.3.3 et correspondant au point γ_i .

Démonstration du point (i). Nous allons appliquer le théorème 2.3.1. Pour cela nous commençons par montrer que les seuls disques singuliers réguliers de B sont $D_{\gamma_1}, \dots, D_{\gamma_{r-1}}$ et D_∞ . Par construction de l'ensemble \mathfrak{A} , on a $|\gamma_j - \gamma_k|_p = 1$ pour $j \neq k$. Donc $\overline{\gamma_j} \neq \overline{\gamma_k}$ pour $j \neq k$ et $D_{\gamma_j} \cap D_{\gamma_k} = \emptyset$ pour $j \neq k$. Montrons dans un premier temps que si le disque D_α de centre α et de rayon 1 est singulier alors il existe $j \in \{1, \dots, r-1\}$ tel que $D_\alpha = D_{\gamma_j}$. Comme D_α est un disque singulier de B , il existe $t \in D_\alpha$ tel que t est une singularité de B , alors t^{p^h} est une singularité de A et il existe $i \in \{1, \dots, r-1\}$ tel que $t^{p^h} = \gamma_i$. D'après l'inégalité (2.22), on a $\overline{\gamma_i} = \overline{\gamma_i}^{p^h}$. Ainsi, on obtient que

$$\overline{t}^{p^h} = \overline{\gamma_i}^{p^h}.$$

Il suit que $\overline{t} = \overline{\gamma_i}$. Ainsi $|t - \gamma_i| < 1$ et comme la norme est ultramétrique, on obtient que

$$|\alpha - \gamma_i| = |\alpha - t + t - \gamma_i| < 1$$

et $D_\alpha = D_{\gamma_i}$.

Montrons dans un deuxième temps que, pour chaque $j \in \{1, \dots, r-1\}$, il existe une matrice B_j à coefficients dans E_p telle que $(z - \gamma_j)B_j$ est à coefficients dans $E(D_{\gamma_j})$ et B est E_p -équivalente à B_j . Cela impliquera que la matrice B est singulière régulière dans les disques D_{γ_j} . D'après la remarque qui suit la preuve du lemme 2.3.3, il existe $H_j \in \text{GL}_n(E_p)$ telle que

$$\frac{d}{dz}H_j = AH_j - H_j \frac{1}{z - \gamma_j} A_j.$$

Posons $Q_j := H_j(z^{p^h}) \in \text{GL}_n(E_p)$. On a

$$\frac{d}{dz}Q_j = \frac{d}{dz}(H_j)(z^{p^h})p^h z^{p^h-1}$$

et ainsi

$$\frac{d}{dz}Q_j = BQ_j - Q_j \left(\frac{p^h z^{p^h-1}}{z^{p^h} - \gamma_j} \right) A_j(z^{p^h}). \quad (2.26)$$

Alors la matrice B est E_p -équivalente à $\left(\frac{p^h z^{p^h-1}}{z^{p^h} - \gamma_j} \right) A_j(z^{p^h})$.

Notons que $Frob(\gamma_k) = \gamma_j$ car $Frob : \mathbb{C}_p \rightarrow \mathbb{C}_p$ fixe \mathbb{Q} et ainsi les singularités de $Frob(A) = A$ sont $\{Frob(\gamma_1), \dots, Frob(\gamma_{r-1}), \infty\} = \{\gamma_1, \dots, \gamma_{r-1}, \infty\}$. De plus, d'après (2.17), on a $Frob(A_k) = A_j$. Nous allons appliquer la proposition 2.3.8 à la matrice $\frac{1}{z - \gamma_k} A_k$, avec $\omega = [(z - \gamma_j)^{p^h} + \gamma_j]$. Montrons d'abord que $|\omega - z^{p^h}|_p < |\pi_p|_p$. Comme $\omega = (z - \gamma_j)^{p^h} + \gamma_j$, on a

$$\omega - z^{p^h} = (\gamma_j - \gamma_j^{p^h}) + \sum_{k=0}^{p^h-1} (-1)^k \binom{p^h}{k} z^{p^h-k} \gamma_j^k.$$

D'après le théorème de Lucas, on a $\binom{p^h}{k} \equiv 0 \pmod{p}$ pour $0 \leq k \leq p^h - 1$ et ainsi $|\binom{p^h}{k}|_p \leq |p|_p$. Or $\gamma_j \in \mathfrak{A}$, donc on a $|\gamma_j|_p = 1$ et

$$\left| \sum_{k=0}^{p^h-1} (-1)^k \binom{p^h}{k} z^{p^h-k} \gamma_j^k \right|_p \leq |p|_p < |\pi_p|_p.$$

L'inégalité (2.22) donne alors que $|\gamma_j^{p^h} - \gamma_j|_p < |\pi_p|_p$. Il suit

$$|\omega - z^{p^h}|_p < |\pi_p|_p < 1. \quad (2.27)$$

Comme $p \in \mathcal{S}$, on a $\|A\|_{\mathcal{G},p} \leq 1$ et $|\gamma_j|_p = 1$ donc le corollaire 2.3.5 entraîne que $\|\frac{1}{z-\gamma_j}A_j\|_{\mathcal{G},p} \leq 1$. Comme $Frob : \mathbb{C}_p \rightarrow \mathbb{C}_p$ est un automorphisme isométrique, on a $\|\frac{1}{z-\gamma_k}A_k\|_{\mathcal{G},p} \leq 1$.

Maintenant, la proposition 2.3.8 appliqué à $\frac{1}{z-\gamma_k}A_k$ implique que les matrices

$$\frac{d}{dz}(z^{p^h}) \left(\frac{1}{z-\gamma_k}A_k \right)^{Frob_{z^{p^h}}} \quad \text{et} \quad B_j = \frac{d}{dz}(\omega) \left(\frac{1}{z-\gamma_k}A_k \right)^{Frob_\omega}$$

sont E_p -équivalentes. D'après la construction de $Frob_{z^{p^h}}$, on a

$$\frac{d}{dz}(z^{p^h}) \left(\frac{1}{z-\gamma_k}A_k \right)^{Frob_{z^{p^h}}} = \frac{p^h z^{p^h-1}}{z^{p^h} - \gamma_j} A_j(z^{p^h}).$$

Notons que

$$\frac{d}{dz}(\omega) = p^h [(z - Frob(\gamma_j))^{p^h-1}],$$

et donc

$$B_j = \frac{p^h}{z-\gamma_j} A_j((z-\gamma_j)^{p^h} + \gamma_j). \quad (2.28)$$

D'après (2.26), il découle que la matrice B et B_j sont E_p -équivalentes. De plus, on a $(z-\gamma_j)B_j = p^h A_j((z-\gamma_j)^{p^h} + \gamma_j)$. Maintenant, si $y \in D_{\gamma_j}$ alors $(y-\gamma_j)^{p^h} + \gamma_j \in D_{\gamma_j}$ et comme A_j est non singulière dans le disque D_{γ_j} , on obtient que $(z-\gamma_j)B_j \in \mathcal{M}_n(E(D_{\gamma_j}))$.

Finalement, montrons que D_∞ est un disque singulier régulier de B . Pour cela, nous posons

$$B_r := \frac{d}{dz}(z^{p^h}) \left(\frac{1}{z^{p^h}} \right) A_r(z^{p^h}) \quad (2.29)$$

D'après le lemme 2.3.3, il existe $H_r \in \text{GL}_n(\mathbb{Q}(z))$ telle que

$$\frac{d}{dz}H_r = AH_r - H_r \frac{1}{z}A_r.$$

Posons $Q_r := H_r(z^{p^h})$, alors on a

$$\frac{d}{dz}Q_r = BQ_r - Q_r B_r.$$

Ainsi la matrice B est E_p -équivalente à B_r . D'après le lemme 2.3.3, A_r n'a pas de pôle à l'infini et le corollaire 2.3.5 donne que A_r n'a pas de singularité dans le disque D_∞ . Ainsi le disque D_∞ est non-singulier pour zB_r , autrement dit $zB_r \in \mathcal{M}_n(E(D_\infty))$. D'après le lemme 2.3.3, les matrices A et $\frac{1}{z-\gamma_j}A_j$ sont $\mathbb{Q}(z)(\gamma_j)$ -équivalentes. Puisque $\frac{1}{z-\gamma_j}A_j \in \mathcal{M}_n(\mathbb{Q}(z)(\gamma_j))$, à la suite de la remarque 2.2.7, il existe $W_j \in \mathcal{M}_n(\mathbb{C}_p(z))$ telle que W_j n'a pas de pôle en γ_j , $C_j = W_j(\gamma_j)$ et $\frac{1}{z-\gamma_j}A_j$ et $\frac{1}{z-\gamma_j}W_j$ sont $\mathbb{C}_p(z)$ -équivalentes. D'où, B_j et $R_j = \frac{p^h}{z-\gamma_j}W_j((z-\gamma_j)^{p^h} + \gamma_j)$ sont E_p -équivalentes. Montrons que W_j n'a pas de pôle dans le disque D_{γ_j} . En effet, soit $P(z)/Q(z) \in \mathbb{C}_p(z)$ une entrée de W_j . Écrivons $P(z) = \sum_{i=0}^r a_i(z-\gamma_j)^i$, $Q(z) = \sum_{l=0}^s b_l(z-\gamma_j)^l \in \mathbb{C}_p[z-\gamma_j]$. Soient $a \in \{a_0, \dots, a_r\}$ tel que $|a| = \max\{|a_0|, \dots, |a_r|\}$ et $P_1(z) = \frac{1}{a}P(z)$. Notons que $|P_1(z)|_{\mathcal{G}} = 1$. Soient $b \in \{b_0, \dots, b_s\}$ tel que $|b| = \max\{|b_0|, \dots, |b_s|\}$ et $Q_1(z) = \frac{1}{b}Q(z)$. Notons que $|Q_1(z)|_{\mathcal{G}} = 1$. Alors $\frac{P(z)}{Q(z)} = \frac{a}{b} \frac{P_1(z)}{Q_1(z)}$ et $|P_1(z)/Q_1(z)|_{\mathcal{G}} = 1$. Notons que les fractions rationnelles $\frac{P(z)}{Q(z)}$ et $\frac{P_1(z)}{Q_1(z)}$ ont les mêmes pôles. Par conséquent, γ_j n'est pas un pôle de $\frac{P_1(z)}{Q_1(z)}$. Alors, $\frac{P_1(z)}{Q_1(z)} =$

$\sum_{n \geq 0} c_n(z - \gamma_j)^n$. Puisque $|P_1(z)/Q_1(z)|_G = 1$ alors, pour tout $n \geq 0$, $|c_n| \leq 1$. Ainsi, la réduction de $\frac{P_1(z)}{Q_1(z)}$ est égale à $\sum_{n \geq 0} \bar{c}_n(z - \bar{\gamma}_j)^n$. D'où, $\bar{\gamma}_j$ n'est pas un pôle de la réduction de la fraction rationnelle $\frac{P_1(z)}{Q_1(z)}$. Par conséquent, la fraction rationnelle $\frac{P_1(z)}{Q_1(z)}$ n'a pas de pôle dans le disque D_{γ_j} et ainsi, la fraction rationnelle $\frac{P(z)}{Q(z)}$ n'a pas de pôle dans le disque D_{γ_j} . Par conséquent, la matrice W_j n'a pas de pôle dans le disque D_{γ_j} . Alors, $(z - \gamma_j)R_j \in \mathcal{M}_n(E(D_{\gamma_j}))$. Ainsi, d'après le théorème 2.3.1, la matrice B est E_p -équivalente à

$$G = \frac{\gamma_1 + m}{(z + m)(z - \gamma_1)} F_1 + \cdots + \frac{\gamma_{r-1} + m}{(z + m)(z - \gamma_{r-1})} F_{r-1} - \frac{1}{z + m} F_r,$$

où $F_j \in \mathcal{M}_n(\mathbb{C}_p)$ pour $j \in \{1, \dots, r\}$ telles que pour $j \in \{1, \dots, r-1\}$, F_j est semblable à $[(z - \gamma_j)R_j](\gamma_j)$, F_r est semblable à $[-zR_r](\infty)$ et $\sum F_i$ est une matrice diagonale à coefficients dans \mathbb{Z} . De plus, il suit que pour $j \in \{1, \dots, r-1\}$, $[(z - \gamma_j)R_j](\gamma_j) = p^h C_j$ et de (2.29) que $[-zR_r](\infty) = -p^h C_r$. Raison pour laquelle F_j est semblable à $p^h C_j$ pour $j \in \{1, \dots, r-1\}$ et F_r semblable à $-p^h C_r$. \square

Démonstration du point (ii). Rappelons que $\kappa : \mathbb{C}_p \rightarrow \mathbb{C}$ est un isomorphisme de corps. En appliquant l'isomorphisme κ , il vient

$$\begin{aligned} G^\kappa &= \frac{\kappa(\gamma_1) + m}{(z + m)(z - \kappa(\gamma_1))} F_1^\kappa + \cdots + \frac{\kappa(\gamma_{r-1}) + m}{(z + m)(z - \kappa(\gamma_{r-1}))} F_{r-1}^\kappa - \frac{1}{z + m} F_r^\kappa \\ &= -\frac{1}{z + m} \left(\sum_{j=1}^r F_j^\kappa \right) + \sum_{j=1}^{r-1} \frac{1}{z - \kappa(\gamma_j)} F_j^\kappa. \end{aligned}$$

Notons que la matrice G^κ est à coefficients dans $\mathbb{C}(z)$ et comme $F_j^\kappa \in \mathcal{M}_n(\mathbb{C})$, la matrice G^κ est fuchsienne, avec $\gamma_0 = -m$, $\kappa(\gamma_1), \dots, \kappa(\gamma_{r-1})$ et l'infini comme singularités.

Montrons que la matrice de monodromie de G^κ en γ_0 est l'identité. En effet, comme $\sum_{j=0}^r F_j$ est une matrice diagonale à coefficients dans \mathbb{Z} , la matrice $[(z + m)G^\kappa](-m) = -\sum_{j=1}^r F_j^\kappa$ est également diagonale et à coefficients entiers, puisque tout homomorphisme de corps de caractéristique zéro fixe \mathbb{Z} . Ainsi, les exposants de G^κ en γ_0 sont des entiers. Donc, d'après le lemme 2.2.6, il existe une matrice $C_0 \in \mathcal{M}_n(\mathbb{C})$ telle que la matrice de monodromie locale de G^κ en γ_0 est conjuguée à $\exp(2\pi i C_0)$ et telle que l'ensemble des valeurs propres de C_0 est réduit à un élément, $\{s\}$, où s est entier. Écrivons $C_0 = P(D + N)P^{-1}$, où $P \in \text{GL}_n(\mathbb{C})$, D est diagonale et N est nilpotente. Le théorème 8.6 de [42, Chap. III] nous assure que $TP(X^D X^N)P^{-1}$ est une solution de G^κ , où $T \in \text{GL}_n(\mathbb{C}((z + m)))$. Mais, d'après la remarque 2.3.2, il suit que G^κ a une base de solutions à coefficients dans $\mathbb{C}((z + m))$. Donc, $X^N = Id_n$. Ainsi, $C_0 = PDP^{-1}$, $D = sId_n$ et $\exp(2\pi i C_0)$ est conjuguée à Id_n . Par conséquent, la matrice de monodromie locale de G^κ en γ_0 est conjuguée à Id_n . Cela montre que la matrice de monodromie locale de G^κ en γ_0 est l'identité.

Notons que la matrice $(z - \kappa(\gamma_j))G^\kappa$ n'a pas de pôle en $\kappa(\gamma_j)$ et que $[(z - \kappa(\gamma_j))G^\kappa](\gamma_j) = F_j^\kappa$. Montrons que les valeurs propres de F_j^κ sont les valeurs propres de C_j multipliées par p^h . En effet, comme remarqué précédemment, F_j est semblable à $p^h C_j$. Écrivons $C_j = U M U^{-1}$, où M est la forme de Jordan de C_j et $U \in \text{GL}_n(\mathbb{C}_p)$. On note que $M \in \mathcal{M}_n(\mathbb{Q})$. En effet, d'après le lemme 2.3.3, les valeurs propres de $A_j(\gamma_j)$ sont les exposants de L en γ_j qui sont des nombres rationnels et donc la remarque 2.3.10 implique que les valeurs propres de C_j sont des nombres rationnels. Ainsi, F_j est semblable à $p^h M$ et, comme $p^h M \in \mathcal{M}_n(\mathbb{Q})$, on obtient que F_j^κ est semblable à $p^h M$. Notre affirmation en découle.

La remarque 2.3.10 entraîne que les valeurs propres de $p^h C_j$ sont de la forme $p^h \beta + s$, où s est un entier et β une valeur propre de $A_j(\gamma_j)$. Montrons que deux valeurs propres distinctes de $p^h C_j$ ne diffèrent pas d'un entier. En effet, supposons que $\lambda' - \beta' \in \mathbb{Z}$, où λ' et β' sont deux valeurs propres de $p^h C_j$. Alors $\lambda' = p^h \lambda$ et $\beta' = p^h \beta$, où λ et β sont deux valeurs propres de C_j . Alors, $p^h(\lambda - \beta) \in \mathbb{Z}$. D'après le premier pas, il existe des entiers m_λ et m_β , et λ_1 et β_1 des exposants de L en γ_j , tels que $\lambda = \lambda_1 + m_\lambda$ et $\beta = \beta_1 + m_\beta$. Alors $p^h(\lambda_1 - \beta_1) \in \mathbb{Z}$. Il découle de (2.23) que $p^h \lambda_1 \equiv \lambda_1 \pmod{\mathbb{Z}}$ et $p^h \beta_1 \equiv \beta_1 \pmod{\mathbb{Z}}$. Ainsi, $p^h(\lambda_1 - \beta_1) \equiv \lambda_1 - \beta_1 \pmod{\mathbb{Z}}$. Mais comme $p^h(\lambda_1 - \beta_1) \in \mathbb{Z}$, on obtient que $\lambda_1 - \beta_1 \in \mathbb{Z}$. On en déduit que $\lambda - \beta = (\lambda_1 - \beta_1) - (m_\beta - m_\lambda) \in \mathbb{Z}$. Par conséquent, d'après le premier pas, $\lambda = \beta$ et ainsi $\lambda' = \beta'$. Alors, on a :

(a') deux valeurs propres de $p^h C_j$ distinctes ne diffèrent pas d'un entier.

Ainsi, deux valeurs propres différentes de F_j^κ ne diffèrent pas d'un entier. D'après la proposition 3.12, le lemme 3.42 et le théorème 5.1 de [72], la matrice de monodromie locale de G^κ en $\kappa(\gamma_j)$, $M(G^\kappa, \kappa(\gamma_j))$, est conjuguée à $\exp(2\pi i F_j^\kappa)$. Comme F_j^κ est semblable à $p^h C_j$, on obtient que les matrices $\exp(2\pi i F_j^\kappa)$ et $\exp(2\pi i p^h C_j)$ sont conjuguées. Cela donne que $M(G^\kappa, \kappa(\gamma_j))$ est conjuguée à $\exp(2\pi i p^h C_j)$. D'après le deuxième pas, $\exp(2\pi i p^h C_j)$ et $\exp(2\pi i C_j)$ sont conjuguées et d'après le premier pas, les matrices $\exp(2\pi i p^h C_j)$ et $M(A, \gamma_j)$ sont conjuguées. Donc $M(G^\kappa, \kappa(\gamma_j))$ est conjuguée à $M(A, \gamma_j)$.

Notons que $\{\kappa(\gamma_1), \dots, \kappa(\gamma_{r-1})\} = \{\gamma_1, \dots, \gamma_{r-1}\}$. Comme le groupe de monodromie de A est rigide, les groupes de monodromie de A et G^κ sont conjugués. \square

Démonstration du point (iii). D'après ce qui précède, il existe $U \in \mathrm{GL}_n(\mathbb{C})$ telle que $M(A, \gamma_j) = UM(G^\kappa, \kappa(\gamma_j))U^{-1}$ pour $1 \leq j \leq r$. D'après la proposition 2.2.4, il existe $H_1 \in \mathrm{GL}_n(\mathbb{C}(z))$ telle que

$$\frac{d}{dz} H_1 = A H_1 - H_1 G^\kappa.$$

On pose $H = H_1^{\kappa^{-1}}$, ainsi $H \in \mathrm{GL}_n(\mathbb{C}_p(z)) \subset \mathrm{GL}_n(E_p)$ et comme $\frac{d}{dz}$ et κ^{-1} commutent, on a

$$\frac{d}{dz} H = A^{\kappa^{-1}} H - H G.$$

Remarquons que $A^{\kappa^{-1}} = A$, puisque A est une matrice à coefficients dans $\mathbb{Q}(z)$. Par conséquent, A et G sont E_p -équivalentes. D'après le point (ii), G est E_p -équivalente à B , alors par transitivité on obtient que A et B sont E_p -équivalentes. \square

Remarque 2.3.11. La preuve précédente montre en réalité que pour tout entier $h' \geq 1$ tel que pour tout $p \in \mathcal{S}$ les équations (2.22) et (2.23) sont vérifiées, alors L a une structure de Frobenius forte de période h' .

2.4 Démonstration du théorème 1.4.12 et 1.4.11

Dans cette partie, nous étudions les structures de Frobenius forte des opérateurs hypergéométriques généralisés. Nous démontrons notamment le théorème 1.4.12.

Considérons l'opérateur différentiel hypergéométrique défini par

$$\mathcal{H}(\underline{\alpha}, \underline{\beta}) : -z(\delta + \alpha_1) \cdots (\delta + \alpha_n)y + (\delta + \beta_1 - 1) \cdots (\delta + \beta_n - 1), \quad (2.30)$$

où $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n$ sont des nombres rationnels tels que $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$. Cet opérateur est fuchsien et a 1, 0 et l'infini comme seules singularités. Les exposants à l'infini sont $\alpha_1, \dots, \alpha_n$, les exposants en 0 sont $1 - \beta_1, \dots, 1 - \beta_n$, et les

exposants en 1 sont $0, 1, \dots, n-2, -1 + \sum(\beta_i - \alpha_i)$. Nous rappelons la définition suivante (voir [14]).

Définition 2.4.1. Supposons que $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{C}^*$ vérifient $a_i \neq b_j$ pour tout $i, j \in \{1, \dots, n\}$. Un groupe hypergéométrique associé aux paramètres $a_1, \dots, a_n, b_1, \dots, b_n$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ engendré par des matrices $h_0, h_1, h_\infty \in \mathrm{GL}_n(\mathbb{C})$ telles que h_1 est une réflexion et

$$\begin{aligned} h_\infty h_1 h_0 &= Id, \\ \det(z - h_\infty) &= \prod (z - a_i), \\ \det(z - h_0^{-1}) &= \prod (z - b_j). \end{aligned}$$

D'après un résultat de Levelt (voir le théorème 3.5 de [14]), si $a_i \neq b_j$ pour tout $i, j \in \{1, \dots, n\}$ alors le groupe hypergéométrique associé aux paramètres $a_1, \dots, a_n, b_1, \dots, b_n$ est rigide. D'autre part, il est connu que le groupe de monodromie de l'opérateur hypergéométrique $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ est un groupe hypergéométrique associé aux paramètres $a_i = \exp(2\pi i \alpha_i)$ et $b_i = \exp(2\pi i \beta_i)$ (voir [14]). Ainsi, le groupe de monodromie de (2.30) est rigide. Donc, grâce au théorème 1.4.10, $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ a une structure de Frobenius forte pour presque tout nombre premier p . En appliquant le théorème 1.4.10 on a le théorème suivant.

2.4.1 Démonstration du théorème 1.4.11

Démonstration. En développant l'équation (2.30), on obtient

$$(1-z)\delta^n + [S_{n,1}(\underline{\beta}-1) - zS_{n,1}(\underline{\alpha})]\delta^{n-1} + \dots + S_{n,n}(\underline{\beta}-1) - zS_{n,n}(\underline{\alpha}),$$

où $\underline{\beta}-1 = (\beta_1-1, \dots, \beta_n-1)$ et $S_{n,k} = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k}$.

En écrivant cette équation en fonction de l'opérateur $\frac{d}{dz}$, il vient

$$L_{\underline{\alpha}, \underline{\beta}} := a_0(z) \frac{d}{dz^n} y + a_1(z) \frac{d}{dz^{n-1}} y + \dots + a_n(z).$$

Soit A la matrice compagnon de ce nouvel opérateur. D'après l'équation (2.16), on a

$$\begin{aligned} (S_{n,n}(\underline{\beta}-1) - zS_{n,n}(\underline{\alpha}), \dots, S_{n,1}(\underline{\beta}-1) - zS_{n,1}(\underline{\alpha}), 1-z) G_{n+1}^{-1} \\ = (a_n(z), \dots, a_1(z), a_0(z)). \end{aligned}$$

Ainsi $a_0(z) = (1-z)z^n$ et le discriminant de $a_0(z)$ est 1. Dans ce cas, on obtient que $\mathfrak{A}_1 = \{1\}$, alors que l'ensemble \mathfrak{A}_2 est donné par les dénominateurs des α_i , des $1 - \beta_j$ et le dénominateur de $-1 + \sum_{i=1}^n (\beta_i - \alpha_i)$. Finalement $\mathfrak{A}_3 = \left\{ \frac{a_i(z)}{a_0(z)} \right\}_{1 \leq i \leq n}$. Comme $p \in \mathcal{S}$, on obtient que pour tout élément de $\mathfrak{A}_1 \cup \mathfrak{A}_2$ est de norme p -adique est égale à 1. A présent, montrons que, pour tout $p \in \mathcal{S}$, $\left| \frac{a_i(z)}{a_0(z)} \right|_{\mathcal{G}} \leq 1$. En effet, si $p \in \mathcal{S}$, alors

$$\left\| (S_{n,n}(\underline{\beta}-1) - zS_{n,n}(\underline{\alpha}), \dots, S_{n,1}(\underline{\beta}-1) - zS_{n,1}(\underline{\alpha}), 1-z) \right\|_{\mathcal{G},p} \leq 1.$$

On vérifie aisément que, pour tout nombre premier p , $\|G_{n+1}^{-1}\|_{\mathcal{G},p} \leq 1$. En particulier, il en est de même pour $p \in \mathcal{S}$. Ainsi, la norme de Gauss du vecteur $(a_n(z), \dots, a_1(z), a_0(z))$ est inférieure ou égale à 1 pour tout $p \in \mathcal{S}$. D'autre part, pour tout $p \in \mathcal{S}$, $|a_0(z)|_{\mathcal{G}} = 1$. On obtient donc que $\left| \frac{a_i(z)}{a_0(z)} \right|_{\mathcal{G}} \leq 1$, pour tout $p \in \mathcal{S}$.

Finalement, comme $|\alpha_i|_p, |\beta_j|_p \leq 1$ pour tout $i, j \in \{1, \dots, n\}$, alors p ne divise pas $d_{\alpha, \beta}$. Ainsi, pour tout $i, j \in \{1, \dots, n\}$, on a

$$p^{\varphi(d_{\alpha, \beta})} \equiv 1 \pmod{d_{\alpha, \beta}}$$

$$p^{\varphi(d_{\alpha, \beta})} \equiv 1 \pmod{d_{\alpha, \beta}}$$

et donc

$$p^{\varphi(d_{\alpha, \beta})} \alpha_i \equiv \alpha_i \pmod{\mathbb{Z}}$$

$$p^{\varphi(d_{\alpha, \beta})} \beta_j \equiv \beta_j \pmod{\mathbb{Z}}.$$

Il suit que $p^{\varphi(d_{\alpha, \beta})} \alpha_i \equiv \alpha_i \pmod{\mathbb{Z}}$, $p^{\varphi(d_{\alpha, \beta})} (1 - \beta_j) \equiv 1 - \beta_j \pmod{\mathbb{Z}}$ et $p^{\varphi(d_{\alpha, \beta})} (-1 + \sum_{i=1}^n (\beta_i - \alpha_i)) \equiv -1 + \sum_{i=1}^n (\beta_i - \alpha_i) \pmod{\mathbb{Z}}$. De plus, ici les zéros de $a_0(z)$ sont $\gamma_1 = 0$ et $\gamma_2 = 1$, d'où $|\gamma_i^{p^{\varphi(d_{\alpha, \beta})}} - \gamma_i| = 0 < |\pi_p|$ pour $i \in \{1, 2\}$. Donc, d'après la remarque 2.3.11, pour tout $p \in \mathcal{S}$ l'opérateur différentiel $L_{\underline{\alpha}, \underline{\beta}}$ possède une structure de Frobenius forte de période $\varphi(d_{\alpha, \beta})$. Ainsi, pour tout $p \in \mathcal{S}$, l'opérateur différentiel $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ a une structure de Frobenius forte de période $\varphi(d_{\alpha, \beta})$. \square

2.4.2 Démonstration du théorème 1.4.12

Démonstration. Soit $p \in \mathcal{S}$. Alors p ne divise pas $d_{\alpha, \beta}$, de sorte que $|\alpha_i|_p, |\beta_j|_p \leq 1$ pour $i, j \in \{1, \dots, n\}$. D'après le théorème 1.4.11, on obtient que

$$-z(\delta + \alpha_1) \cdots (\delta + \alpha_n) + (\delta + \beta_1 - 1) \cdots (\delta + \beta_n - 1)$$

possède une structure de Frobenius forte pour p de période h . Par hypothèse, on a également ${}_n F_{n-1}(\underline{\alpha}, \underline{\beta}, z) \in \mathbb{Z}_{(p)}[[z]]$. Le théorème 1.4.6 implique donc que la réduction de ${}_n F_{n-1}(\underline{\alpha}, \underline{\beta}, z)$ modulo p est algébrique sur $\mathbb{F}_p(z)$ de degré majoré par $p^{n^2 h}$. Enfin, la démonstration du théorème 1.4.11 montre que l'on peut prendre $h = \phi(d_{\alpha, \beta})$. \square

Chapitre 3

Monodromie unipotente maximale, congruences « à la Lucas » et indépendance algébrique

Ce chapitre est organisé de la manière suivante. Dans la partie 3.1, nous décrivons la stratégie que employée pour démontrer le théorème 1.7.6. Dans la partie 3.2, nous rappelons la définition d'opérateur différentiel fuchsien et la notion d'opérateur différentiel MOM en zéro. Dans la partie 3.3, nous illustrons le deuxième point théorème 1.7.6 en montrant que la série 210 de [9] appartient à $\mathcal{L}(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers. La pertinence de cet exemple provient du fait que les méthodes combinatoires et les techniques développées dans [2, section 8] ne parviennent pas encore à montrer que cette série appartient à $\mathcal{L}(\mathcal{S})$. La preuve du théorème 1.7.6 repose sur le lemme 3.4.2. Notre approche de la démonstration du lemme 3.4.2 est fondée sur la théorie des équations différentielles p -adiques. Dans la partie 3.4, nous démontrons le théorème 1.7.6, en admettant le lemme 3.4.2. Celui-ci est prouvé ultérieurement dans la partie 3.5. La partie 3.6 est consacrée à montrer que la série hypergéométrique $h_2(z)$ appartient à $\mathcal{L}^2(\mathcal{S}) \setminus \mathcal{L}(\mathcal{S})$, quel que soit l'ensemble infini \mathcal{S} de nombres premiers. Dans la partie 3.7, nous appliquons le théorème 1.7.6 à l'étude des solutions d'opérateurs différentiels de type Calabi-Yau. Enfin, la partie 3.8 est dédiée à l'étude de l'indépendance algébrique de certaines séries de $\mathcal{L}^2(\mathcal{S})$ et nous démontrerons le théorème 1.7.8.

3.1 Stratégie de la démonstration du théorème 1.7.6

À présent, nous allons expliquer la stratégie que nous allons utiliser pour démontrer le théorème 1.7.6.

Nous esquissons d'abord comment obtenir les équations de la forme (1.16) sous les hypothèses du théorème 1.7.6. Les équations de la forme (1.16) sont dites équations « à la Lucas ».

Soient $f(z) \in \mathcal{F}(\mathcal{S})$ et \mathcal{D} un opérateur différentiel à coefficients dans $\mathbb{Q}(z)$ tel que \mathcal{D} est MUM en zéro et $f(z)$ annule \mathcal{D} . Soient $p \in \mathcal{S}$ tel que l'on peut réduire \mathcal{D} modulo p et \mathcal{D}_p la réduction de \mathcal{D} modulo p . L'hypothèse que \mathcal{D} est MUM en zéro va entraîner que le $\mathbb{F}_p((z^p))$ -espace vectoriel formé des solutions de \mathcal{D}_p qui appartiennent à $\mathbb{F}_p((z))$ est de dimension 1. Remarquons que $f|_p(z)$ est une solution de \mathcal{D}_p non nulle appartenant

à $\mathbb{F}_p((z))$. Comme $f|_p$ est non nulle, la théorie des équations différentielles sur les corps finis va garantir que \mathcal{D}_p a aussi une solution $A_p(z)$ non nulle appartenant à $\mathbb{F}_p[[z]]$. Par conséquent, il existe $g(z^p) \in \mathbb{F}_p((z^p))$, non nulle, telle que

$$f|_p(z) = A_p(z)g(z^p) \quad (3.1)$$

Puisque $f(0) = 1$ alors $g(z) \in \mathbb{F}_p[[z]]$. Rappelons que l'opérateur Λ_p a la propriété suivante : pour tout $h(z), t(z) \in \mathbb{F}_p[[z]]$, on a

$$\Lambda_p(t(z)h(z^p)) = \Lambda_p(t(z))h(z). \quad (3.2)$$

Les égalités (3.1) et (3.2) impliquent que $\Lambda_p(f|_p(z)) = \Lambda_p(A_p(z))g(z)$. Ainsi

$$f|_p(z) = A_1(z)\Lambda_p(f|_p)(z^p) \quad \text{où} \quad A_1(z) = \frac{A_p(z)}{\Lambda_p(A_p)(z^p)}. \quad (3.3)$$

Si $\Lambda_p(f|_p)(z^p) = f|_p(z^p)$, alors $f|_p(z) = A_1(z)f|_p(z^p)$.

Remarquons que jusqu'ici nous n'avons pas utilisé l'hypothèse que $f(z)$ annule un opérateur différentiel muni d'une structure de Frobenius forte pour p . Cette hypothèse est utilisée pour étudier le cas où $\Lambda_p(f|_p)(z^p) \neq f|_p(z^p)$. En effet, l'hypothèse que $f(z)$ annule un opérateur muni d'une structure de Frobenius forte pour p ainsi que l'opérateur \mathcal{D} , peut être utilisée pour montrer que, pour tout entier $k \geq 1$, la série $\Lambda_p^k(f|_p(z))$ annule un opérateur $\mathcal{D}_{k,p}$ non nul à coefficients dans $\mathbb{F}_p(z)$ tel que le $\mathbb{F}_p((z^p))$ -espace vectoriel formé des solutions de $\mathcal{D}_{k,p}$ qui appartiennent à $\mathbb{F}_p((z))$ est de dimension 1.

En raisonnant comme précédemment, on obtient l'existence de $g_k(z^p) \in \mathbb{F}_p((z^p))$, non nulle, telle que $\Lambda_p^k(f|_p(z)) = A_{k,p}(z)g_k(z^p)$. Comme $\Lambda_p^k(f|_p(0)) = 1$, on a $g_k(z) \in \mathbb{F}_p[[z]]$. Il découle alors de l'égalité (3.2) que $\Lambda_p^{k+1}(f|_p(z)) = \Lambda_p(A_{k,p}(z))g_k(z)$. Par conséquent, pour tout entier $k \geq 1$, on a

$$\Lambda_p^k(f|_p(z)) = A_{k+1}(z)\Lambda_p^{k+1}(f|_p)(z^p) \quad \text{où} \quad A_{k+1}(z) = \frac{A_{k,p}(z)}{\Lambda_p(A_p)(z^p)}. \quad (3.4)$$

Pour chaque $k \geq 1$, on pose $B_k(z) = A_1(z)A_2(z^p) \cdots A_k(z^{p^{k-1}})$. Il découle donc des égalités (3.3) et (3.4) que, pour tout entier $k \geq 1$,

$$f|_p(z) = B_k(z)\Lambda_p^k(f|_p)(z^{p^k}). \quad (3.5)$$

Si $f|_p(z) = \Lambda_p^k(f|_p(z))$ pour un certain entier $k \geq 1$, alors $f|_p(z) = B_k(z)f|_p(z^{p^k})$.

Dans le cas où $f|_p(z) \neq \Lambda_p^k(f|_p)(z)$ pour tout entier $k \geq 1$, nous utilisons à nouveau l'hypothèse que $f(z)$ annule un opérateur muni d'une structure de Frobenius forte pour p ainsi que l'opérateur \mathcal{D} pour montrer que, pour toute couple $(k, m) \in \mathbb{Z}_{\geq 0}^2$, il existe une fraction rationnelle $B_{k,m}(z) \in \mathbb{F}_p(z)$ telle que

$$\Lambda_p^m(f|_p)(z) = B_{k,m}(z)\Lambda_p^{k+m}(f|_p)(z^{p^k}).$$

Remarquons que lorsque $m = 0$ nous récupérons l'égalité (3.5). Comme $f(z)$ annule un opérateur muni d'une structure de Frobenius forte, le théorème 1.4.6 implique que la série $f|_p(z)$ est algébrique sur $\mathbb{F}_p(z)$. Les théorèmes D et E entraînent alors qu'il existe un entier $l > 0$ tel que, $\Lambda_p^l(f|_p)(z) = \Lambda_p^{2l}(f|_p)(z)$. En particulier, on a

$$\Lambda_p^l(f|_p)(z) = B_{l,l}(z)\Lambda_p^l(f|_p)(z^{p^l}) \quad \text{et} \quad B_{l,l}(z) = \frac{\Lambda_p^l(f|_p)(z)}{\Lambda_p^l(f|_p)(z^{p^l})}.$$

L'égalité (3.5) implique que $f_{|p}(z) = B_l(z)\Lambda_p^l(f_{|p})(z^{p^l})$ et

$$\frac{1}{B_l(z)} = \frac{\Lambda_p^l(f_{|p})(z^{p^l})}{f_{|p}(z)}.$$

Remarquons que

$$\frac{B_{l,l}(z)}{B_l(z)} = \frac{\Lambda_p^l(f_{|p})(z)}{f_{|p}(z)}.$$

Ainsi,

$$\begin{aligned} f_{|p}(z) &= B_l(z)\Lambda_p^l(f_{|p})(z^{p^l}) \\ &= B_l(z)\frac{\Lambda_p^l(f_{|p})(z^{p^l})}{f_{|p}(z^{p^l})}f_{|p}(z^{p^l}) \\ &= B_l(z)\frac{B_{l,l}(z^{p^l})}{B_l(z^{p^l})}f_{|p}(z^{p^l}). \end{aligned}$$

Finalement, nous montrons que, pour tout entier $k \geq 1$, la hauteur de $B_k(z)$ est inférieure ou égale à Cp^k et que la hauteur $B_k(z)\frac{B_{k,k}(z^{p^k})}{B_k(z^{p^k})}$ est inférieure ou égale à Cp^{2k} , où $C \leq 2nr$, n est l'ordre de \mathcal{D} et r est le nombre de singularités de \mathcal{D} dans $\overline{\mathbb{Q}}$.

Exemple 3.1.1. *Soit*

$$\mathbf{a}_1(z) = \sum_{n \geq 0} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \right) z^n$$

Comme nous l'avons déjà mentionné, grâce à [49], on a que $\mathbf{a}_1(z) \in \mathcal{L}(\mathcal{P})$, où \mathcal{P} est l'ensemble des nombres premiers. Maintenant nous allons montrer qu'en appliquant la stratégie précédente nous obtenons aussi ce résultat. La série $\mathbf{a}_1(z)$ annule l'opérateur différentiel

$$\mathcal{D} : (1 - 34z + z^2)z^2 \frac{dz}{dz^3} + (3 - 153z + 6z^2)z \frac{d}{dz^2} + (1 - 112z + 7z^2) \frac{d}{dz} - 5 + z.$$

Cet opérateur est MUM en zéro car ses exposants en zéro sont tous égaux à zéro. Soit p un nombre premier, le polynôme $A_p(z) = \sum_{n=0}^{p-1} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \pmod{p} \right) z^n$ annule \mathcal{D}_p . Il découle donc de l'égalité (3.3) que, pour tout nombre premier p ,

$$\mathbf{a}_{1|p}(z) = A_p(z)\Lambda_p(\mathbf{a}_1)(z^p).$$

Maintenant montrons que, pour tout nombre premier p , $\Lambda_p(\mathbf{a}_{1|p}(z)) = \mathbf{a}_{1|p}(z)$, c'est-à-dire il faut montrer que pour tout entier $n \geq 0$ et tout nombre premier p ,

$$\sum_{k=0}^{np} \binom{np}{k}^2 \binom{np+k}{k}^2 \equiv \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \pmod{p}.$$

Soit $k \in \{0, 1, \dots, np\}$. Alors $k = lp + s$, où $s \in \{0, \dots, p-1\}$ et $l \in \{0, 1, \dots, n\}$. Ainsi, d'après le théorème de Lucas

$$\binom{np}{lp+s} \equiv \binom{n}{l} \binom{0}{s} \pmod{p}.$$

Par conséquent,

$$\binom{np}{lp+s} \equiv \begin{cases} \binom{n}{l} \pmod p & \text{si } s = 0 \\ 0 \pmod p & \text{si } s > 0 \end{cases}$$

Alors,

$$\sum_{k=0}^{np} \binom{np}{k}^2 \binom{np+k}{k}^2 \equiv \sum_{l=0}^n \binom{n}{l}^2 \binom{np+lp}{lp}^2 \pmod p.$$

Mais d'après le théorème de Lucas

$$\binom{np+lp}{lp}^2 \equiv \binom{n+l}{l}^2 \pmod p,$$

d'où

$$\sum_{k=0}^{np} \binom{np}{k}^2 \binom{np+k}{k}^2 \equiv \sum_{l=0}^n \binom{n}{l}^2 \binom{n+l}{l}^2 \pmod p.$$

Par conséquent, $\Lambda_p(\mathbf{a}_{1|p}(z)) = \mathbf{a}_{1|p}(z)$. Ainsi, l'équation 3.3 entraîne que

$$\mathbf{a}_1(z) = A_p(z)\mathbf{a}_r(z^p).$$

L'intérêt de cet exemple est donné par le fait qu'on n'utilise pas la structure de Frobenius forte. Par contre, dans l'exemple suivant nous aurons besoin d'utiliser la structure de Frobenius forte.

Exemple 3.1.2. Pour chaque entier $r \geq 1$, soit $\mathfrak{h}_r(z) = \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n}^r z^n$. La série $\mathfrak{h}_r(z)$ annule l'opérateur différentiel

$$\mathcal{L}_r = \delta^r - 4^r z(\delta - 1/2)(\delta + 1/2)^{r-1}.$$

Cet opérateur est MUM en zéro et pour tout nombre premier p différent de 2 nous pouvons réduire \mathcal{L} modulo p , nous notons par $\mathcal{L}_{r,p}$ sa réduction modulo p . De plus, comme nous le verrons dans le chapitre 3, la série $\mathfrak{h}_r(z)$ appartient à $\mathbb{Z}[[z]]$. Il suit du théorème de Lucas que, pour tout nombre premier p différent de 2 et tout entier $k \geq 1$,

$$\Lambda_p^k(\mathfrak{h}_{r|p}) = \sum_{n \geq 0} \left(\frac{-1}{2np^k-1} \binom{2np^k}{np^k} \pmod p \right) z^n = \sum_{n \geq 0} \left(\binom{2n}{n} \pmod p \right) z^n \neq \mathfrak{h}(z)_{r|p}.$$

Par conséquent, pour montrer que $\mathfrak{h}_{r|p}$ vérifie une équation « à la Lucas », il suffit de montrer que \mathfrak{h}_r annule un opérateur muni d'une structure de Frobenius forte pour tout nombre premier différent de 2. D'après le théorème 1.4.11, c'est bien le cas.

3.2 Opérateurs différentiels

Dans cette partie nous allons rappeler quelques notions classiques des opérateurs différentiels, la lettre K désigne un corps quelconque. Un opérateur différentiel à coefficients dans $K(z)$ est un objet de la forme

$$L := \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} + a_n(z), \quad (3.6)$$

où les $a_i(z)$ appartiennent à $K(z)$. L'ordre de L est n . Un point α dans la clôture algébrique de K est un point *singulier* de L s'il existe $i \in \{1, \dots, n\}$ tel que α est un pôle pour $a_i(z)$.

Nous disons que α est un point *singulier régulier* de L si α est un point singulier de L et, pour tout $i \in \{1, \dots, n\}$, $\tilde{a}_i(z) := (z - \alpha)^i a_i(z)$ n'a pas de pôle en α . Soit L_∞ l'opérateur différentiel obtenu après avoir appliqué le changement de variable $z \mapsto 1/z$ à L . Nous disons que l'infini est un point *singulier régulier* de L si zéro est un point singulier régulier de L_∞ . Remarquons que si, pour chaque $i \in \{1, \dots, n\}$, nous écrivons $a_i(z) = \frac{b_{i,1}(z)}{b_{i,2}(z)}$, où $b_{i,1}(z)$ et $b_{i,2}(z)$ appartiennent à $K[z]$ et sont premiers entre eux alors, l'infini est un point singulier régulier de L si et seulement si, pour tout $i \in \{1, \dots, n\}$, $\deg(b_{i,1}(z)) \leq \deg(b_{i,2}(z)) - i$.

Nous dirons que α est une *singularité à distance finie* de L si α est un point singulier de L et α n'est pas l'infini. Soit $\delta = z \frac{d}{dz}$ l'opérateur d'Euler. Nous réécrivons $z^n L$ en fonction de δ et obtenons

$$L_\delta := \delta^n + b_1(z)\delta^{n-1} + \dots + b_{n-1}(z)\delta + b_n(z),$$

où les $b_i(z)$ appartiennent à $K(z)$. Comme nous le verrons dans la proposition suivante, si zéro est un point singulier régulier de L alors pour tout $i \in \{1, \dots, n\}$, $b_i(z) \in K[[z]]$. Ainsi, lorsque zéro est un point singulier régulier de L nous définissons les *exposants* en zéro de L comme les racines du polynôme

$$x^n + b_1(0)x^{n-1} + \dots + b_{n-1}(0)x + b_n(0).$$

Ce polynôme est connu comme le polynôme *indiciel* en zéro de L . Si l'infini est un point singulier régulier de L , nous définissons les *exposants* en l'infini de L comme les exposants en zéro de L_∞ .

Proposition 3.2.1. *Soient K un corps quelconque et L défini comme en (3.6). Le point zéro est un point singulier régulier de L si et seulement si, pour tout $i \in \{1, \dots, n\}$, $b_i(z)$ appartient à $K[[z]]$.*

Nous montrerons cette proposition à la fin de cette partie. Lorsque $K = \mathbb{C}$, ce résultat est le critère de Fuchs dont on trouve une démonstration dans [72, corollaire 5.5]. Maintenant rappelons la définition d'opérateur fuchsien.

Définition 3.2.2 (Opérateur fuchsien). Soient K un corps quelconque et L défini comme en (3.6). L'opérateur L est *fuchsien* si l'infini est un point singulier régulier de L et si toutes les singularités à distance finie de L sont des points singuliers réguliers de L . Par abus de langage nous dirons que l'opérateur différentiel L_δ est fuchsien si, lorsque nous réécrivons l'opérateur $\frac{1}{z^n} L_\delta$ en fonction de d/dz , il est fuchsien.

Dans la suite de l'article, nous utiliserons à plusieurs reprises la notion de MOM en zéro, notion algébrique définie ci-dessous qui généralise la notion de monodromie unipotente maximale lorsque $K = \mathbb{C}$.

Définition 3.2.3 (Opérateur MOM en zéro). Soient K un corps quelconque et L défini comme en (3.6). L'opérateur différentiel L est MOM¹ en zéro si : L est fuchsien, zéro est un point singulier régulier de L et tous les exposants en zéro de L sont égaux à zéro.

Lorsque $K = \mathbb{C}$, à chaque point singulier α de L est associé une matrice qui s'appelle la matrice de monodromie locale en α , cette matrice est unique à conjugaison près et sa construction dépend de la géométrie euclidienne de \mathbb{C} . Le lecteur trouvera une construction de cette matrice dans [72, Chap. 5]. Supposons que zéro est un point singulier régulier de L . La matrice de monodromie locale en zéro est unipotente si et seulement si toutes ses valeurs propres sont égales à 1. Mais il découle de la proposition 3.12 et du théorème 5.1 de

1. L'abréviation MOM en anglais signifie maximal order multiplicity.

[72] que toutes les valeurs propres de la matrice de monodromie locale en zéro sont égales à 1 si et seulement si tous les exposants en zéro de L sont égaux à zéro. Ainsi, lorsque $K = \mathbb{C}$, l'opérateur L est MOM en zéro si L est fuchsien, zéro est un point singulier de L et la matrice de monodromie locale en zéro est unipotente.

Démonstration de la proposition 3.2.1. Remarquons d'abord que pour tout entier j strictement positif, $z^j \frac{d^j}{dz^j} = \delta(\delta+1) \cdots (\delta+j-1)$. Ainsi, pour chaque entier j strictement positif, il existe $c_{1,j}, c_{2,j}, \dots, c_{j-1,j} \in K$ tels que $\frac{d^j}{dz^j} = \frac{c_{1,j}}{z^j} \delta + \frac{c_{2,j}}{z^j} \delta^2 + \dots + \frac{c_{j-1,j}}{z^j} \delta^{j-1} + \frac{1}{z^j} \delta^j$. Donc, pour chaque entier j strictement positif, nous posons

$$G_j = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \frac{1}{z} & 0 & \dots & 0 \\ 0 & \frac{c_{1,2}}{z^2} & \frac{1}{z^2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \frac{c_{1,j-1}}{z^{j-1}} & \frac{c_{2,j-1}}{z^{j-1}} & \dots & \frac{1}{z^{j-1}} \end{pmatrix} \in \mathrm{GL}_j(K[1/z])$$

la matrice exprimant $\{1, \dots, \frac{d^{j-1}}{dz^{j-1}}\}$ en fonction de $\{1, \delta, \dots, \delta^{j-1}\}$. Rappelons que par définition, l'opérateur différentiel L_δ est obtenu après avoir réécrit l'opérateur $z^n L$ en fonction de δ . Par conséquent, on a

$$(b_n(z), \dots, b_1(z), 1) = (a_n(z), \dots, a_1(z), 1) z^n G_{n+1}. \quad (3.7)$$

Il découle de l'égalité (3.7) que pour tout $i \in \{1, \dots, n\}$,

$$b_i(z) = z^i a_i(z) + c_{n-i, n-i+1} z^{i-1} a_{i-1}(z) + \dots + c_{n-i, n-1} z a_1(z) + c_{n-i, n}. \quad (3.8)$$

Supposons que zéro est un point singulier régulier de L . Donc, pour tout $i \in \{1, \dots, n\}$, $z^i a_i(z) \in K(z) \cap K[[z]]$ et par conséquent, d'après l'égalité (3.8), pour tout $i \in \{1, \dots, n\}$, $b_i(z) \in K(z) \cap K[[z]]$.

Maintenant supposons que pour tout $i \in \{1, \dots, n\}$, $b_i(z) \in K(z) \cap K[[z]]$. Montrons par récurrence sur i que $z^i a_i(z) \in K[[z]]$. À la suite de (3.8), on a que $z a_1(z) = b_1(z) - c_{n-1, n}$. Puisque $b_1(z) \in K[[z]]$ alors $z a_1(z) \in K[[z]]$. Supposons que $z a_1(z), \dots, z^{i-1} a_{i-1}(z) \in K[[z]]$. L'égalité (3.8) entraîne que,

$$z^i a_i(z) = b_i(z) - c_{n-i, n-i+1} z^{i-1} a_{i-1}(z) - \dots - c_{n-i, n-1} z a_1(z) - c_{n-i, n}.$$

Puisque $b_i(z) \in K[[z]]$ et par l'hypothèse de récurrence, $z a_1(z), \dots, z^{i-1} a_{i-1}(z)$ appartiennent à $K[[z]]$ alors $z^i a_i(z) \in K[[z]]$. Ainsi, pour tout $i \in \{1, \dots, n\}$, $z^i a_i(z)$ n'as pas de pôle en zéro et par conséquent, zéro est un point singulier régulier de L . \square

3.3 Un premier exemple

Dans la partie 1.7.1 nous avons montré que la série $f_4(z)$ appartient à $\mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{J} est un ensemble infini de nombres premiers. L'importance de cet fait est donnée par le fait que les méthodes combinatoires et les techniques développées dans [2, section 8] ne semblent pas suffire à montrer que cette série appartient à $\mathcal{L}(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers. Nous rappelons ici la stratégie que nous avons utilisée pour démontrer que $f_4(z) \in \mathcal{L}(\mathcal{P} \setminus \mathcal{J})$. Rappelons que la série en question est donnée par l'expression suivante

$$f_4(z) = \sum_{j \geq 0} \left(\binom{2j}{j} \left(\sum_{k=0}^{2j} (-1)^k \binom{2j}{k}^4 \right) \right) z^j \in 1 + z\mathbb{Z}[[z]].$$

Nous avons d'abord démontré, en utilisant le théorème de Lucas, que pour tout nombre premier différent de 2, $\Lambda_p(f_4(z))|_p = f(z)_{4|p}(z)$. Puis, le théorème 3.5 de [17] nous assure que la série $f_4(z)$ est la diagonale d'une fraction rationnelle, alors, d'après [25], $f_4(z)$ annule un opérateur différentiel $\mathcal{H} \in \mathbb{Q}(z)[d/dz]$ muni d'une structure de Frobenius forte pour presque tout nombre premier p . Finalement la série $f_4(z)$ est la série 210 de de la liste donnée dans [9] et par conséquent, elle annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ qui est MUM en zéro. Alors, on est en mesure d'appliquer le théorème 1.7.6 et ainsi $f_4(z) \in \mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{J} est un ensemble fini de nombres premiers. Nous rappelons cette stratégie car on peut l'appliquer pour montrer que de nombreuses séries qui apparaissent dans [9] appartiennent à $\mathcal{L}(\mathcal{S})$, où $\mathcal{P} \setminus \mathcal{S}$ est fini, voir par exemple la partie 3.7.

3.4 Démonstration du théorème 1.7.6

La preuve du théorème 1.7.6 repose sur le lemme 3.4.2. Nous énonçons le lemme 3.4.2 et nous passons tout de suite à la démonstration du théorème 1.7.6. Rappelons que pour $f(z) = \sum_{n \geq 0} a(n)z^n \in \mathbb{Q}[[z]]$ et p un nombre premier, $\Lambda_p(f(z)) = \sum_{n \geq 0} a(np)z^n$. Notons que si $f(z) \in \mathbb{Z}_{(p)}[[z]]$ alors $\Lambda_p(f(z))|_p = \Lambda_p(f|_p(z))$. Pour un entier $k \geq 1$, $\Lambda_p^k = \Lambda_p \circ \dots \circ \Lambda_p$ k -fois et $\Lambda_p^0 = Id$ est l'opérateur identité. Nous rappelons la définition de l'ensemble $\mathcal{F}(\mathcal{S})$.

Définition 3.4.1 ($\mathcal{F}(\mathcal{S})$). Soit \mathcal{S} un ensemble infini de nombres premiers. L'ensemble $\mathcal{F}(\mathcal{S})$ est constitué des séries $f(z) \in 1 + z\mathbb{Q}[[z]]$ telles que :

- Pour tout $p \in \mathcal{S}$, la série $f(z) \in \mathbb{Z}_{(p)}[[z]]$;
- $f(z)$ annule un opérateur différentiel $\mathcal{H} \in \mathbb{Q}(z)[\delta]$ muni d'une structure de Frobenius forte pour tout $p \in \mathcal{S}$, où $\delta = zd/dz$.

Lemme 3.4.2. Soit \mathcal{S} un ensemble infini de nombres premier et supposons que $f(z) \in \mathcal{F}(\mathcal{S})$. Si $f(z)$ annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MOM en zéro alors, il existe $\mathcal{S}' \subset \mathcal{S}$ infini et une constante strictement positive C tels que : l'ensemble $\mathcal{S} \setminus \mathcal{S}'$ est fini et, pour tout $p \in \mathcal{S}'$ et pour tout couple d'entiers i, m supérieurs ou égaux à zéro, il existe une fraction rationnelle $A_{p,i,m}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^m telle que $\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)(\Lambda_p^{i+m}(f|_p(z)))^{p^m}$.

Démonstration du théorème 1.7.6. Par hypothèse on a que $f(z) \in \mathcal{F}(\mathcal{S})$ et $f(z)$ annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MOM en zéro. Donc, d'après le lemme 3.4.2, il existe un ensemble infini $\mathcal{S}' \subset \mathcal{S}$ et une constante strictement positive C tels que : $\mathcal{S} \setminus \mathcal{S}'$ est fini et pour tout $p \in \mathcal{S}'$ et tout couple d'entiers positifs i, m , il existe une fraction rationnelle $A_{p,i,m}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^m telle que

$$\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)(\Lambda_p^{i+m}(f|_p(z)))^{p^m}. \quad (3.9)$$

1- Montrons que $f(z) \in \mathcal{L}^2(\mathcal{S}')$. Soit $p \in \mathcal{S}'$, comme $f(z)$ annule un opérateur différentiel muni d'une structure de Frobenius forte pour p et $f(z) \in \mathbb{Z}_{(p)}[[z]]$ alors, d'après le théorème 2.1 de [73] ou Christol [26], la série $f|_p(z)$ est algébrique sur $\mathbb{F}_p(z)$. Donc, il suit du théorème 1 de [20] que la suite définie par les coefficients de $f|_p(z)$ est p -automatique. Donc, il découle de la proposition 3.3 de [43, p. 107] qu'il existe un entier a positif et un entier b strictement positif tels que $\Lambda_p^a(f|_p(z)) = \Lambda_p^{a+b}(f|_p(z))$. Soit c un entier strictement positif tel que $cb > a$ et soit $l = cb$. En particulier, $\Lambda_p^a(f|_p(z)) = \Lambda_p^{a+l}(f|_p(z))$. Montrons

que $\Lambda_p^{2l}(f|_p(z)) = \Lambda_p^l(f|_p(z))$. En effet,

$$\begin{aligned}\Lambda_p^l(f|_p(z)) &= \Lambda_p^{l-a+a}(f|_p(z)) = \Lambda_p^{l-a}(\Lambda_p^a(f|_p(z))) \\ &= \Lambda_p^{l-a}(\Lambda_p^{a+l}(f|_p(z))) \\ &= \Lambda_p^{2l}(f|_p(z)).\end{aligned}$$

Il suit de (3.9) qu'il existe $A_{p,l,l}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^l telle que

$$\Lambda_p^l(f|_p(z)) = A_{p,l,l}(z)(\Lambda_p^{2l}(f|_p(z)))^{p^l}.$$

Comme $\Lambda_p^{2l}(f|_p(z)) = \Lambda_p^l(f|_p(z))$ alors,

$$\Lambda_p^l(f|_p(z)) = A_{p,l,l}(z)(\Lambda_p^l(f|_p(z)))^{p^l} \text{ et } A_{p,l,l}(z) = \frac{\Lambda_p^l(f|_p(z))}{\Lambda_p^l(f|_p(z))^{p^l}}.$$

Il suit aussi de (3.9) qu'il existe $A_{p,0,l}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^l telle que

$$f|_p(z) = A_{p,0,l}(z)\Lambda_p^l(f|_p(z))^{p^l} \text{ et } \frac{1}{A_{p,0,l}(z)} = \frac{\Lambda_p^l(f|_p(z))^{p^l}}{f|_p(z)}.$$

Par conséquent, $\frac{A_{p,l,l}(z)}{A_{p,0,l}(z)} = \frac{\Lambda_p^l(f|_p(z))}{f|_p(z)}$. Finalement, soit

$$A_p(z) = A_{p,0,l}(z) \left(\frac{A_{p,l,l}(z)}{A_{p,0,l}(z)} \right)^{p^l}.$$

Notons que le terme constant de $A_{p,0,l}(z)$ est 1 car le terme constant des séries $f|_p(z)$ et $\Lambda_p^l(f|_p(z))$ est 1. Donc, $\frac{1}{A_{p,0,l}(z)} \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$. D'où, $A_p(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$. De plus, la hauteur de $A_p(z)$ est inférieure ou égale à $2Cp^{2l}$ et

$$f|_p(z) = A_{p,0,l}(z)\Lambda_p^l(f|_p(z))^{p^l} = A_{p,0,l}(z) \frac{\Lambda_p^l(f|_p(z))^{p^l}}{f|_p(z)^{p^l}} f|_p(z)^{p^l} = A_p(z) f|_p(z)^{p^l}.$$

Comme \mathbb{F}_p est de caractéristique p alors $f|_p(z) = A_p(z) f|_p(z)^{p^l}$. Il suit donc que $f(z) \in \mathcal{L}^2(\mathcal{S}')$.

2- Montrons que $f(z) \in \mathcal{L}(\mathcal{S}')$. Soit $p \in \mathcal{S}'$, par hypothèse on sait qu'il existe un entier l strictement positif tel que $\Lambda_p^l(f|_p(z)) = f|_p(z)$. D'après (3.9), il existe une fraction rationnelle $A_{p,0,l}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^l telle que $f|_p(z) = A_{p,0,l}(z)(\Lambda_p^l(f|_p(z)))^{p^l}$. Ainsi, $f|_p(z) = A_{p,0,l}(z) f|_p(z)^{p^l}$ car \mathbb{F}_p est de caractéristique p et $\Lambda_p^l(f|_p(z)) = f|_p(z)$. D'où $f(z) \in \mathcal{L}(\mathcal{S}')$. \square

3.5 Démonstration du lemme 3.4.2

La démonstration du lemme 3.4.2 repose sur les propositions 3.5.2 et 3.5.4 énoncées ci-dessous. Avant de les énoncer nous allons introduire la définition d'un opérateur différentiel p -unipotent. Pour chaque nombre premier p nous notons E_p le corps des éléments analytiques. Le lecteur trouvera par exemple dans [73, section 3] la définition de ce corps. Nous soulignons que ce corps est muni de la norme ultramétrique de Gauss, nous notons ϑ_{E_p}

l'anneau des éléments de E_p tels que leurs normes sont inférieures ou égales à 1 et \mathfrak{m}_p son unique idéal maximal. Le corps résiduel de E_p est par définition $\vartheta_{E_p}/\mathfrak{m}_p$ et d'après le corollaire 1.3 de [26], $\vartheta_{E_p}/\mathfrak{m}_p$ est contenu dans $\overline{\mathbb{F}_p}((z))$, où $\overline{\mathbb{F}_p}$ est la clôture algébrique de \mathbb{F}_p . De plus, grâce au lemme 4.1 de [73] il existe un isomorphisme $\phi : \vartheta_{E_p}/\mathfrak{m}_p \rightarrow \overline{\mathbb{F}_p}(z)$. Il suit, d'après la définition de l'isomorphisme ϕ , que tout élément de $\vartheta_{E_p}/\mathfrak{m}_p$ est une fraction rationnelle à coefficients dans un corps fini de caractéristique p . Ainsi, le corps $\vartheta_{E_p}/\mathfrak{m}_p$ est contenu dans $\overline{\mathbb{F}_p}(z)$. Étant donné un opérateur différentiel \mathcal{D} à coefficients dans ϑ_{E_p} , l'opérateur différentiel \mathcal{D}_p à coefficients dans $\overline{\mathbb{F}_p}(z)$ est l'opérateur différentiel obtenu après avoir réduit chaque coefficient de \mathcal{D} modulo l'idéal maximal \mathfrak{m}_p . Remarquons qu'en fait \mathcal{D}_p est à coefficients dans $k(z)$, où k est un corps fini de caractéristique p . Maintenant, nous introduisons la notion d'opérateur p -unipotent.

Définition 3.5.1. [p -unipotent.] Soit \mathcal{D} un opérateur différentiel à coefficients dans E_p . On dit que \mathcal{D} est p -unipotent si :

1. \mathcal{D} est un opérateur différentiel à coefficients dans ϑ_{E_p} .
2. L'opérateur différentiel \mathcal{D}_p est non nul et MOM en zéro.

Proposition 3.5.2. Soient p un nombre premier et $f(z) \in \mathbb{Z}_{(p)}[[z]]$. Soient \mathcal{D} un opérateur p -unipotent d'ordre n et r le nombre de singularités à distance finie de \mathcal{D}_p dans $\overline{\mathbb{F}_p}$. Si $f(z)$ est solution de \mathcal{D} alors, il existe une fraction rationnelle $A_p(z) \in \overline{\mathbb{F}_p}(z)$ de hauteur inférieure ou égale à $nrp - 1$ telle que $f|_p(z) = A_p(z)(\Lambda_p(f|_p(z)))^p$.

Sous les hypothèses de la proposition 3.5.2, si $f(0) = 1$ alors $A_p(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$.

Définition 3.5.3. Étant donnée une série $f(z) \in \mathbb{Q}[[z]]$ qui annule un opérateur différentiel non nul à coefficients dans $\mathbb{Q}(z)$, nous notons \mathcal{M}_f l'opérateur différentiel minimal de $f(z)$ à coefficients dans $\mathbb{Q}(z)$.

L'opérateur différentiel \mathcal{M}_f jouit des propriétés suivantes : d'abord il n'est pas nul et, deuxièmement un opérateur différentiel \mathcal{L} à coefficients dans $\mathbb{Q}(z)$ est annulé par $f(z)$ si et seulement si \mathcal{L} appartient à l'idéal $\mathbb{Q}(z)[d/dz]\mathcal{M}_f$.

Proposition 3.5.4. Soient \mathcal{S} un ensemble infini de nombres premiers et $f(z) \in \mathcal{F}(\mathcal{S})$. Soient n l'ordre de \mathcal{M}_f et r le nombre de singularité à distance finie de \mathcal{M}_f dans $\overline{\mathbb{Q}}$. Si $f(z)$ annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MOM en zéro alors, il existe un ensemble $\mathcal{S}' \subset \mathcal{S}$ infini tel que : l'ensemble $\mathcal{S} \setminus \mathcal{S}'$ est fini et, pour tout $p \in \mathcal{S}'$ et tout entier positif k , la série $\Lambda_p^k(f(z))$ annule un opérateur p -unipotent \mathcal{L}_k d'ordre n tel que le nombre de singularités à distance finie de $\mathcal{L}_{k,p}$ dans $\overline{\mathbb{F}_p}$ est inférieur ou égal à r .

Nous rappelons que l'opérateur différentiel $\mathcal{L}_{k,p}$ est l'opérateur obtenu après avoir réduit \mathcal{L}_k modulo l'idéal maximal \mathfrak{m}_p .

3.5.1 Démonstration du lemme 3.4.2

Étant données les propositions 3.5.5 et 3.5.4 nous montrons le lemme 3.4.2.

Démonstration. Soient n l'ordre de \mathcal{M}_f et r le nombre de singularités à distance finie de \mathcal{M}_f dans $\overline{\mathbb{Q}}$. Par hypothèse la série $f(z)$ appartient à $\mathcal{F}(\mathcal{S})$ et annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MOM en zéro. Donc, on est en mesure d'appliquer la proposition 3.5.4 et ainsi, il existe un ensemble $\mathcal{S}' \subset \mathcal{S}$ infini tel que : l'ensemble $\mathcal{S} \setminus \mathcal{S}'$ est fini et pour tout $p \in \mathcal{S}'$ et tout entier positif k , la série $\Lambda_p^k(f(z))$ annule un opérateur p -unipotent \mathcal{L}_k d'ordre n dont le nombre de singularités à distance finie de $\mathcal{L}_{k,p}$ dans $\overline{\mathbb{F}_p}$ est inférieur

ou égal à r . Soient $p \in \mathcal{S}'$ et $i \in \mathbb{N}$, nous allons montrer par récurrence sur $m \in \mathbb{N}$ qu'il existe $A_{p,i,m} \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à $2nrp^m$ telle que

$$\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)(\Lambda_p^{i+m}(f|_p(z)))^{p^m}. \quad (3.10)$$

Il est clair que (3.10) est vrai pour $m = 0$. Maintenant supposons que l'égalité (3.10) est vraie pour m et montrons qu'elle l'est aussi pour $m + 1$. Donc, d'après notre hypothèse de récurrence il existe $A_{p,i,m}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à $2nrp^m$ telle que $\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)(\Lambda_p^{i+m}(f|_p(z)))^{p^m}$. Comme $p \in \mathcal{S}'$ alors, d'après la proposition 3.5.4, la série $\Lambda_p^{i+m}(f(z))$ annule un opérateur p -unipotent \mathcal{L}_{i+m} d'ordre n dont le nombre de singularités à distance finie de $\mathcal{L}_{i+m,p}$ est inférieur ou égal à r . Ainsi, on est en mesure d'appliquer la proposition 3.5.2 et par conséquent, il existe une fraction rationnelle $A_p(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à $nrp - 1$ telle que $\Lambda_p^{i+m}(f|_p(z)) = A_p(z)(\Lambda_p^{i+m+1}(f|_p(z)))^p$. D'où, $(\Lambda_p^{i+m}(f(z)))^{p^m} = A_p(z)^{p^m}(\Lambda_p^{i+m+1}(f|_p(z)))^{p^{m+1}}$. Il suit donc que,

$$\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)A_p(z)^{p^m}(\Lambda_p^{i+m+1}(f|_p(z)))^{p^{m+1}}.$$

On pose $A_{p,i,m+1}(z) = A_{p,i,m}(z)A_p(z)^{p^m}$. Alors, $A_{p,i,m+1}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ car $A_{p,i,m}(z)$ et $A_p(z)$ appartiennent à $\mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$. Montrons que la hauteur de $A_{p,i,m+1}(z)$ est inférieure ou égale à $2nrp^{m+1}$. Comme la hauteur de $A_p(z)$ est inférieure ou égale à $nrp - 1$ alors la hauteur de $A_p(z)^{p^m}$ est inférieure ou égale à $nrp^{m+1} - p^m$ et ainsi, la hauteur de $A_{p,i,m+1}(z)$ est inférieure ou égale à $2nrp^m + nrp^{m+1} - p^m$. Mais $2nrp^m + nrp^{m+1} - p^m = nrp^{m+1} + p^m(2nr - 1)$ et $p^m(2nr - 1) \leq nrp^{m+1}$ car $2nr - 1 \leq nrp$. Par conséquent, la hauteur de $A_{p,i,m+1}(z)$ est inférieure ou égale à $2nrp^{m+1}$. Finalement, on pose $C = 2nr$. Donc C est une constante strictement positive indépendante de p . Ainsi nous avons montré que pour tout $p \in \mathcal{S}'$ et tout couple d'entiers positifs i, m , il existe une fraction rationnelle $A_{p,i,m}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^m telle que

$$\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)(\Lambda_p^{i+m}(f|_p(z)))^{p^m}.$$

□

3.5.2 Démonstration de la proposition 3.5.2

Notre but dans cette partie est de montrer la proposition 3.5.2. Pour se faire nous aurons besoins de quelques résultats concernant la théorie des opérateurs différentiels à coefficients dans un corps de caractéristique non nulle. Nos résultats de cette partie s'appuient sur, Bostan, Schost [16], Cluzeau [30] et Honda [50]. Étant donné un opérateur différentiel \mathcal{D} à coefficients dans $K(z)$, K un corps quelconque, les ensembles $\text{Ker}(K(z), \mathcal{D})$ et $\text{Ker}(K((z)), \mathcal{D})$ désignent respectivement les solutions de \mathcal{D} qui sont dans $K(z)$ et $K((z))$. Dans le cas où K est un corps de caractéristique p , les deux ensembles sont respectivement $K(z^p)$, $K((z^p))$ -espaces vectoriels.

Lemme 3.5.5. *Soient \mathcal{D} un opérateur différentiel p -unipotent et k un corps fini de caractéristique p tel que \mathcal{D}_p est un opérateur différentiel à coefficients dans $k(z)$. Si le $k(z^p)$ -espace vectoriel $\text{ker}(k(z), \mathcal{D}_p)$ est différent de zéro alors $\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_p) = 1$.*

Démonstration. Par hypothèse il existe une fraction rationnelle $P(z) \in k(z)$ non nulle telle que $\mathcal{D}_p(P(z)) = 0$. Écrivons

$$\mathcal{D}_p := a_0(z) \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{dz^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} + a_n(z),$$

où les $a_i(z)$ appartiennent à $k[z]$. Considérons $\mathcal{D}_{\infty,p}$ l'opérateur différentiel

$$\mathcal{D}_{\infty,p} := b_0(z) \frac{d^n}{dz^n} + b_1 \frac{d^{n-1}}{dz^{n-1}} + \cdots + b_{n-1}(z) \frac{d}{dz} + b_n(z),$$

où le vecteur $(b_0(z), \dots, b_n(z))^t \in k[z]^{n+1}$ est égal à

$$\frac{(-1)^n}{z^{2n}} \left(a_0\left(\frac{1}{z}\right), a_1\left(\frac{1}{z}\right), \dots, a_{n-1}\left(\frac{1}{z}\right), a_n\left(\frac{1}{z}\right) \right) \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & -z^2 & 0 & 0 & \dots & 0 & 0 \\ 0 & 2z^3 & z^4 & 0 & 0 \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \\ 0 & * & * & * & \dots & * & 0 \\ 0 & * & * & * & \dots & * & (-z^2)^n \end{pmatrix}.$$

Cette matrice exprime le vecteur $(1, D, \dots, D^n)$ en fonction du vecteur $(1, \frac{d}{dz}, \dots, \frac{d^n}{z^{n-1}})$, où $D = -z^2 \frac{d}{dz}$. Comme \mathcal{D}_p est singulier régulier en zéro et ses exposants en zéro sont tous égaux, alors l'opérateur différentiel $\mathcal{D}_{\infty,p}$ est singulier régulier en l'infini et ses exposants en l'infini sont tous égaux. De plus, $\text{Ker}(k(z), \mathcal{D}_{\infty,p}) \neq 0$ car $\mathcal{D}_{\infty,p}(P(\frac{1}{z})) = 0$ et $P(\frac{1}{z})$ est non nulle. Montrons que $\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_{\infty,p}) = 1$. Pour ce faire on va démontrer que si $P_1(z), P_2(z) \in \text{Ker}(k(z), \mathcal{D}_{\infty,p})$ sont non nulles alors il existe $c(z^p) \in k(z^p)$ non nulle telle que $P_2(z) = c(z^p)P_1(z)$. Raisonnons par l'absurde et supposons que $P_1(z), P_2(z)$ sont linéairement indépendantes sur $k(z^p)$. Grâce au lemme 1.1 de [42, Chap. III], on a que $(\frac{d}{dz}P_1(z))P_2(z) - P_1(z)(\frac{d}{dz}P_2(z)) \neq 0$. Puisque k est un corps de caractéristique p alors, d'après la remarque 3 de [30, section 1.1.4], il existe $D_1(z)$ et $D_2(z)$ dans $k[z]$ non nuls tels que $D_1(z)^p P_1(z)$ et $D_2(z)^p P_2(z)$ appartiennent à $k[z] \cap \text{Ker}(k(z), \mathcal{D}_{\infty,p})$. Comme la caractéristique du corps k est p alors,

$$\begin{aligned} \left(\frac{d}{dz}(D_1(z)^p P_1(z)) \right) D_2(z)^p P_2(z) - D_1(z)^p P_1(z) \left(\frac{d}{dz}(D_2(z)^p P_2(z)) \right) = \\ D_1(z)^p D_2(z)^p \left[\left(\frac{d}{dz}P_1(z) \right) P_2(z) - P_1(z) \left(\frac{d}{dz}P_2(z) \right) \right] \neq 0. \end{aligned}$$

Ainsi, d'après le lemme 1.1 de [42, Chap III], les polynômes $D_1(z)^p P_1(z)$ et $D_2(z)^p P_2(z)$ sont linéairement indépendants sur $k(z^p)$. Soit \mathfrak{A} l'ensemble constitué des entiers strictement positifs qui sont de la forme $\deg(R(z)) + \deg(S(z))$, où $R(z)$ et $S(z)$ appartiennent à $k[z] \cap \text{Ker}(k(z), \mathcal{D}_{\infty,p})$ et sont linéairement indépendants sur $k(z^p)$. Notons que \mathfrak{A} est non vide car

$$\deg(D_1(z)^p P_1(z)) + \deg(D_2(z)^p P_2(z))$$

appartient à \mathfrak{A} . Par conséquent, il existe deux polynômes $Q_1(z)$ et $Q_2(z)$ linéairement indépendants sur $k(z^p)$ tels que, $Q_1(z)$ et $Q_2(z)$ sont dans $k[z] \cap \text{Ker}(k(z), \mathcal{D}_{\infty,p})$ et $\deg(Q_1(z)) + \deg(Q_2(z))$ est l'élément le plus petit de \mathfrak{A} . Démontrons maintenant en utilisant les arguments donnés par Honda dans [50, proposition 5.1] que

$$\deg(Q_1(z)) \neq \deg(Q_2(z)) \pmod{p}. \quad (3.11)$$

Raisonnons par l'absurde et supposons que $\deg(Q_1(z)) - \deg(Q_2(z)) = vp \geq 0$. Donc, il existe $c \in k$ non nul tel que $\deg(Q_1(z) - cz^{vp}Q_2(z)) < \deg(Q_1(z))$. Soit $R_1(z) = Q_1(z) - cz^{vp}Q_2(z)$. Les polynômes $R_1(z)$ et $Q_2(z)$ sont linéairement indépendants sur $k(z^p)$ car $Q_1(z)$ et $Q_2(z)$ le sont aussi. Notons que $R_1(z)$ est solution de $\mathcal{D}_{\infty,p}$ car k est de caractéristique p . Alors, $\deg(R_1(z)) + \deg(Q_2(z))$ appartient à \mathfrak{A} . Mais, $\deg(R_1(z)) + \deg(Q_2(z)) < \deg(Q_1(z)) + \deg(Q_2(z))$. Cela contredit le fait que $\deg(Q_1(z)) + \deg(Q_2(z))$

est l'élément le plus petit de \mathfrak{A} . Donc, $\deg(Q_1(z)) \neq \deg(Q_2(z)) \pmod{p}$. Maintenant, d'après la proposition 2.2 de [50], on a que $-\deg(Q_1(z)) \pmod{p}$ et $-\deg(Q_2(z)) \pmod{p}$ sont exposants en l'infini de $\mathcal{D}_{\infty,p}$. Mais, nous savons que les exposants en l'infini de $\mathcal{D}_{\infty,p}$ sont tous égaux. Alors,

$$\deg(Q_1(z)) = \deg(Q_2(z)) \pmod{p}. \quad (3.12)$$

Les égalités (3.11) et (3.12) se contredisent et par conséquent, $P_1(z)$ et $P_2(z)$ sont polynômes linéairement dépendantes sur $k(z^p)$. D'où il existe $c(z^p) \in k(z^p)$ non nulle telle que $P_2(z) = c(z^p)P_1(z)$. Ainsi, $\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_{\infty,p}) = 1$. Montrons que cette égalité implique que,

$$\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_p) = 1.$$

En effet, soit $B(z) \in \text{Ker}(k(z), \mathcal{D}_p)$ non nulle, alors $B(1/z) \in \text{Ker}(k(z), \mathcal{D}_{\infty,p})$, d'où il existe $c(z^p) \in k(z^p)$ non nulle telle que $B(1/z) = c(z^p)P(1/z)$. Par conséquent, $B(z) = c(1/z^p)P(z)$ et ainsi $\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_p) = 1$. \square

La proposition 3.5.6 à été démontrée par Bostan et Schost dans [16] lorsque $k = \mathbb{F}_p$ (voir proposition 1 de [16]). Nous omettons la preuve de la proposition 3.5.6 car nous remarquons que les arguments donnés par Bostan et Schost dans leur preuve restent valides quel que soit le corps fini de caractéristique p .

Proposition 3.5.6. *Soient k un corps fini de caractéristique p et*

$$\mathcal{L}_p = l_0(z) \frac{d^n}{dz^n} + l_1(z) \frac{d^{n-1}}{z^{n-1}} + \cdots + l_{n-1}(z) \frac{d}{dz} y + l_n(z),$$

où les $l_i(z)$ appartiennent à $k[z]$ et $l_0(z)$ est non nul. Soit d un entier strictement positif tel que pour chaque $i \in \{0, \dots, n\}$, le degré de $l_i(z)$ est majoré par d . Si $\text{Ker}(k(z), \mathcal{L}_p) \neq 0$ alors il existe $P_1(z), \dots, P_s(z)$ qui appartiennent à $k[z] \cap \text{Ker}(k(z), \mathcal{L}_p)$ tels que : l'ensemble $\{P_1(z), \dots, P_s(z)\}$ est une base de $\text{Ker}(k(z), \mathcal{L}_p)$ sur $k(z^p)$ et pour chaque $i \in \{1, \dots, s\}$, le degré de $P_i(z)$ est inférieur ou égal à $pd - 1$.

Nous allons appliquer la proposition 3.5.6 dans le cas d'un opérateur différentiel fuchsien.

Lemme 3.5.7. *Soient k un corps fini de caractéristique p et*

$$\mathcal{D}_p := \frac{d^n}{dz^n} + a_1(z) \frac{d^{n-1}}{z^{n-1}} + \cdots + a_{n-1}(z) \frac{d}{dz} y + a_n(z),$$

un opérateur différentiel fuchsien, où les $a_i(z)$ appartiennent à $k(z)$. Soient $\gamma_1, \dots, \gamma_r$ les singularités à distance finie de \mathcal{D}_p dans $\overline{\mathbb{F}_p}$. Si $\text{Ker}(k(z), \mathcal{D}_p) \neq 0$ alors l'opérateur différentiel \mathcal{D}_p est annulé par un polynôme $P(z) \in k[z]$ non nul de degré inférieur ou égal à $pnr - 1$.

Démonstration. On pose $l_0(z) = \prod_{j=1}^r (z - \gamma_j)^n$. Pour chaque $i \in \{1, \dots, n\}$, écrivons $a_i(z) = \frac{b_{i,1}(z)}{b_{i,2}(z)}$, où $b_{i,1}(z)$ et $b_{i,2}(z)$ appartiennent à $k[z]$ et sont premiers entre eux. Comme $\gamma_1, \dots, \gamma_r$ sont les points singuliers de \mathcal{D}_p dans $\overline{\mathbb{F}_p}$ alors pour tout $i \in \{1, \dots, n\}$, $b_{i,2}(z) = \prod_{j=1}^r (z - \gamma_j)^{m_{j,i}}$, où $m_{j,i}$ est un entier supérieur ou égal à zéro. Maintenant, puisque \mathcal{D}_p est fuchsien alors pour chaque $j \in \{1, \dots, r\}$, $(z - \gamma_j)^i a_i(z)$ n'a pas de pôle en γ_j , d'où $i \geq m_{j,i}$ pour chaque $j \in \{1, \dots, r\}$. Comme l'infini est un point singulier régulier de

\mathcal{D}_p alors, $\deg(b_{i,1}(z)) \leq \deg(b_{i,2}(z)) - i$. Par conséquent, le degré du polynôme $P_i(z) := \prod_{j=1}^r (z - \gamma_j)^{i - m_{j,i}} b_{i,1}(z)$ est inférieur ou égal à $i(r-1)$. De plus, pour chaque $i \in \{1, \dots, n\}$,

$$a_i(z) = \frac{\prod_{j=1}^r (z - \gamma_j)^{i - m_{j,i}} b_{i,1}(z)}{\prod_{j=1}^r (z - \gamma_j)^i} = \frac{P_i(z)}{\prod_{j=1}^r (z - \gamma_j)^i}.$$

Posons $\mathcal{L}_p := l_0(z)\mathcal{D}_p$. Alors,

$$\mathcal{L}_p = l_0(z) \frac{d^n}{dz^n} + l_1(z) \frac{d^{n-1}}{dz^{n-1}} y + \dots + l_{n-1}(z) \frac{d}{dz} + l_n(z),$$

où pour chaque $i \in \{1, \dots, n\}$, $l_i(z) = \prod_{j=1}^r (z - \gamma_j)^{n-i} P_i(z)$. Montrons que \mathcal{L}_p est à coefficients dans $k[z]$. Pour cela il suffit de montrer que $l_0(z) \in k[z]$ car par hypothèse \mathcal{D}_p est à coefficients dans $k(z)$. Soit $k' = k(\gamma_1, \dots, \gamma_r)$. Notons que k' est le corps de décomposition des polynômes, $b_{1,2}(z), \dots, b_{n,2}(z) \in k[z]$ et ainsi, k' est une extension normale de k . De plus, k' est aussi une extension séparable de k car k est fini. Par conséquent, k' est une extension galoisienne de k . Puisque $l_0(z) \in k'[z]$ et k' est une extension galoisienne de k alors, d'après le théorème fondamental de la théorie de Galois, pour montrer que $l_0(z) \in k[z]$ il suffit de montrer que pour tout automorphisme $\sigma : k' \rightarrow k'$ qui laisse fixe k on a que, $l_0^\sigma(z) = l_0(z)$, où $l_0^\sigma(z)$ est le polynôme obtenu après avoir appliqué σ à chaque coefficient de $l_0(z)$. En effet, notons que $\{\sigma(\gamma_1), \dots, \sigma(\gamma_r)\} = \{\gamma_1, \dots, \gamma_r\}$ car σ fixe k et $\gamma_1, \dots, \gamma_r$ sont les racines des polynômes $b_{1,2}(z), \dots, b_{n,2}(z) \in k[z]$. Alors,

$$l_0(z) = \prod_{j=1}^r (z - \gamma_j)^n = \prod_{j=1}^r (z - \sigma(\gamma_j))^n = l_0^\sigma(z).$$

Maintenant, puisque pour tout $i \in \{1, \dots, n\}$, le degré de $P_i(z)$ est inférieur ou égal à $i(r-1)$ alors le degré de $l_i(z)$ est inférieur ou égal à $nr - i$ pour tout $i \in \{1, \dots, n\}$ et ainsi, $d = \max\{\deg(l_0(z)), \dots, \deg(l_n(z))\} = nr$ car $\deg(l_0(z)) = nr$. Par hypothèse il existe $Q(z) \in \text{Ker}(k(z), \mathcal{D}_p)$ non nulle et comme, $\mathcal{L}_p = l_0(z)\mathcal{D}_p$ alors $Q(z) \in \text{Ker}(k(z), \mathcal{L}_p)$ et ainsi, $\text{Ker}(k(z), \mathcal{L}_p) \neq 0$. Donc, il découle de la proposition 3.5.6 qu'il existe un polynôme $P(z) \in k[z]$ non nul solution de l'opérateur \mathcal{L}_p de degré inférieur ou égal à $pnr - 1$. Finalement, puisque $\mathcal{L}_p = l_0(z)\mathcal{D}_p$ et $l_0(z)$ est non nul alors $P(z) \in \text{Ker}(k(z), \mathcal{D}_p)$. \square

Le lemme suivant se sert d'un résultat de Katz que nous utilisons sous la forme énoncée dans le lemme 9 de [30, section 1.3.5]. Cette démonstration utilise la notion de p -courbure d'un opérateur différentiel. Avant de donner la démonstration nous rappelons cette notion.

Définition 3.5.8 (p -Courbure). Soit \mathbb{K} le corps $k(z)$ ou $k((z))$, où k est un corps de caractéristique p . Soit $\mathcal{D}_p \in \mathbb{K}[d/dz]$ un opérateur différentiel d'ordre n et soit A la matrice compagnon de \mathcal{D}_p . La p -courbure de \mathcal{D}_p est l'opérateur de \mathbb{K}^n dans \mathbb{K}^n défini par

$$\psi_{p,\mathbb{K}} := \left(\frac{d}{dz} - A \right)^p.$$

Il suit du lemme 1 de [30, section 1.3] que $\psi_{p,\mathbb{K}}$ est une application \mathbb{K} -linéaire. Ainsi, $\psi_{p,\mathbb{K}}(\sum_{i=1}^n r_i e_i) = \sum_{i=0}^n r_i \psi_{p,\mathbb{K}}(e_i)$, où les $r_i \in \mathbb{K}$ et les e_i sont les vecteurs canoniques de \mathbb{K}^n . En particulier, si \mathcal{D}_p est un opérateur différentiel à coefficients dans $k(z)$ il est aussi un opérateur différentiel à coefficients dans $k((z))$ et par conséquent, $\psi_{p,k(z)} \otimes_{k(z)} Id = \psi_{p,k((z))}$, où Id est l'identité sur $k((z))$. Remarquons que $k((z))^n = k(z)^n \otimes_{k(z)} k((z))$.

Lemme 3.5.9. Soit \mathcal{D}_p un opérateur différentiel à coefficients dans $k(z)$, k un corps de caractéristique p . Alors, $\text{Ker}(k(z), \mathcal{D}_p) \neq 0$ si et seulement si, $\text{Ker}(k((z)), \mathcal{D}_p) \neq 0$ et,

$$\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_p) = \dim_{k((z^p))} \text{Ker}(k((z)), \mathcal{D}_p).$$

Démonstration. Il est clair que si $\text{Ker}(k(z), \mathcal{D}_p) \neq 0$ alors $\text{Ker}(k((z)), \mathcal{D}_p) \neq 0$. Maintenant, montrons que si $\text{Ker}(k(z), \mathcal{D}_p) = 0$ alors $\text{Ker}(k((z)), \mathcal{D}_p) = 0$. D'après le lemme 9 de [30, section 1.3.5], on a que

$$\dim_{k(z^p)} \ker(k(z), \mathcal{D}_p) = \dim_{k(z)} \text{Ker}(\psi_{p,k(z)}) \quad (3.13)$$

$$\dim_{k((z^p))} \ker(k((z)), \mathcal{D}_p) = \dim_{k((z))} \text{Ker}(\psi_{p,k((z))}). \quad (3.14)$$

Considérons la suite exacte

$$0 \rightarrow \text{Ker}(\psi_{p,k(z)}) \xrightarrow{i} k(z)^n \xrightarrow{\psi_{p,k(z)}} \text{Img}(\psi_{p,k(z)}) \rightarrow 0,$$

où, $i(x) = x$ pour tout $x \in \text{Ker}(\psi_{p,k(z)})$. Puisque $k((z))$ est un $k(z)$ -espace vectoriel alors la suite

$$0 \rightarrow \text{Ker}(\psi_{p,k(z)}) \otimes_{k(z)} k((z)) \xrightarrow{\phi} k(z)^n \otimes_{k(z)} k((z)) \xrightarrow{\tau} \text{Img}(\psi_{p,k(z)}) \otimes_{k(z)} k((z)) \rightarrow 0$$

est exacte, où $\phi = i \otimes \text{Id}$, $\tau = \psi_{p,k(z)} \otimes \text{Id}$ et Id est l'identité sur $k((z))$. Comme on a vu, $\psi_{p,k(z)} \otimes_{k(z)} \text{Id} = \psi_{p,k((z))}$ et $k(z)^n \otimes_{k(z)} k((z)) = k((z))^n$. Donc,

$$\text{Ker}(\psi_{p,k((z))}) = \text{Ker}(\psi_{p,k(z)}) \otimes_{k(z)} k((z)). \quad (3.15)$$

Ainsi, si $\ker(k(z), \mathcal{D}_p) = 0$ alors (3.13) entraîne que, $\text{Ker}(\psi_{p,k(z)}) = 0$. Par conséquent, de (3.15) découle que $\text{Ker}(\psi_{p,k((z))}) = 0$. Ainsi de (3.14) on obtient que $\ker(k((z)), \mathcal{D}_p) = 0$. Finalement montrons que

$$\dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_p) = \dim_{k((z^p))} \text{Ker}(k((z)), \mathcal{D}_p).$$

En effet, soit $l = \dim_{k(z^p)} \text{Ker}(k(z), \mathcal{D}_p)$ alors il suit de (3.13) que $l = \dim_{k(z)} \text{Ker}(\psi_{p,k(z)})$. Donc, il découle de (3.15) que $\text{Ker}(\psi_{p,k((z))})$ comme $k((z))$ espace vectoriel est isomorphe à $k((z))^l$ et ainsi, on a l'égalité suivante $\dim_{k((z))} \text{Ker}(\psi_{p,k((z))}) = l$ et il suit de (3.14) que, $\dim_{k((z^p))} \text{Ker}(k((z)), \mathcal{D}_p) = l$. \square

Démonstration de la proposition 3.5.2. Notons que si la série $f_{|p}(z)$ est nulle alors la proposition 3.5.2 découle tout de suite. Supposons que $f_{|p}(z)$ est non nulle. Comme $f_{|p}(z)$ est solution de \mathcal{D}_p et $f_{|p}(z) \in k((z))$ est non nulle donc $\ker(k((z)), \mathcal{D}_p) \neq 0$. Ainsi, d'après le lemme 3.5.9, $\ker(k(z), \mathcal{D}_p) \neq 0$. Comme \mathcal{D} est p -unipotent il suit du lemme 3.5.5 que $\dim_{k(z^p)} \ker(k(z), \mathcal{D}_p) = 1$. Alors, selon le lemme 3.5.9, $\dim_{k((z^p))} \ker(k((z)), \mathcal{D}_p) = 1$. De plus, on a que \mathcal{D}_p est fuchsien car \mathcal{D} est p -unipotent. Puisque $\ker(k(z), \mathcal{D}_p) \neq 0$, alors le lemme 3.5.7 nous garantie l'existence d'un polynôme $P(z) \in \text{Ker}(k(z), \mathcal{D}_p)$ non nul de degré inférieur ou égal à $pnr - 1$. Finalement, comme $f_{|p}(z), P(z)$ appartiennent à $\ker(k((z)), \mathcal{D}_p)$ et $\dim_{k((z^p))} \ker(k((z)), \mathcal{D}_p) = 1$ alors il existe $g(z) \in k((z))$ telle que $f_{|p}(z) = P(z)g(z^p)$. Notons que $\Lambda_p(P(z)g(z^p)) = \Lambda_p(P(z))g(z)$ et ainsi, $\Lambda_p(f_{|p}(z)) = \Lambda_p(P(z))g(z)$ et comme $f_{|p}(z) \in \mathbb{F}_p[z]$ alors, $\frac{\Lambda_p(f_{|p}(z))^p}{\Lambda_p(P(z^p))} = g(z^p)$. Par conséquent, $f_{|p}(z) = \frac{P(z)}{\Lambda_p(P(z^p))} \Lambda_p((f_{|p}(z))^p)$. Finalement, comme $\deg(\Lambda_p(P(z^p))) \leq \deg(P(z)) \leq nrp - 1$ alors la hauteur de $\frac{P(z)}{\Lambda_p(P(z^p))}$ est inférieur ou égale à $nrp - 1$. \square

3.5.3 Démonstration de la proposition 3.5.4

Le but de cette partie est de démontrer la proposition 3.5.4. La démonstration que nous faisons de cette proposition repose sur la théorie des équations différentielles p -adiques.

Équations différentielles p -adiques

Dans cette partie nous travaillons à p fixé. Notre principal résultat dans cette partie est le lemme 3.5.18. Avant de l'énoncer nous commençons avec la définition des ensembles $E_{0,p}$, \mathcal{M}_p , des disques singuliers réguliers et de la propriété $(\mathbf{P})_{p,r,n}$. Nous rappelons que \mathbb{C}_p est le complété de la clôture algébrique de \mathbb{Q}_p .

Définition 3.5.10. $E_{0,p}$ est l'ensemble des éléments analytiques E_p qui n'ont pas de pôle dans le disque ouvert $D(0,1)$.

En particulier, l'ensemble $E_{0,p}$ est un anneau contenu dans $\mathbb{C}_p[[z]]$. La définition suivante a été introduite par Christol dans [24, Chap 4] dans un contexte plus large.

Définition 3.5.11. Soit p un nombre premier, nous notons \mathcal{M}_p l'ensemble des matrices carrées L à coefficients dans E_p qui satisfont aux conditions suivantes :

- i) L est une matrice dont les coefficients appartiennent à $E_{0,p}$.
- ii) Les valeurs propres de la matrice $L(0)$ sont toutes égales à zéro.
- iii) Il existe une matrice inversible U , dont les coefficients sont analytiques dans le disque générique ouvert $D(z,1)$, telle que $\delta(U) = LU$, où $\delta = z \frac{d}{dz}$.

Définition 3.5.12 ([24]). Nous dirons que deux matrices F et L de même taille qui appartiennent à \mathcal{M}_p sont équivalentes s'il existe une matrice inversible H à coefficients dans E_p de même taille que F et L qui vérifie les conditions suivantes :

- 1. Il existe un entier n pour lequel les coefficients des matrices $z^n H$ et $z^n H^{-1}$ sont dans $E_{0,p}$.
- 2. On a $\delta H = FH - HL$.

Définition 3.5.13 (Structure de Frobenius forte). Soient $\mathcal{H} \in \mathbb{Q}(z)[\delta]$, $A(z)$ la matrice compagnon de \mathcal{H} et p un nombre premier. On dit que l'opérateur différentiel \mathcal{H} est muni d'une structure de Frobenius forte pour p de période h s'il existe une matrice inversible $H(z)$ à coefficients dans E_p de même taille que A et un entier $h > 0$ tels que

$$\delta H(z) = A(z)H(z) - p^h H(z)A(z^{p^h}).$$

Remarque 3.5.14. Soit $G(z) \in \mathcal{M}_p$ de taille n . Alors que le système $\delta X = G(z)X$ à une base de solutions dans l'anneau $\mathbb{C}_p[[z, \text{Log}z]]$, où $\delta \text{Log}z = 1$. En effet, comme les valeurs propres de la matrice $G(0)$ sont toutes égales à zéro et $G(z)$ est à coefficients dans $\mathbb{C}_p[[z]]$ alors, d'après la proposition 8.5 de [42, Chap III], une matrice fondamentale de solutions du système $\delta X = G(z)X$ est donné par $Y_G X^{G(0)}$, où $Y_G \in \text{Gl}_n(\mathbb{C}_p[[z]])$, $Y_G(0)$ est la matrice identité et $X^{G(0)} = \sum_{j \geq 0} G(0)^j \frac{(\text{Log}z)^j}{j!}$. Comme $\delta \text{Log}z = 1$ alors $\delta X^{G(0)} = G(0)X^{G(0)}$. Ainsi, $\delta(Y_G) + G(z)G(0) = G(z)Y_G(z)$ car $\delta(Y_G X^{G(0)}) = G(z)Y_G X^{G(0)}$. Comme toutes les valeurs propres de $G(0)$ sont égales à zéro alors $G(0)^n = 0$ et ainsi, $X^{G(0)} = \sum_{j=0}^{n-1} G(0)^j \frac{(\text{Log}z)^j}{j!}$. La matrice Y_G est appelée *la part uniforme* de la matrice G .

Le lemme suivant nous assure l'existence de la structure de Frobenius faible pour toute matrice dans \mathcal{M}_p .

Lemme 3.5.15. *Si $G(z)$ appartient à \mathcal{M}_p alors il existe $F(z)$ dans \mathcal{M}_p telle que les matrices G et $pF(z^p)$ sont équivalentes. Plus précisément on a :*

1. $F(z) = [\delta(\Lambda_p(Y_G)) + \frac{1}{p}\Lambda_p(Y_G)G(0)](\Lambda_p(Y_G))^{-1}$, où Y_G est la part uniforme de la matrice G et $\Lambda_p(Y_G)$ est la matrice obtenue après avoir appliqué Λ_p à chaque entrée de Y_G .
2. Il existe une matrice $H \in Gl_n(E_{0,p})$ telle que $H(0)$ est la matrice identité et $\delta H = pF(z^p)H - HG$.

La démonstration que nous présentons de ce lemme suit les arguments donnés par Christol dans [24, lemme 5.1].

Démonstration. Soit $G(z)$ dans \mathcal{M}_p de taille n . D'après la remarque 3.5.14, une matrice fondamentale de solutions du système $\delta X = G(z)X$ est donnée par $Y_G X^{G(0)}$, où $Y_G \in Gl_n(\mathbb{C}_p[[z]])$ et $Y_G(0) = I_n$, où I_n est la matrice identité de taille n . Maintenant considérons la suite de matrices G_j définie comme suit : $G_0(z) = Id$ et $G_{j+1}(z) = \delta G_j(z) + G_j(z)(G(z) - jI_n)$. On pose $H(z) = \frac{1}{p} \sum_{\xi^p=1} \sum_{j \geq 0} G_j(z) \frac{(\xi-1)^j}{j!}$. Comme $G(z)$ vérifie la condition iii) de la définition 3.5.11 alors, il est montré dans [24, p. 164] que la matrice H appartient à $Gl_n(E_{0,p})$. Écrivons $Y_G = \sum_{j \geq 0} Y_j z^j$, où pour tout $j \geq 0$, Y_j est une matrice à coefficients dans \mathbb{C}_p . Comme la matrice $G(0)$ est nilpotente car $G(0)^n = 0$ (voir remarque 3.5.14) alors, il est montré dans [24, p. 165] que, $HY_G = \sum_{j \geq 0} Y_j z^{jp}$. Ainsi, $HY_G = \Lambda_p(Y_G)(z^p)$, où $\Lambda_p(Y_G)$ désigne la matrice obtenue après avoir appliqué Λ_p à chaque entrée de Y_G . Par conséquent, $H(0) = I_n$. Maintenant on pose

$$F(z) = [\delta(\Lambda_p(Y_G)) + \frac{1}{p}\Lambda_p(Y_G)G(0)](\Lambda_p(Y_G))^{-1}. \quad (3.16)$$

Ainsi, $pF(z^p) = [p(\delta(\Lambda_p(Y_G)))(z^p) + HY_G G(0)][Y_G^{-1}H^{-1}]$. Notons que

$$(\delta H)Y_G + H(\delta Y_G) = \delta(HY_G) = \delta(\Lambda_p(Y_G)(z^p)) = p(\delta(\Lambda_p(Y_G)))(z^p).$$

D'après la remarque 3.5.14, $\delta Y_G = GY_G - Y_G G(0)$ alors,

$$p(\delta(\Lambda_p(Y_G)))(z^p) = (\delta H)Y_G + H[G Y_G - Y_G G(0)].$$

Donc,

$$\begin{aligned} pF(z^p) &= [(\delta H)Y_G + H[G Y_G - Y_G G(0)] + HY_G G(0)][Y_G^{-1}H^{-1}] \\ &= [(\delta H)Y_G + HGY_G][Y_G^{-1}H^{-1}] \\ &= (\delta H)H^{-1} + HGH^{-1}. \end{aligned}$$

Par conséquent, $\delta H = pF(z^p)H - HG$. Il est montré dans [24, p.165-166] que la matrice $F(z)$ vérifie les conditions i) et iii) de la définition 3.5.11. En particulier on peut évaluer la matrice F en zéro. Comme $H(0) = I_n$ alors l'égalité $\delta H = pF(z^p)H - HG$ entraîne que, $pF(0) = G(0)$. Ainsi, toutes les valeurs propres de $F(0)$ sont égales à zéro. Donc, la matrice F vérifie la condition ii) de la définition 3.5.11. Ainsi, la matrice $F(z)$ appartient à \mathcal{M}_p et les matrices $pF(z^p)$ et $G(z)$ sont équivalentes. \square

Nous rappelons les notions de *pôle* pour un élément de E_p et de *disque singulier régulier* pour une matrice à coefficients dans E_p . Pour chaque $\alpha \in \overline{\mathbb{F}_p}$, l'anneau E_p^α est la fermeture dans le cors E_p de l'anneau des fractions rationnelles de $\mathbb{C}_p(z)$ dont tous les pôles appartiennent à $\mathfrak{v}_{\mathbb{C}_p}$ et ont α pour image dans le corps $\overline{\mathbb{F}_p}$ et qui sont nulles à l'infini.

D'une manière analogue l'anneau E_p^∞ est la fermeture dans le corps E_p de l'ensemble des fractions rationnelles de $\mathbb{C}_p(z)$ qui n'ont pas de pôle dans $\vartheta_{\mathbb{C}_p}$. Donc, grâce au théorème de Mittag-Leffler, voir par exemple théorème 2.1.6 de [23], à tout élément $a(z) \in E_p$ on peut associer de manière unique des éléments analytiques $a_\alpha(z) \in E_p^\alpha$, pour α parcourant l'ensemble $\overline{\mathbb{F}_p} \cup \{\infty\}$, tels que la famille $\{a_\alpha(z)\}$ tende vers zéro selon le filtre des complémentaires des parties finies de $\overline{\mathbb{F}_p} \cup \{\infty\}$ et qui vérifient

$$a(z) = \sum_{\alpha \in \overline{\mathbb{F}_p} \cup \{\infty\}} a_\alpha(z), \quad |a(z)| = \sup |a_\alpha(z)|.$$

Soient $\gamma \in \vartheta_{\mathbb{C}_p} \cup \{\infty\}$ et $a(z) \in E_p$. Le point γ est un *pôle* de $a(z)$ si dans l'écriture donnée par le théorème de Mittag-Leffler l'élément qui correspond à l'anneau E_p^γ est non nul.

Pour $\gamma \in \vartheta_{\mathbb{C}_p}$, nous notons D_γ le disque ouvert de centre γ et de rayon 1 et D_∞ est l'ensemble des éléments de \mathbb{C}_p qui ont une norme supérieure à 1. Remarquons que $D_\gamma = D_\beta$ si et seulement si $|\gamma - \beta|_p < 1$. Nous avons aussi que $|\gamma - \beta|_p = 1$ si, et seulement si $D_\gamma \cap D_\beta = \emptyset$. Soit $A \in M_n(E_p)$. La matrice A est *singulière régulière* dans le disque D_γ , s'il existe une matrice A_γ telle que, les matrices A et A_γ sont E_p -équivalentes² et il existe $\beta_\gamma \in D_\gamma$ tel que la matrice $(z - \beta_\gamma)A_\gamma$ n'a pas de pôle dans le disque D_γ . La matrice A est *singulière régulière* dans le disque D_∞ , s'il existe une matrice A_∞ telle que les matrices A et A_∞ sont E_p -équivalentes et la matrice zA_∞ n'a pas de pôle dans le disque D_∞ .

Remarque 3.5.16. Soient $A, B \in M_n(E_p)$. Supposons que A et B sont E_p -équivalentes. La matrice A est *singulière régulière* dans le disque D_γ si et seulement si la matrice B est *singulière régulière* dans le disque D_γ . En effet, si A est *singulière régulière* dans le disque D_γ alors il existe une matrice A_γ telle que A et A_γ sont E_p -équivalentes et il existe $\beta_\gamma \in D_\gamma$ tel que $(z - \beta_\gamma)A_\gamma$ n'a pas de pôle dans le disque D_γ . Comme A et B sont E_p -équivalentes alors par transitivité les matrices B et A_γ sont E_p -équivalentes. Par conséquent, la matrice B est *singulière régulière* dans le disque D_γ . Maintenant, si D_γ est un disque singulier régulier de B alors, en appliquant le même argument précédent on obtient que la matrice A est *singulière régulière* dans le disque D_γ .

Nous rappelons que pour un opérateur unitaire $\mathcal{L} \in E_p[d/dz]$ d'ordre n nous dénotons par $\mathcal{L}_\delta \in E_p[\delta]$ l'opérateur obtenu après avoir réécrit $z^n \mathcal{L}$ en fonction de δ . Nous notons par $L(z)$ la matrice compagnon de \mathcal{L} et par $L_\delta(z)$ la matrice compagnon de \mathcal{L}_δ .

Définition 3.5.17. Soit $f(z) \in 1 + z\mathbb{C}_p[[z]]$. Nous disons que $f(z)$ satisfait la propriété $(\mathbf{P})_{p,r,n}$ s'il existe un opérateur différentiel unitaire $\mathcal{L} \in E_p[d/dz]$, tel que :

1. L'opérateur \mathcal{L} est annulé par $f(z)$.
2. L'ordre de \mathcal{L} est n .
3. La matrice $L_\delta(z)$ appartient à \mathcal{M}_p .
4. L'opérateur \mathcal{L} est p -unipotent.
5. Tous les disques singuliers de la matrice $L(z)$ sont singuliers réguliers.
6. La matrice $L(z)$ a exactement r disques singuliers réguliers à *distance finie*.³

Lemme 3.5.18. Soit $f(z) \in 1 + z\mathbb{C}_p[[z]]$. Si $f(z)$ vérifie la propriété $(\mathbf{P})_{p,r,n}$ alors $\Lambda_p(f(z))$ vérifie aussi la propriété $(\mathbf{P})_{p,r,n}$.

2. Deux matrices $A, B \in M_n(E_p)$ sont E_p -équivalentes s'il existe $H \in Gl_n(E_p)$ telle que $\frac{d}{dz}H = AH - HB$. La relation de E_p -équivalence est une relation d'équivalence.

3. Le disque ouvert de centre $\gamma \in \mathbb{C}_p$ et de rayon 1 est à distance finie si la norme de γ est inférieure ou égale à 1.

En particulier, si $f(z) \in 1 + z\mathbb{C}_p[[z]]$ vérifie la propriété $(\mathbf{P})_{p,r,n}$ alors, pour tout entier k positif, la série $\Lambda_p^k(f(z))$ vérifie la propriété $(\mathbf{P})_{p,r,n}$.

Démonstration. Nous allons faire la démonstration en cinq pas.

Premier pas. Il existe un opérateur différentiel $\mathcal{L}_{1,\delta} \in E_{0,p}[\delta]$ d'ordre n qui est annulé par $\Lambda_p(f(z))$.

Écrivons $\mathcal{L}_\delta := \delta^n + e_1(z)\delta^{n-1} + \dots + e_{n-1}(z)\delta + e_n(z)$, où les $e_i(z) \in \mathbb{C}_p[[z]]$ pour $i \in \{1, \dots, n\}$ car les $e_i(z) \in E_{0,p}$. Par définition,

$$L_\delta(z) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ -e_n(z) & -e_{n-1}(z) & -e_{n-3}(z) & \dots & -e_2(z) & -e_1(z) \end{pmatrix}.$$

Les valeurs propres de $L_\delta(0)$ sont les racines du polynôme $X^n + e_1(0)X^{n-1} + \dots + e_{n-1}(0)X + e_n(0)$ mais, par hypothèse, les valeurs propres de $L_\delta(0)$ sont toutes égales à zéro, donc $e_i(0) = 0$. D'où

$$L_\delta(0) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

Soit $\delta f = (f(z), \delta f(z), \dots, \delta^{(n-1)}f(z))^t$. Comme par hypothèse $\mathcal{L}_\delta(f) = 0$ alors $\delta(\delta f) = L_\delta(z)\delta f$. D'après la remarque 3.5.14, une matrice fondamentale de solutions du système $\delta X = L_\delta(z)X$ est donnée par

$$Y_L X^{L_\delta(0)} = Y_L \cdot \begin{pmatrix} 1 & \text{Log}z & \frac{(\text{Log}z)^2}{2!} & \dots & \frac{(\text{Log}z)^{n-1}}{(n-1)!} \\ 0 & 1 & \text{Log}z & \dots & \frac{(\text{Log}z)^{n-2}}{(n-2)!} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \text{Log}z \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

où $Y_L \in Gl_n(\mathbb{C}_p[[z]])$ est telle que $Y_L(0)$ est la matrice identité. Alors, le système différentiel $\delta X = L_\delta(z)X$ a une unique solution dans $\mathbb{C}_p[[z]]^n$ à constante près⁴. Puisque $\delta f \in \mathbb{C}_p[[z]]^n$ est solution du système $\delta X = L_\delta(z)X$ et $f(0) = 1$ on obtient que la première colonne de la matrice Y_L est le vecteur δf . Comme $L_\delta(z)$ est dans \mathcal{M}_p , d'après le lemme 3.5.15, il existe $F(z)$ dans \mathcal{M}_p telle que les matrices $L_\delta(z)$ et $pF(z^p)$ sont équivalentes. De plus, il suit encore du lemme 3.5.15 que

$$F(z) = [\delta(\Lambda_p(Y_L)) + \frac{1}{p}\Lambda_p(Y_L)L_\delta(0)](\Lambda_p(Y_L))^{-1}, \quad (3.17)$$

où $\Lambda_p(Y_L)$ désigne la matrice obtenue après avoir appliqué Λ_p à chaque entrée de Y_L . Soit I_n la matrice identité de taille n . Notons que $\Lambda_p(Y_L)(0) = I_n$ car $Y_L(0) = I_n$ donc, d'après

4. Ici nous avons utilisé le fait que $\text{Log}z$ est transcendant sur $\mathbb{C}_p((z))$.

(3.17), on a

$$F(0) = \frac{1}{p}L_\delta(0) = \begin{pmatrix} 0 & \frac{1}{p} & 0 & \dots & 0 & 0 \\ 0 & 0 & \frac{1}{p} & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & \frac{1}{p} \\ 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}. \quad (3.18)$$

Considérons le produit

$$\Lambda_p(Y_L)X^{F(0)} = \Lambda_p(Y_L) \cdot \begin{pmatrix} 1 & \frac{\text{Log}z}{p} & \frac{1}{p^2} \frac{(\text{Log}z)^2}{2!} & \dots & \frac{1}{p^{n-1}} \frac{(\text{Log}z)^{n-1}}{(n-1)!} \\ 0 & 1 & \frac{1}{p} \text{Log}z & \dots & \frac{1}{p^{n-2}} \frac{(\text{Log}z)^{n-2}}{(n-2)!} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \frac{1}{p} \text{Log}z \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \quad (3.19)$$

Comme $\delta X^{F(0)} = F(0)X^{F(0)}$ alors, il suit de (3.17) et (3.18) que

$$\delta(\Lambda_p(Y_L)X^{F(0)}) = F(z)\Lambda_p(Y_L)X^{F(0)}.$$

Par conséquent, la matrice $\Lambda_p(Y_L)X^{F(0)}$ est une matrice fondamentale de solutions du système différentiel $\delta X = F(z)X$. Comme la première colonne de Y_L est donnée par le vecteur

$$\delta f = (f(z), \delta f(z), \dots, \delta^{(n-1)} f(z))^t$$

alors la première colonne de $\Lambda_p(Y_L)$ est le vecteur

$$\Lambda_p(\delta f) = (\Lambda_p(f(z)), \Lambda_p(\delta f(z)), \dots, \Lambda_p(\delta^{(n-1)} f(z)))^t.$$

Ainsi, $\Lambda_p(\delta f)$ est solution du système différentiel $\delta \vec{y} = F(z)\vec{y}$. Écrivons la matrice $F(z) = (a_{i,j}(z))_{1 \leq i,j \leq n}$, où les $a_{i,j}(z)$ appartiennent à $E_{0,p}$ car $F(z)$ est dans \mathcal{M}_p . Alors,

$$\begin{pmatrix} a_{1,1}(z) & a_{1,2}(z) & \dots & a_{1,n}(z) \\ a_{2,1}(z) & a_{2,2}(z) & \dots & a_{2,n}(z) \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}(z) & a_{n,2}(z) & \dots & a_{n,n}(z) \end{pmatrix} \begin{pmatrix} \Lambda_p(f(z)) \\ \Lambda_p(\delta f(z)) \\ \vdots \\ \Lambda_p(\delta^{(n-1)} f(z)) \end{pmatrix} = \begin{pmatrix} \delta(\Lambda_p(f(z))) \\ \delta(\Lambda_p(\delta f(z))) \\ \vdots \\ \delta(\Lambda_p(\delta^{(n-1)} f(z))) \end{pmatrix}.$$

Par conséquent,

$$\begin{aligned} & a_{n,1}(z)\Lambda_p(f(z)) + a_{n,2}(z)\Lambda_p(\delta f(z)) + \dots + \\ & + a_{n,n-1}(z)\Lambda_p(\delta^{n-2} f(z)) + a_{n,n}(z)\Lambda_p(\delta^{n-1} f(z)) = \delta(\Lambda_p(\delta^{n-1} f(z))). \end{aligned} \quad (3.20)$$

Mais $\Lambda_p(\delta^j f(z)) = p^j \delta^j \Lambda_p(f(z))$, alors $\Lambda_p(f(z))$ est solution de l'opérateur différentiel

$$\mathcal{L}_{1,\delta} = \delta^n - a_{n,n}(z)\delta^{n-1}(z) - \frac{a_{n,n-1}(z)}{p}\delta^{n-2} - \dots - \frac{a_{n,2}(z)}{p^{n-2}}\delta - \frac{a_{n,1}(z)}{p^{n-1}}.$$

Notons que $\mathcal{L}_{1,\delta}$ est à coefficients dans $E_{0,p}$ car $a_{n,n}(z), \dots, a_{n,1}(z) \in E_{0,p}$.

Deuxième pas. Soit $L_{1,\delta}(z)$ la matrice compagnon de $\mathcal{L}_{1,\delta}$. Alors $L_{1,\delta}(z)$ est dans \mathcal{M}_p . Par définition la matrice compagnon de $\mathcal{L}_{1,\delta}$ est

$$L_{1,\delta}(z) = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 1 \\ \frac{a_{n,1}(z)}{p^{n-1}} & \frac{a_{n,2}(z)}{p^{n-2}} & \frac{a_{n,3}(z)}{p^{n-3}} & \dots & \frac{a_{n,n-1}(z)}{p} & a_{n,n}(z) \end{pmatrix}$$

Comme $a_{n,1}(z), \dots, a_{n,n}(z)$ sont dans $E_{0,p}$ alors $L_{1,\delta}(z)$ est une matrice à coefficients dans $E_{0,p}$. D'après (3.18), $a_{n,1}(0) = \dots = a_{n,n}(0) = 0$ donc, toutes les valeurs propres de $L_{1,\delta}(0)$ sont égales à zéro et ainsi la matrice $L_{1,\delta}(z)$ satisfait la condition ii) de la définition 3.5.11. Il nous reste à voir que $L_{1,\delta}(z)$ vérifie la condition iii) de la définition 3.5.11. À la suite de la remarque 3.5.14 on a qu'une matrice fondamentale de solutions du système $\delta X = L_{1,\delta}(z)X$ est donnée par

$$Y_{L_1} X^{L_{1,\delta}(0)} = Y_{L_1} \cdot \begin{pmatrix} 1 & \text{Log}z & \frac{(\text{Log}z)^2}{2!} & \dots & \frac{(\text{Log}z)^{n-1}}{(n-1)!} \\ 0 & 1 & \text{Log}z & \dots & \frac{(\text{Log}z)^{n-2}}{(n-2)!} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \text{Log}z \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

où $Y_{L_1} \in Gl_n(\mathbb{C}_p[[z]])$ est telle que $Y_{L_1}(0)$ est la matrice identité. Écrivons la matrice $Y_{L_1} = (g_{i,j}(z))_{1 \leq i,j \leq n}$. Comme la matrice $L_{1,\delta}(z)$ est à coefficients dans $E_{0,p}$ et toutes les valeurs propres de $L_{1,\delta}(0)$ sont égales à zéro alors, d'après le théorème 2 de [24], pour montrer que $L_{1,\delta}(z)$ vérifie la condition iii) de la définition 3.5.11, il suffit de voir que le rayon de convergence des séries $g_{i,j}(z)$ est supérieur ou égal à 1. Écrivons $Y_L = (f_{i,j}(z))_{1 \leq i,j \leq n}$. On a déjà vu que $f_{i,1}(z) = \delta^{i-1}f(z)$ pour $i \in \{1, \dots, n\}$. Pour chaque $i \in \{1, \dots, n\}$, soit

$$\omega_i := \frac{\Lambda_p(f_{1,1}(z))(\text{Log}z)^{i-1}}{p^{i-1}(i-1)!} + \dots + \frac{\Lambda_p(f_{1,i}(z))\text{Log}z}{p} + \Lambda_p(f_{1,i}(z)).$$

Montrons que les ω_i sont solutions de l'opérateur différentiel $\mathcal{L}_{1,\delta}$. Nous allons d'abord montrer que pour tout $j \in \{1, \dots, n-1\}$ et tout $i \in \{1, \dots, n\}$, $f_{j+1,i} = f_{j,i-1} + \delta f_{j,i}$. En effet, pour chaque $i \in \{1, \dots, n\}$, considérons

$$F_i = f_{1,1} \frac{(\text{Log}z)^{i-1}}{(i-1)!} + f_{1,2} \frac{(\text{Log}z)^{i-2}}{(i-2)!} + \dots + f_{1,i-1} \text{Log}z + f_{1,i}.$$

Remarquons que F_i est l'entrée $(1, i)$ de la matrice $Y_L X^{L_\delta(0)}$. Soit $(h_{1,i}, \dots, h_{n,i})^t$ le vecteur qui représente la i -ième colonne de la matrice $Y_L X^{L_\delta(0)}$. Par conséquent,

$$\delta((h_{1,i}, \dots, h_{n,i})^t) = L_\delta(z)(h_{1,i}, \dots, h_{n,i})^t.$$

Ainsi, pour chaque $k \in \{1, \dots, n\}$, $h_{k,i} = \delta^{k-1}h_{1,i} = \delta^{k-1}F_i$. Donc,

$$Y_L \cdot \begin{pmatrix} 1 & \text{Log}z & \frac{(\text{Log}z)^2}{2!} & \dots & \frac{(\text{Log}z)^{n-1}}{(n-1)!} \\ 0 & 1 & \text{Log}z & \dots & \frac{(\text{Log}z)^{n-2}}{(n-2)!} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \text{Log}z \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} F_1 & \dots & F_n \\ \delta(F_1) & \dots & \delta(F_n) \\ \vdots & \vdots & \vdots \\ \delta^{n-1}(F_1) & \dots & \delta^{n-1}(F_n) \end{pmatrix}.$$

Soit $j \in \{1, \dots, n-1\}$ et $i \in \{1, \dots, n\}$ et montrons que $f_{j+1,i} = f_{j,i-1} + \delta f_{j,i}$. Il suit de la dernière égalité matricielle que,

$$\delta^{j-1}F_i = f_{j,1} \frac{(\text{Log}z)^{i-1}}{(i-1)!} + f_{j,2} \frac{(\text{Log}z)^{i-2}}{(i-2)!} + \dots + f_{j,i-1} \text{Log}z + f_{j,i}$$

et

$$\delta^j F_i = f_{j+1,1} \frac{(Logz)^{i-1}}{(i-1)!} + f_{j+1,2} \frac{(Logz)^{i-2}}{(i-2)!} + \cdots + f_{j+1,i-1} Logz + f_{j+1,i}.$$

Comme $\delta^j F_i = \delta(\delta^{j-1} F_i)$ et $Logz$ est transcendant sur $\mathbb{C}_p((z))$ alors, $f_{j+1,i} = f_{j,i-1} + \delta f_{j,i}$.

Maintenant soit $i \in \{1, \dots, n\}$ et montrons que par récurrence sur $j \in \{1, \dots, n\}$ on a

$$p^{j-1} \delta^{j-1} \omega_i = \frac{\Lambda_p(f_{j,1}(z))(Logz)^{i-1}}{p^{i-1}(i-1)!} + \cdots + \frac{\Lambda_p(f_{j,i-1}(z))Logz}{p} + \Lambda_p(f_{j,i}(z)).$$

Si $j = 1$, alors l'égalité découle toute de suite de la définition de ω_i . Maintenant supposons que l'égalité est vérifiée pour $j-1 \geq 0$. Montrons qu'elle l'est aussi pour j . Par hypothèse de récurrence on a

$$p^{j-1} \delta^{j-1} \omega_i = \frac{\Lambda_p(f_{j,1}(z))(Logz)^{i-1}}{p^{i-1}(i-1)!} + \cdots + \frac{\Lambda_p(f_{j,i-1}(z))Logz}{p} + \Lambda_p(f_{j,i}(z)).$$

Soit $k \in \{1, \dots, i-1\}$. Puisque $\Lambda_p \circ \delta = p\delta \circ \Lambda_p$ et $f_{j,k} + \delta f_{j,k+1} = f_{j+1,k+1}$ alors,

$$\begin{aligned} & \delta \left(\frac{\Lambda_p(f_{j,k})(Logz)^{i-k}}{p^{i-k}(i-k)!} + \frac{\Lambda_p(f_{j,k+1})(Logz)^{i-k-1}}{p^{i-k-1}(i-k-1)!} \right) \\ &= \frac{1}{p} \Lambda_p(\delta f_{j,k}) \frac{(Logz)^{i-k}}{p^{i-k}(i-k)!} + \frac{\Lambda_p(f_{j,k})(Logz)^{i-k-1}}{p^{i-k}(i-k-1)!} \\ &+ \frac{1}{p} \Lambda_p(\delta f_{j,k+1}) \frac{(Logz)^{i-k-1}}{p^{i-k-1}(i-k-1)!} + \frac{\Lambda_p(f_{j,k+1})(Logz)^{i-k-2}}{p^{i-k-1}(i-k-2)!} \\ &= \frac{\Lambda_p(\delta f_{j,k})(Logz)^{i-k}}{p^{i-k+1}(i-k)!} + \frac{[\Lambda_p(f_{j+1,k+1})](Logz)^{i-k-1}}{p^{i-k}(i-k-1)!} + \frac{\Lambda_p(f_{j,k+1})(Logz)^{i-k-2}}{p^{i-k-1}(i-k-2)!}. \end{aligned}$$

Par conséquent,

$$\delta(p^{j-1} \delta^{j-1} \omega_i) = \frac{\Lambda_p(f_{j+1,1}(z))(Logz)^{i-1}}{p^{i-2}(i-1)!} + \cdots + \frac{\Lambda_p(f_{j+1,i-1}(z))Logz}{p^2} + \frac{\Lambda_p(f_{j+1,i}(z))}{p}.$$

D'où,

$$p^j \delta^j \omega_i = \frac{\Lambda_p(f_{j+1,1}(z))(Logz)^{i-1}}{p^{i-1}(i-1)!} + \cdots + \frac{\Lambda_p(f_{j+1,i-1}(z))Logz}{p} + \Lambda_p(f_{j+1,i}(z)).$$

Maintenant, si $(\tau_{j,i}(z))_{1 \leq j, i \leq n} = \Lambda_p(Y_L) X^{F(0)}$ alors de (3.19) on a que

$$\tau_{j,i}(z) = \frac{\Lambda_p(f_{j,1}(z))(Logz)^{i-1}}{p^{i-1}(i-1)!} + \cdots + \frac{\Lambda_p(f_{j,i-1}(z))Logz}{p} + \Lambda_p(f_{j,i}(z)).$$

D'où, $\tau_{j,i}(z) = p^{j-1} \delta^{j-1} \omega_i$ et ainsi,

$$\Lambda_p(Y_L) X^{F(0)} = \begin{pmatrix} \omega_1 & \cdots & \omega_i & \cdots & \omega_n \\ p\delta\omega_1 & \cdots & p\delta\omega_i & \cdots & p\delta\omega_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p^{n-2}\delta^{n-2}\omega_1 & \cdots & p^{n-2}\delta^{n-2}\omega_i & \cdots & p^{n-2}\delta^{n-2}\omega_n \\ p^{n-1}\delta^{n-1}\omega_1 & \cdots & p^{n-1}\delta^{n-1}\omega_i & \cdots & p^{n-1}\delta^{n-1}\omega_n \end{pmatrix}.$$

D'après le premier pas, on a $\delta(\Lambda_p(Y_L)X^{F(0)}) = F(z)\Lambda_p(Y_L)X^{F(0)}$. Rappelons que $F(z) = (a_{i,j}(z))_{1 \leq i,j \leq n}$. Alors, pour tout $i \in \{1, \dots, n\}$,

$$\begin{pmatrix} \delta(\omega_i) \\ \delta(p\delta\omega_i) \\ \vdots \\ \delta(p^{n-1}\delta^{n-1}\omega_i) \end{pmatrix} = \begin{pmatrix} a_{1,1}(z) & a_{1,2}(z) & \cdots & a_{1,n}(z) \\ a_{2,1}(z) & a_{2,2}(z) & \cdots & a_{2,n}(z) \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}(z) & a_{n,2}(z) & \cdots & a_{n,n}(z) \end{pmatrix} \begin{pmatrix} \omega_i \\ p\delta\omega_i \\ \vdots \\ p^{n-1}\delta^{n-1}\omega_i \end{pmatrix}.$$

Ainsi,

$$\delta^n \omega_i = \frac{a_{n,1}(z)\omega_i}{p^{n-1}} + \frac{a_{n,2}(z)\delta\omega_i}{p^{n-2}} + \cdots + \frac{a_{n,n-1}(z)\delta^{n-2}\omega_i}{p} + a_{n,n}(z)\delta^{n-1}\omega_i.$$

Par conséquent, les ω_i sont solutions de $\mathcal{L}_{1,\delta}$.

Notons que la famille $\{\omega_i\}_{1 \leq i \leq n}$ est linéairement indépendante sur \mathbb{C}_p . Pour cette raison la matrice

$$\omega = \begin{pmatrix} \omega_1 & \cdots & \omega_n \\ \delta(\omega_1) & \cdots & \delta(\omega_n) \\ \vdots & \vdots & \vdots \\ \delta^{n-1}(\omega_1) & \cdots & \delta^{n-1}(\omega_n) \end{pmatrix}$$

est une matrice fondamentale de solutions du système différentiel $\delta X = L_{1,\delta}(z)X$. Par hypothèse $L_\delta(z)$ est dans \mathcal{M}_p alors, d'après le théorème 2 de [24], le rayon de convergence des séries $f_{i,j}(z)$ est supérieur ou égal à 1 pour $i, j \in \{1, \dots, n\}$. Comme la norme est ultramétrique alors le rayon de convergence des séries $\Lambda_p(f_{i,j}(z))$ est supérieur ou égal à 1. Finalement, comme $Y_{L_1}X^{L_{1,\delta}(0)}$ et ω sont deux matrices fondamentales de solutions du système différentiel $\delta X = L_{1,\delta}(z)X$ et $\text{Log}z$ est transcendant sur $\mathbb{C}_p[[z]]$ alors, pour tout $i, j \in \{1, \dots, n\}$ on peut écrire $g_{i,j}(z)$ comme une combinaison linéaire des séries $\Lambda_p(f_{i,j}(z))$ sur \mathbb{C}_p . Raison pour laquelle le rayon de convergence des séries $g_{i,j}(z)$ est supérieur ou égal à 1.

Troisième pas. *L'opérateur différentiel $\mathcal{L}_1 \in E_p[d/dz]$ est p -unipotent.* Nous rappelons que \mathcal{L}_1 est l'opérateur différentiel obtenu après avoir réécrit $\frac{1}{z^n}\mathcal{L}_{1,\delta}$ en termes de d/dz . Comme la matrice $L_{1,\delta}(z)$ vérifie la condition iii) de la définition 5.11 alors il existe une matrice inversible \widehat{U} dont les coefficients sont analytiques dans le disque générique ouvert $D(z, 1)$, telle que $\delta\widehat{U} = L_{1,\delta}(z)\widehat{U}$. Pour chaque $i \in \{1, \dots, n\}$, soit F_i l'entrée $(1, i)$ de \widehat{U} . Donc, F_i est solution de $\mathcal{L}_{1,\delta}$ et la i -ième colonne de la matrice \widehat{U} est le vecteur $\delta F_i = (F_i, \delta F_i, \dots, \delta^{n-1}F_i)^t$. Maintenant soit $\mathbf{d}F_i = (F_i, \frac{d}{dz}F_i, \dots, \frac{d^{n-1}}{dz^{n-1}}F_i)^t$. Donc, $G_n\delta F_i = \mathbf{d}F_i$ où G_n est la matrice construite dans la proposition 3.2.1. Remarquons que F_i est solution de l'opérateur \mathcal{L}_1 car F_i est solution de l'opérateur différentiel $\mathcal{L}_{1,\delta}$ et $\mathcal{L}_{1,\delta}$ est obtenu après avoir réécrit $z^n\mathcal{L}_1$ en fonction de δ . Par conséquent, $\frac{d}{dz}(\mathbf{d}F_i) = L_1(z)\mathbf{d}F_i$. Ainsi, $\frac{d}{dz}(G_n\widehat{U}) = L_1(z)G_n\widehat{U}$. Posons $U = G_n\widehat{U}$. Donc, U est inversible à coefficients analytiques dans le disque générique ouvert $D(z, 1)$ et $\frac{d}{dz}U = L_1(z)U$. Grâce au théorème de Frobenius–Dwork (voir [22, Proposition 8.1]), on obtient que les normes des coefficients de l'opérateur différentiel \mathcal{L}_1 sont inférieures ou égales à 1. Autrement dit, \mathcal{L}_1 est à coefficients dans ϑ_{E_p} . Notons $\mathcal{L}_{1,p}$ l'opérateur obtenu après avoir réduit chaque coefficient de \mathcal{L}_1 modulo l'idéal maximal \mathfrak{m}_p de ϑ_{E_p} . Le rayon de convergence de \mathcal{L}_1 au point générique est égal à 1 car $\frac{d}{dz}U = L_1(z)U$ et U est une matrice inversible dont les coefficients sont analytiques dans le disque générique ouvert $D(z, 1)$. Il suit alors de la proposition 5.1 de [42, Chap III] que

$\mathcal{L}_{1,p}$ est nilpotent⁵. Donc, d'après la proposition de [50, Appendix] et le théorème 1 de [50, p.177], l'opérateur $\mathcal{L}_{1,p}$ est fuchsien. Finalement, montrons que les exposants en zéro de $\mathcal{L}_{1,p}$ sont tous égaux à zéro. Rappelons que $\mathcal{L}_{1,\delta} = \delta^n - a_{n,n}(z)\delta^{n-1}(z) - \frac{a_{n,n-1}(z)}{p}\delta^{n-2} - \dots - \frac{a_{n,2}(z)}{p^{n-2}}\delta - \frac{a_{n,1}(z)}{p^{n-1}}$. D'après l'équation (3.7),

$$\left(\frac{-a_{n,1}(z)}{p^{n-1}}, \dots, -a_{n,n}(z), 1 \right) = (c_n(z), c_{n-1}(z), \dots, c_1(z), 1)z^n G_{n+1},$$

où $\mathcal{L}_1(z) = \frac{d}{dz^n} + c_1(z)\frac{d}{dz^{n-1}} + \dots + c_{n-1}(z)\frac{d}{dz} + c_n(z)$. On a montré que $\mathcal{L}_1(z)$ est à coefficients dans ϑ_{E_p} . Puisque \mathbb{C}_p est un corps de caractéristique zéro alors $G_{n+1} \in Gl_n(\mathbb{Z}[1/z])$. Ainsi, chaque coefficient de G_{n+1} appartient à ϑ_{E_p} . D'où, $-\frac{a_{n,1}(z)}{p^{n-1}}, -\frac{a_{n,2}(z)}{p^{n-2}}, \dots, -a_{n,n}(z)$ appartiennent à ϑ_{E_p} . Notamment, pour chaque $i \in \{1, \dots, n\}$, $-\frac{a_i(0)}{p^{n-i}}$ appartient à $\vartheta_{\mathbb{C}_p}$. Ainsi, les exposants de $\mathcal{L}_{1,p}$ en zéro sont les racines du polynôme indiciel

$$X^n - (a_{n,n}(0) \pmod{\mathfrak{n}_p})X^{n-1} - \dots - \frac{a_{n,1}(0)}{p^{n-1}} \pmod{\mathfrak{n}_p},$$

où \mathfrak{n}_p est l'idéal maximal de $\vartheta_{\mathbb{C}_p}$. Mais on a vu dans le deuxième pas que $a_{n,n}(0) = \dots = a_{n,1}(0) = 0$, d'où le polynôme indiciel est égal à X^n . Par conséquent, les exposants en zéro sont tous égaux à zéro. Ainsi, l'opérateur $\mathcal{L}_{1,p}$ est MOM en zéro. Il suit donc que \mathcal{L}_1 est p -unipotent.

Quatrième pas. Les matrices $L_\delta(z)$ et $pL_{1,\delta}(z^p)$ sont équivalentes. On veut montrer qu'il existe une matrice $T(z)$ inversible à coefficients dans $E_{0,p}$ telle que $T(z)^{-1}$ est à coefficients dans $E_{0,p}$ et $\delta T(z) = pL_{1,\delta}(z^p)T(z) - T(z)L_\delta(z)$. On a montré dans le deuxième pas que la matrice ω est une matrice fondamentale de solutions du système $\delta X = L_{1,\delta}(z)X$.

Pour $i, j \in \{1, \dots, n\}$ nous rappelons la formule

$$p^{j-1}\delta^{j-1}\omega_i = \frac{\Lambda_p(f_{j,1}(z))(Logz)^{i-1}}{p^{i-1}(i-1)!} + \dots + \frac{\Lambda_p(f_{j,i-1}(z))Logz}{p} + \Lambda_p(f_{j,i}(z)).$$

Ainsi, $\omega(z) = A(z)X^{\frac{1}{p}L_{1,\delta}(0)}$, où

$$A(z) = \begin{pmatrix} \Lambda_p(f_{1,1}(z)) & \dots & \Lambda_p(f_{1,n}(z)) \\ \frac{\Lambda_p(f_{2,1}(z))}{p} & \dots & \frac{\Lambda_p(f_{2,n}(z))}{p} \\ \vdots & \vdots & \vdots \\ \frac{\Lambda_p(f_{n-1,1}(z))}{p^{n-2}} & \dots & \frac{\Lambda_p(f_{n-1,n}(z))}{p^{n-2}} \\ \frac{\Lambda_p(f_{n,1}(z))}{p^{n-1}} & \dots & \frac{\Lambda_p(f_{n,n}(z))}{p^{n-1}} \end{pmatrix}.$$

D'après la remarque 3.5.14, $\delta(X^{\frac{1}{p}L_{1,\delta}(0)}) = \frac{1}{p}L_{1,\delta}(0)X^{\frac{1}{p}L_{1,\delta}(0)}$ et comme

$$\delta(A(z)X^{\frac{1}{p}L_{1,\delta}(0)}) = L_{1,\delta}(z)A(z)X^{\frac{1}{p}L_{1,\delta}(0)}$$

alors $\delta(A(z)) + A(z)\frac{1}{p}L_{1,\delta}(0) = L_{1,\delta}(z)A(z)$. Montrons que $A(z^p)X^{L_{1,\delta}(0)}$ est solution du système $\delta X = pL_{1,\delta}(z^p)X$. En effet,

$$\begin{aligned} \delta(A(z^p)X^{L_{1,\delta}(0)}) &= p[(\delta(A))(z^p) + A(z^p)\frac{1}{p}L_{1,\delta}(0)]X^{L_{1,\delta}(0)} \\ &= pL_{1,\delta}(z^p)A(z^p)X^{L_{1,\delta}(0)}. \end{aligned}$$

5. Un opérateur différentiel \mathcal{D}_p à coefficients dans $k(z)$, k un cors fini de caractéristique p , est nilpotent si la p -courbure de \mathcal{D}_p est nilpotente.

Donc, la matrice $A(z^p)X^{L_{1,\delta}(0)}$ est une matrice fondamentale de solutions du système $\delta X = pL_{1,\delta}(z^p)X$. D'autre part, la matrice $Y_L X^{L_\delta(0)}$ est une matrice fondamentale de solutions de $\delta X = L_\delta(z)X$. Par conséquent, si l'on pose $T(z) = (A(z^p)X^{L_{1,\delta}(0)})(Y_L X^{L_\delta(0)})^{-1}$ alors $\delta T(z) = pL_{1,\delta}(z^p)T(z) - T(z)L_\delta(z)$. En conséquence, il suffit de montrer que $T(z)$ est une matrice inversible à coefficients dans $E_{0,p}$ telle que $T(z)^{-1}$ est à coefficients dans $E_{0,p}$. Notons d'abord que $T(z) = A(z^p)Y_L^{-1}$ car $L_{1,\delta}(0) = L_\delta(0)$. Nous allons montrer que ce dernier produit est à coefficients dans $E_{0,p}$. Comme $L_\delta(z) \in \mathcal{M}_p$, il suit du lemme 3.5.15 qu'il existe une matrice $H(z)$ inversible telle que $H(z)$ et $H^{-1}(z)$ sont à coefficients dans $E_{0,p}$, $H(0) = I_n$ et $\delta H(z) = pF(z^p)H(z) - H(z)L_\delta(z)$, où $F(z)$ est la matrice définie dans (3.17). On a montré dans le premier pas que $\Lambda_p(Y_L)X^{F(0)}$ est une matrice fondamentale de solutions du système $\delta X = F(z)X$. Donc la matrice $(\Lambda_p(Y_L))(z^p)X^{pF(0)}$ est une matrice fondamentale de solutions du système $\delta X = pF(z^p)X$. Il suit de (3.18) que $pF(0) = L_{1,\delta}(0)$. Par conséquent, la matrice $(\Lambda_p(Y_L))(z^p)X^{L_\delta(0)}$ est une matrice fondamentale de solutions de $\delta X = pF(z^p)X$. Notons que la matrice $(\Lambda_p(Y_L))(z^p)X^{L_\delta(0)}$ est égale à

$$\begin{pmatrix} (\Lambda_p(f_{1,1}))(z^p) & \dots & (\Lambda_p(f_{1,n}))(z^p) \\ (\Lambda_p(f_{2,1}))(z^p) & \dots & (\Lambda_p(f_{2,n}))(z^p) \\ \vdots & \vdots & \vdots \\ (\Lambda_p(f_{n-1,1}))(z^p) & \dots & (\Lambda_p(f_{n-1,n}))(z^p) \\ (\Lambda_p(f_{n,1}))(z^p) & \dots & (\Lambda_p(f_{n,n}))(z^p) \end{pmatrix} \begin{pmatrix} 1 & \text{Log}z & \frac{(\text{Log}z)^2}{2!} & \dots & \frac{(\text{Log}z)^{n-1}}{(n-1)!} \\ 0 & 1 & \text{Log}z & \dots & \frac{(\text{Log}z)^{n-2}}{(n-2)!} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \text{Log}z \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Puisque $Y_L X^{L_\delta(0)}$ est une matrice fondamentale de solutions du système $\delta X = L_\delta(z)X$ alors, l'expression $\delta H(z) = pF(z^p)H(z) - H(z)L_\delta(z)$ entraîne que, $HY_L X^{L_\delta(0)}$ est une matrice fondamentale de solutions du système $\delta X = pF(z^p)X$. Ainsi, les matrices $HY_L X^{L_\delta(0)}$ et $(\Lambda_p(Y_L))(z^p)X^{L_\delta(0)}$ sont deux matrices fondamentales de solutions du système $\delta X = pF(z^p)X$. D'où il existe une matrice $C \in Gl_n(\mathbb{C}_p)$ telle que

$$H(z)Y_L X^{L_\delta(0)} = (\Lambda_p(Y_L))(z^p)X^{L_\delta(0)}C.$$

Ainsi, $(\Lambda_p(Y_L))(z^p)^{-1}H(z)Y_L = X^{L_\delta(0)}C(X^{L_\delta(0)})^{-1}$. Comme Y_L , $\Lambda_p(Y_L)$ et H appartiennent à $Gl_n(\mathbb{C}_p[[z]])$ et $H(0) = Y_L(0) = (\Lambda_p(Y_L))(0) = I_n$ alors $X^{L_\delta(0)}C(X^{L_\delta(0)})^{-1} = I_n$. Ainsi $H(z) = (\Lambda_p(Y_L))(z^p)Y_L^{-1}$. Donc,

$$H(z) = \begin{pmatrix} (\Lambda_p(f_{1,1}))(z^p) & \dots & (\Lambda_p(f_{1,n}))(z^p) \\ (\Lambda_p(f_{2,1}))(z^p) & \dots & (\Lambda_p(f_{2,n}))(z^p) \\ \vdots & \vdots & \vdots \\ (\Lambda_p(f_{n-1,1}))(z^p) & \dots & (\Lambda_p(f_{n-1,n}))(z^p) \\ (\Lambda_p(f_{n,1}))(z^p) & \dots & (\Lambda_p(f_{n,n}))(z^p) \end{pmatrix} Y_L^{-1}.$$

Alors,

$$\begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1/p & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \dots & 1/p^{n-2} & 0 \\ 0 & 0 & \dots & 0 & 1/p^{n-1} \end{pmatrix} H(z) = A(z^p)Y_L^{-1} = T(z).$$

Comme la matrice $H(z) \in Gl_n(E_{0,p})$ alors $T(z) \in Gl_n(E_{0,p})$. Par conséquent, les matrices $pL_{1,\delta}(z^p)$ et $L_\delta(z)$ sont équivalentes.

Cinquième pas. *Les disques singuliers de $L_1(z)$ sont singuliers réguliers et $L_1(z)$ a exactement r disques singuliers réguliers à distance finie.* Nous rappelons que $L_1(z)$ est la

matrice compagnon de \mathcal{L}_1 et que \mathcal{L}_1 est l'opérateur différentiel obtenu après avoir réécrit $\frac{1}{z^n}\mathcal{L}_{1,\delta}$ en termes de d/dz . Soit G_n la matrice construite dans la proposition 3.2.1. Montrons d'abord que les matrices $\frac{p}{z}L_{1,\delta}(z^p)$ et $pz^{p-1}L_1(z^p)$ sont E_p -équivalentes. Soit g une solution quelconque de \mathcal{L}_1 . On pose $(\mathbf{d}g) = (g, g', \dots, g^{(n-1)})^t$ et $(\delta g) = (g, \delta g, \dots, \delta^{(n-1)}g)^t$. Alors, $\frac{d}{dz}(\mathbf{d}g) = L_1(z)(\mathbf{d}g)$ et $\delta(\delta g) = L_{1,\delta}(\delta g)$. D'après la construction de la matrice G_n , nous avons que $(\mathbf{d}g) = G_n(\delta g)$. En appliquant d/dz à cette dernière égalité, on a que

$$L_1(z)(\mathbf{d}g) = \left(\frac{d}{dz}G_n\right)(\delta g) + G_n\frac{d}{dz}(\delta g) = \left(\frac{d}{dz}G_n\right)(\delta g) + G_n\frac{1}{z}\delta(\delta g).$$

Mais $(\mathbf{d}g) = G_n(\delta g)$ et $\delta(\delta g) = L_1(z)(\delta g)$. Donc,

$$L_1(z)G_n(\delta g) = \left(\frac{d}{dz}G_n\right)(\delta g) + G_n\frac{1}{z}L_{1,\delta}(\delta g).$$

Finalement, comme g est une solution quelconque de \mathcal{L}_1 et l'espace de solutions de \mathcal{L}_1 est de dimension n sur \mathbb{C}_p , on obtient que $L_1(z)G_n = \frac{d}{dz}G_n + G_n\frac{1}{z}L_{1,\delta}$. Par conséquent, $d/dz(G_n(z^p)) = pz^{p-1}L_1(z^p)G_n(z^p) - G_n(z^p)\frac{p}{z}L_{1,\delta}(z^p)$. Ainsi, la matrice $\frac{p}{z}L_{1,\delta}(z^p)$ et E_p -équivalente à la matrice $pz^{p-1}L_1(z^p)$. Le quatrième pas entraîne que $\frac{1}{z}L_\delta(z)$ est E_p -équivalente à $\frac{p}{z}L_{1,\delta}(z^p)$. Alors, par transitivité la matrice $\frac{1}{z}L_\delta(z)$ est E_p -équivalente à $pz^{p-1}L_1(z^p)$. Rappelons que $L(z)$ est la matrice compagnon de \mathcal{L} . En appliquant le même argument précédent on a que, $d/dzG_n = L(z)G_n(z) - G_n\frac{1}{z}L_\delta(z)$. Donc, les matrices $\frac{1}{z}L_\delta(z)$ et $L(z)$ sont E_p -équivalentes. Ainsi par transitivité, les matrices $pz^{p-1}L_1(z^p)$ et $L(z)$ sont E_p -équivalentes. Par hypothèse tous les disques singuliers de $L(z)$ sont singuliers réguliers et $L(z)$ a exactement r disques singuliers réguliers à distance finie. Comme $L(z)$ est E_p équivalente à $pz^{p-1}L_1(z^p)$ alors il suit de la remarque 3.5.16 que tous les disques singuliers de la matrice $pz^{p-1}L_1(z^p)$ sont singuliers réguliers et que cette matrice a exactement r disques singuliers à distance finie.

Comme on l'a déjà montré dans le troisième pas, il existe une matrice inversible U , dont les coefficients sont analytiques dans le disque générique ouvert $D(z, 1)$, telle que $\frac{d}{dz}U = L_1(z)U$. Donc, il découle du corollaire 6.4.2 et de la propositions 6.4.6 de [23] que, D_γ est un disque singulier régulier de $L_1(z)$ si et seulement si D_γ est un disque singulier régulier de $pz^{p-1}L_1(z^p)$. Comme on l'a vu tous les disques singuliers de $pz^{p-1}L_1(z^p)$ sont singuliers réguliers et cette matrice a exactement r disques singuliers à distance finie. Par conséquent, les disques singuliers de la matrice $L_1(z)$ sont singuliers réguliers et $L_1(z)$ a exactement r disques singuliers à distance finie.

Pour finir la démonstration du lemme 3.5.18, montrons que l'opérateur \mathcal{L}_1 obtenu après avoir réécrit $1/z^n\mathcal{L}_{1,\delta}$ en termes de d/dz vérifie les conditions 1-6 de la définition 3.5.17. Il suit du premier pas que l'opérateur \mathcal{L}_1 est d'ordre n et annulé par $\Lambda_p(f(z))$. D'après le deuxième pas, la matrice compagnon de $\mathcal{L}_{1,\delta}$ est dans \mathcal{M}_p . Il découle du troisième pas que l'opérateur \mathcal{L}_1 est p -unipotent et finalement du cinquième pas que, tous les disques singuliers de $L_1(z)$ sont singuliers réguliers et $L_1(z)$ a exactement r disques singuliers réguliers à distance finie. \square

Lemme 3.5.19. *Soient $\mathcal{L} \in \vartheta_{E_p}[d/dz]$ un opérateur différentiel unitaire et $L(z)$ sa matrice compagnon. Si $L(z)$ a exactement r disques singuliers à distance finie alors le nombre de singularités de l'opérateur \mathcal{L}_p dans $\overline{\mathbb{F}_p}$ est inférieur ou égal à r .*

Démonstration. Soient $D_{\gamma_1}, \dots, D_{\gamma_r}$ les disques singuliers de $L(z)$. Par hypothèse ils sont tous différents, d'où pour $i \neq j$ on a que $|\gamma_i - \gamma_j| = 1$, ce qui revient à dire que $\overline{\gamma_i} \neq \overline{\gamma_j}$. Montrons que les singularités de \mathcal{L}_p appartiennent à $\{\overline{\gamma_1}, \dots, \overline{\gamma_r}\}$. Soit $A_i(z)$ un des

coefficients de \mathcal{L} alors les pôles de $A_i(z)$ sont dans $D_{\gamma_1} \cup \dots \cup D_{\gamma_r}$. Par conséquent, d'après le théorème de Mittag-Leffler, les pôles de $\overline{A_i(z)}$ appartiennent à $\{\overline{\gamma_1}, \dots, \overline{\gamma_r}\}$. D'où les pôles de \mathcal{L}_p sont dans $\{\overline{\gamma_1}, \dots, \overline{\gamma_r}\}$. \square

Construction de l'ensemble \mathcal{S}'

Soit \mathcal{S} un ensemble infini de nombres premiers et soient $f(z) \in \mathcal{F}(\mathcal{S})$, n l'ordre de \mathcal{M}_f et r le nombre de singularités à distance finie de \mathcal{M}_f dans $\overline{\mathbb{Q}}$. Dans cette partie nous allons construire un ensemble $\mathcal{S}' \subset \mathcal{S}$ tel que : l'ensemble $\mathcal{S} \setminus \mathcal{S}'$ est fini et pour tout $p \in \mathcal{S}'$, la série $f(z)$ vérifie la propriété $(\mathbf{P})_{p,r,n}$. Dans ce qui suit nous fixons l'ensemble \mathcal{S} , la série $f(z) \in \mathcal{F}(\mathcal{S})$ et les entiers n et r . Soient $\gamma_1, \dots, \gamma_r$ les singularités à distance finie de \mathcal{M}_f dans $\overline{\mathbb{Q}}$ et écrivons $\mathcal{M}_f = \frac{d^n}{dz^n} + a_1(z)\frac{d^{n-1}}{dz^{n-1}} + \dots + a_{n-1}(z)\frac{d}{dz} + a_n(z) \in \mathbb{Q}(z)[d/dz]$. Soit $d = \prod_{i \neq j} (\gamma_i - \gamma_j)$. Alors d est un nombre algébrique différent de zéro. Nous posons $B_{\mathcal{S}}$ comme l'ensemble des nombres premiers p contenu dans \mathcal{S} tel que la norme p -adique de γ_i pour tout $\gamma_i \neq 0$ est égale à 1, la norme de Gauss des $a_i(z)$ est inférieure ou égale à 1 et la norme p -adique de d est égale à 1. Notons que $\mathcal{S} \setminus B_{\mathcal{S}}$ est fini.

Lemme 3.5.20. *Si $f(z)$ annule un opérateur différentiel MOM en zéro à coefficient dans $\mathbb{Q}(z)$ alors l'opérateur différentiel \mathcal{M}_f est MOM en zéro.*

Démonstration. Supposons que $f(z) \in \mathbb{Q}[[z]]$ annule l'opérateur différentiel \mathcal{D} à coefficients dans $\mathbb{Q}(z)$ qui est MOM en zéro. Comme \mathcal{M}_f est l'opérateur minimal de $f(z)$ alors $\mathcal{D} = \mathcal{T}\mathcal{M}_f$, où \mathcal{T} est un opérateur différentiel à coefficients dans $\mathbb{Q}(z)$. Pour montrer que \mathcal{M}_f est MOM en zéro nous devons montrer que \mathcal{M}_f est fuchsien, zéro est un point singulier et les exposants de \mathcal{M}_f en zéro sont tous égaux à zéro. En effet, supposons que α est une singularité de \mathcal{M}_f . Sans perdre en généralité, supposons que $\alpha = 0$. Comme \mathcal{D} est fuchsien alors, d'après la proposition 1.4.2 de [67], \mathcal{D} a une base de solutions dans l'anneau $\mathbb{C}\{\{z\}\}[z^\beta, \text{Log}(z) : \beta \in \mathbb{C}]$, où $\mathbb{C}\{\{z\}\}$ est l'anneau des séries au voisinages de 0 qui sont convergentes et z^β désigne la solution de l'opérateur différentiel $\delta - \beta$. Par conséquent, \mathcal{M}_f a une base de solutions dans l'anneau $\mathbb{C}\{\{z\}\}[z^\beta, \text{Log}(z) : \beta \in \mathbb{C}]$ car $\mathcal{D} = \mathcal{T}\mathcal{M}_f$. Il découle donc de la proposition 1.4.2 de [67] que, le point 0 est un point singulier régulier de \mathcal{M}_f . Par conséquent, l'opérateur \mathcal{M}_f est fuchsien. Maintenant, comme \mathcal{D} est MOM en zéro alors zéro est un point singulier régulier de \mathcal{D} . En appliquant l'argument précédent on obtient donc que \mathcal{M}_f a une base de solutions dans l'anneau $\mathbb{C}\{\{z\}\}[z^\beta, \text{Log}(z) : \beta \in \mathbb{C}]$. Par conséquent, d'après la proposition 1.4.2 de [67], le point 0 est un point singulier régulier de \mathcal{M}_f . Soit $\mathcal{M}_{f,\delta}$ l'opérateur obtenu après avoir réécrit $z^n \mathcal{M}_f$ en fonction de δ . Écrivons

$$\mathcal{M}_{f,\delta} = \delta^n + b_1(z)\delta^{n-1} + \dots + n_{n-1}(z)\delta + b_n(z),$$

où les $b_i(z)$ appartiennent à $\mathbb{C}(z) \cap \mathbb{C}[[z]]$ car zéro est un point singulier régulier de \mathcal{M}_f et n est l'ordre de \mathcal{M}_f . Rappelons que les exposants de \mathcal{M}_f en zéro sont les racines du polynôme $X^n + b_1(0)X^{n-1} + \dots + b_{n-1}(0)X + b_n(0)$. Donc, pour montrer que les exposants de \mathcal{M}_f en zéro sont tous égaux à zéro il faut montrer que $b_i(0) = 0$ pour tout $i \in \{1, \dots, n\}$. Soit $\{\rho_1, \dots, \rho_n\}$ l'ensemble des exposants de \mathcal{M}_f en zéro. Partitionnons l'ensemble $\{\rho_1, \dots, \rho_n\}$ avec des ensembles E_1, \dots, E_r tels que les éléments de E_j sont égaux modulo \mathbb{Z} mais, pour tous $j \neq k$, si $x \in E_j$ et $y \in E_k$ alors $x \neq y \pmod{\mathbb{Z}}$. Notons e_j l'élément le plus petit de E_j . Alors, il suit de l'équation (6.2) de [59] que, pour tout $i \in \{1, \dots, r\}$, il existe $h_i(z) \in \mathbb{C}[[z]]$ telle que $z^{e_i} h_i(z)$ est solution de \mathcal{M}_f et en conséquence solution de \mathcal{D} . Donc, e_i est un exposant de \mathcal{D} en zéro. D'où $e_i = 0$ pour tout $i \in \{1, \dots, r\}$ car tous les exposants de \mathcal{D} en zéro sont égaux à zéro. Ainsi, l'ensemble $\{\rho_1, \dots, \rho_n\}$ modulo \mathbb{Z} est égal à $\{0\}$. Donc, il

suit des égalités (6.2) et (6.3) de [59] qu'il existe $f_1, \dots, f_n \in \mathbb{C}[[z]]$ telles que pour chaque $j \in \{1, \dots, n\}$,

$$g_j = f_1(z) \frac{(\text{Log}z)^{j-1}}{(j-1)!} + f_2(z) \frac{(\text{Log}z)^{j-2}}{(j-2)!} + \dots + f_{j-1}(z) \text{Log}z + f_j(z)$$

est solution de \mathcal{M}_f . Par conséquent, pour chaque $j \in \{1, \dots, m\}$, g_j est solution de $\mathcal{M}_{f,\delta}$. Écrivons $f_1(z) = z^m g(z)$, où $g(0) \neq 0$. Comme $f_1(z)$ est solution de \mathcal{D} alors m est un exposant de \mathcal{D} en zéro. Donc, $m = 0$ et ainsi, $f_1(0) \neq 0$. Montrons par récurrence sur $j \in \{0, \dots, n-1\}$ que $b_{n-j}(0) = 0$. Notons que par définition $e_j \in \{\rho_1, \dots, \rho_n\}$ et on a montré que $e_j = 0$. Donc, 0 est un exposant de \mathcal{M}_f en zéro et par conséquent, $b_n(0) = 0$. Maintenant supposons que $b_n(0) = \dots = b_{n-j+2}(0) = 0$. Montrons que $b_{n-j+1}(0) = 0$. Soit $k \in \mathbb{N}$. On note par $(\delta^k g_j)_0(z)$ la série telle que $\delta^k g_j - (\delta^k g_j)_0(z) \in (\text{Log}z)\mathbb{C}[[z, \text{Log}z]]$. Montrons que pour tout $j \geq 2$, $(\delta^{j-1} g_j)_0(z) - f_1(z) \in z\mathbb{C}[[z]]$ et que pour tout $k \geq j$, $(\delta^k g_j)_0(0) = 0$. Soit $i, r \in \{1, \dots, n\}$. Montrons d'abord par récurrence sur $k \in \mathbb{N}$ que, $\delta^k (f_i \frac{(\text{Log}z)^r}{r!}) = \sum_{s=0}^r \binom{k}{s} (\delta^{k-s} f_i) \frac{(\text{Log}z)^{r-s}}{(r-s)!}$. Il est clair qu'on a l'égalité pour $k = 0$. Maintenant, supposons que l'égalité est vraie pour $k > 0$. Montrons qu'elle est aussi vraie pour $k + 1$. D'après l'hypothèse de récurrence, on a

$$\delta^{k+1} \left(f_i \frac{(\text{Log}z)^r}{r!} \right) = \delta \left(\sum_{s=0}^r \binom{k}{s} (\delta^{k-s} f_i) \frac{(\text{Log}z)^{r-s}}{(r-s)!} \right).$$

Mais, il est clair que

$$\delta \left(\sum_{s=0}^r \binom{k}{s} (\delta^{k-s} f_i) \frac{(\text{Log}z)^{r-s}}{(r-s)!} \right) = \sum_{s=0}^r \binom{k+1}{s} (\delta^{k+1-s} f_i) \frac{(\text{Log}z)^{r-s}}{(r-s)!}.$$

Ainsi, on a montré que pour tout $i, r \in \{1, \dots, n\}$ et pour tout $k \in \mathbb{N}$,

$$\delta^k \left(f_i \frac{(\text{Log}z)^r}{r!} \right) = \sum_{s=0}^r \binom{k}{s} (\delta^{k-s} f_i) \frac{(\text{Log}z)^{r-s}}{(r-s)!}. \quad (3.21)$$

Soit $(\delta^k f_i \frac{(\text{Log}z)^r}{r!})_0(z)$ la série telle que $(\delta^k f_i \frac{(\text{Log}z)^r}{r!})(z) - (\delta^k f_i \frac{(\text{Log}z)^r}{r!})_0(z)$ appartient à $(\text{Log}z)\mathbb{C}[[z, \text{Log}z]]$. Donc, il suit de l'égalité (3.21) que pour tout $k \geq r$, $(\delta^k f_i \frac{(\text{Log}z)^r}{r!})_0 = \binom{k}{r} \delta^{k-r} f_i$. Ainsi, pour tout $r \geq 2$ et $k \geq r-1$ on a que $(\delta^k g_r)_0 = \sum_{i=1}^r \binom{k}{r-i} \delta^{k-r+i} f_i$. Notamment, pour $j \geq 2$ et $k \geq j$, $(\delta^k g_j)_0(0) = 0$ et pour $j \geq 2$, $(\delta^{j-1} g_j)_0 - f_1 \in z\mathbb{C}[[z]]$. Soit $j \geq 2$. Maintenant, d'une part

$$\begin{aligned} \delta^n g_j(z) + b_1(z) \delta^{n-1} g_j(z) + \dots + b_{n-1}(z) \delta g_j(z) + b_n(z) g_j(z) = \\ t_{j,j-1}(z) \frac{(\text{Log}z)^{j-1}}{(j-1)!} + t_{j,j-2}(z) \frac{(\text{Log}z)^{j-2}}{(j-2)!} + \dots + t_{j,1}(z) \text{Log}z + t_{j,0}(z), \end{aligned}$$

où les $t_{j,i}(z)$ appartiennent à $\mathbb{C}[[z]]$ pour $i \in \{0, \dots, j-1\}$. En particulier, $t_{j,0}(z) = b_n(z) f_j(z) + b_{n-1}(z) (\delta g_j)_0(z) + \dots + b_1(z) (\delta^{n-1} g_j)_0(z) + (\delta^n g_j)_0(z)$. Ainsi, on a $t_{j,0}(0) = b_{n-j+1}(0) f_1(0)$ car par hypothèse de récurrence $b_{n-1}(0) = \dots = b_{n-j+2}(0) = 0$ et comme on l'a montré, pour tout $k \geq j$, $(\delta^k g_j)_0(0) = 0$ et $(\delta^{j-1} g_j)_0(z) - f_1(z) \in z\mathbb{C}[[z]]$. D'autre part, comme $g_j(z)$ est solution de $\mathcal{M}_{f,\delta}$ alors

$$\delta^n g_j(z) + b_1(z) \delta^{n-1} g_j(z) + \dots + b_{n-1}(z) \delta g_j(z) + b_n(z) g_j(z) = 0.$$

Ainsi, $t_{j,i}(z)$ est la série nulle pour tout $i \in \{0, \dots, j-1\}$ car $\text{Log}z$ est transcendante sur $\mathbb{C}((z))$. En particulier, $t_{j,0}(z)$ est la série nulle et ainsi $b_{n-j}(0)f_1(0) = 0$. D'où $b_{n-j}(0) = 0$ car $f_1(0) \neq 0$. Ainsi, le polynôme indiciel de \mathcal{M}_f est égal à X^n et par conséquent, les exposants en zéro de \mathcal{M}_f sont tous égaux à zéro. \square

Lemme 3.5.21. *Soit \mathcal{S} un ensemble infini de nombres premiers et $f(z) \in \mathcal{F}(\mathcal{S})$. Si $f(z)$ annule $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MOM en zéro alors pour tout $p \in B_{\mathcal{S}}$, la série $f(z)$ vérifie la propriété $(\mathbf{P})_{p,r,n}$.*

Démonstration. On va montrer que pour tout $p \in B_{\mathcal{S}}$, l'opérateur \mathcal{M}_f satisfait aux conditions 1-6 de la définition 3.5.17. Soit $p \in B_{\mathcal{S}}$. Il est clair que \mathcal{M}_f est annulé par f et que l'ordre de \mathcal{M}_f est n . Soit $\mathcal{M}_{f,\delta}$ l'opérateur différentiel obtenu après avoir réécrit $z^n \mathcal{M}_f$ en fonction de δ et soit $M_{f,\delta}$ la matrice compagnon de $\mathcal{M}_{f,\delta}$. Écrivons $M_{f,\delta} = \delta^n + b_1(z)\delta^{n-1} + \dots + b_{n-1}(z)\delta + b_n(z)$. Montrons que $M_{f,\delta}$ appartient à \mathcal{M}_p . Il suit du lemme 3.5.20 que zéro est un point singulier régulier de \mathcal{M}_f alors, d'après la proposition 3.2.1, $b_i(z) \in \mathbb{Q}[[z]]$. Ainsi, les $b_i(z)$ sont dans $\mathbb{Q}(z) \cap \mathbb{Q}[[z]]$. Par conséquent, ils appartiennent à $E_{0,p}$. Le lemme 3.5.20 entraîne que les exposants en zéro de \mathcal{M}_f sont tous égaux à zéro. Donc les valeurs propres de $M_{f,\delta}(0)$ sont toutes égales à zéro. Finalement, montrons que $M_{f,\delta}$ vérifie la condition iii) de la définition 3.5.11. Comme $f(z) \in \mathcal{F}(\mathcal{S})$, alors il existe $\mathcal{H} \in \mathbb{Q}(z)[\delta]$ muni d'une structure de Frobenius forte pour tout $p \in \mathcal{S}$ tel que \mathcal{H} est annulé par $f(z)$. Ainsi pour chaque $p \in \mathcal{S}$ les propositions 4.1.2, 4.6.4 et 4.7.2 de [23] montrent qu'il existe une matrice inversible W dont les coefficients sont analytiques dans le disque générique ouvert $D(z, 1)$ telle que $\delta W = AW$, où A est la matrice compagnon de \mathcal{H} . Finalement, à la suite de l'équation (5.2) de [42, chap III], il existe une matrice inversible U dont les coefficients sont analytiques dans le disque générique telle que $\delta U = M_{f,\delta}U$. Montrons que la matrice U est à coefficients dans le disque générique $D(z, 1)$. En effet, comme $\mathcal{H} = \mathcal{T}\mathcal{M}_{f,\delta}$ car $\mathcal{M}_{f,\delta}$ est l'opérateur minimal de $f(z)$ et W est une matrice inversible à coefficients dans le disque générique $D(z, 1)$ telle que $\delta W = AW$ alors les coefficients de la matrice U sont analytiques dans le disque générique ouvert $D(z, 1)$. Par conséquent, la matrice $M_{f,\delta}$ appartient à \mathcal{M}_p .

D'après le lemme 3.5.20, l'opérateur \mathcal{M}_f est MOM en zéro et par conséquent, si $p \in B_{\mathcal{S}}$ alors l'opérateur \mathcal{M}_f est p -unipotent. Soit M_f la matrice compagnon de \mathcal{M}_f . Rappelons que $\gamma_1, \dots, \gamma_r$ sont les singularités à distance finie de \mathcal{M}_f dans $\overline{\mathbb{Q}}$. Montrons que si $p \in B_{\mathcal{S}}$ alors la matrice M_f vue comme un élément de $M_n(\mathbb{C}_p[[z]])$ a comme uniques disques singuliers à distance finie les disques $D_{\gamma_1}, \dots, D_{\gamma_r}$. Soit D_γ un disque singulier à distance finie de M_f alors le disque D_γ contient une singularité de \mathcal{M}_f . Disons que $\gamma_i \in D_\gamma$ pour un certain $i \in \{1, \dots, r\}$. Ainsi, $D_\gamma \cap D_{\gamma_i} \neq \emptyset$. Par conséquent, $D_\gamma = D_{\gamma_i}$. Maintenant, il suffit de montrer que $D_{\gamma_i} \cap D_{\gamma_j} = \emptyset$ si $i \neq j$. En effet, comme $p \in B_{\mathcal{S}}$ alors pour tout $\gamma_i \neq 0$, $|\gamma_i|_p = 1$ et ainsi, pour tout $i, j \in \{1, \dots, r\}$, $|\gamma_i - \gamma_j|_p \leq 1$. Maintenant, comme $|d|_p = 1$ alors $\prod_{i \neq j} |\gamma_i - \gamma_j|_p = 1$, d'où $|\gamma_i - \gamma_j|_p = 1$ pour $i \neq j$. Ainsi, $D_{\gamma_i} \cap D_{\gamma_j} = \emptyset$.

Finalement, d'après le lemme 3.5.20, \mathcal{M}_f est fuchsien. Donc, la proposition 6.1.3 de [23] entraîne que les disques singuliers de M_f sont singuliers réguliers. Raison pour laquelle, pour tout $p \in B_{\mathcal{S}}$ la série $f(z)$ vérifie la propriété $(\mathbf{P})_{p,r,n}$ car l'opérateur \mathcal{M}_f satisfait aux conditions 1-6 de la définition 3.5.17. \square

Démonstration de la proposition 3.5.4

Démonstration. Soit $\mathcal{S}' = B_{\mathcal{S}}$. Alors $\mathcal{S}' \subset \mathcal{S}$ est infini et $\mathcal{S} \setminus \mathcal{S}'$ est fini. D'après le lemme 3.5.21, pour tout $p \in \mathcal{S}'$ la série $f(z)$ vérifie la propriété $(\mathbf{P})_{p,r,n}$. Ainsi, d'après le lemme 3.5.18, pour tout $p \in \mathcal{S}'$ et tout entier k positif la série $\Lambda_p^k(f(z))$ vérifie la propriété

(**P**)_{*p,r,n*}. En particulier $\Lambda_p^k(f(z))$ annule un opérateur p -unipotent $\mathcal{L}_k \in \vartheta_{E_p}[d/dz]$. Si $L_k(z)$ est la matrice compagnon de \mathcal{L}_k alors, d'après le lemme 3.5.18, les disques singuliers de $L_k(z)$ sont singuliers réguliers et $L_k(z)$ a exactement r disques singuliers à distance finie. Par conséquent, d'après le lemme 3.5.19, le nombre de singularités à distance finie de $\mathcal{L}_{k,p}$ dans $\overline{\mathbb{F}_p}$ est inférieur ou égal à r . \square

Remarque 3.5.22. Soient \mathcal{S} un ensemble infini de nombres premiers et $f(z) \in \mathcal{F}(\mathcal{S})$. Supposons que $f(z)$ annule un opérateur différentiel $\mathcal{D} \in \mathbb{Q}(z)[d/dz]$ MOM en zéro. D'après la première partie du théorème 1.7.6, il existe $\mathcal{S}' \subset \mathcal{S}$ infini tel que $f(z) \in \mathcal{L}^2(\mathcal{S}')$ et $\mathcal{S} \setminus \mathcal{S}'$ est fini. Il suit des parties 3.5.3 et 3.5.3 que nous pouvons prendre $\mathcal{S}' = B_{\mathcal{S}}$.

3.6 La série hypergéométrique ${}_2F_1(-1/2, 1/2, 1; 16z)$

Nous allons montrer que la série

$$\mathfrak{h}_2(z) := {}_2F_1(-1/2, 1/2, 1; 16z) = \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n}^2 z^n$$

appartient à $\mathcal{L}^2(\mathcal{P}) \setminus \mathcal{L}(\mathcal{P})$, où \mathcal{P} est l'ensemble des nombres premiers. Remarquons que la série $\mathfrak{h}_2(z)$ satisfait aux conditions du premier point du théorème 1.7.6. La série $\mathfrak{h}_2(z)$ annule l'opérateur différentiel $\mathcal{L} := z(1-16z)\frac{d}{dz^2} + (1-16z)\frac{d}{dz} + 4$. Cet opérateur est fuchsien, zéro est un point singulier régulier et les exposants de \mathcal{L} en zéro sont égaux à zéro. Donc, l'opérateur \mathcal{L} est MOM en zéro. Notons que $\mathfrak{h}_2(z)$ est le produit de Hadamard des séries $(1-4z)^{1/2} = \sum_{n \geq 0} \binom{2n}{n} z^n$ et $(1-4z)^{-1/2} = \sum_{n \geq 0} -\frac{1}{2n-1} \binom{2n}{n} z^n$. Par conséquent, d'après la proposition 6 de [28], \mathfrak{h}_2 est la diagonale d'une fraction rationnelle. Donc, d'après [25], la série \mathfrak{h}_2 annule un opérateur muni d'une structure de Frobenius forte pour presque tout nombre premier.

Lemme 3.6.1. *La série $\mathfrak{h}_2(z)$ appartient à $1 + z\mathbb{Z}[[z]]$ et, pour tout $p \in \mathcal{P}$, $\mathfrak{h}_{2|p}(z) = P_{0,p}(z)\Lambda_p(\mathfrak{h}_{2|p}(z))^p$, où $P_{0,2}(z) = 1$ si $p = 2$ et $P_{0,p}(z) = \sum_{i=0}^{(p-1)/2} \left(\frac{-1}{2i-1} \binom{2i}{i} \right)^2 \pmod{p} z^i$ si $p \geq 3$.*

Démonstration. La série $\mathfrak{h}_2(z)$ est le produit de Hadamard des $(1-4z)^{1/2} = \sum_{n \geq 0} \binom{2n}{n} z^n$ et $(1-4z)^{-1/2} = \sum_{n \geq 0} -\frac{1}{2n-1} \binom{2n}{n} z^n$. Il est clair que la série $(1-4z)^{1/2}$ appartient à $1 + z\mathbb{Z}[[z]]$. Montrons maintenant que la série $(1-4z)^{-1/2}$ appartient à $1 + z\mathbb{Z}[[z]]$. Cela revient à montrer que pour tout entier n positif, $\frac{1}{2n-1} \binom{2n}{n} \in \mathbb{Z}$. En effet, pour tout entier $n > 0$, $\frac{1}{2n-1} \binom{2n}{n} = 2C_{n-1}$, où $C_n := \frac{1}{2n+1} \binom{2n+1}{n}$ est le nombre de Catalan de rang n . Il suit du corollaire 6.2.3 de [69] que pour tout entier $n \geq 0$, $C_n \in \mathbb{N}$. Par conséquent, la série $(1-4z)^{-1/2}$ appartient à $1 + z\mathbb{Z}[[z]]$. Comme \mathfrak{h}_2 est le produit de Hadamard de $(1-4z)^{1/2}$ et $(1-4z)^{-1/2}$ alors $\mathfrak{h}_2(z) \in 1 + z\mathbb{Z}[[z]]$. Ainsi, on peut réduire $\mathfrak{h}_2(z)$ pour tout nombre premier. La série $\mathfrak{h}_2(z)$ annule l'opérateur différentiel $\mathcal{L} := z(1-16z)\frac{d}{dz^2} + (1-16z)\frac{d}{dz} + 4$. Cet opérateur est fuchsien avec une singularité en zéro dont les exposants en zéro sont égaux à zéro. Donc, pour tout nombre premier p , l'opérateur différentiel \mathcal{L} est p -unipotent. Alors, la proposition 3.5.2 implique que pour tout nombre premier p , il existe une fraction rationnelle $P_{0,p}(z)$ de hauteur inférieure ou égale à $4p-1$ telle que

$$\mathfrak{h}_{2|p}(z) = P_{0,p}(z)\Lambda_p(\mathfrak{h}_{2|p}(z))^p. \quad (3.22)$$

Nous montrerons que pour $p = 2$, $P_{0,2}(z) = 1$ et pour $p \neq 2$,

$$P_{0,p}(z) = \sum_{i=0}^{(p-1)/2} \left(\frac{-1}{2i-1} \binom{2i}{i}^2 \pmod{p} \right) z^i.$$

Pour $p = 2$, il suit du théorème de Lucas que si n est impaire alors $\binom{2n}{n} \equiv 0 \pmod{2}$ alors $\mathfrak{h}_{2|2}(z) = \sum_{n \geq 0} \left(\binom{4n}{2n} \pmod{p} \right) z^{2n} = \Lambda_2(\mathfrak{h}_{2|2}(z))^2$. Maintenant soit $p \neq 2$. Écrivons $\mathfrak{h}_{2|p}(z) = \sum_{n \geq 0} a_n z^n$ et $Q_n(z) = \sum_{i=0}^{p-1} a_{np+i} z^i$. Alors $\mathfrak{h}_{2|p}(z) = \sum_{n \geq 0} z^{np} Q_n(z)$. Montrons que pour tout $n \geq 0$, $\mathcal{L}_p(Q_n(z)) = 0$. En effet, notons d'abord que $\deg(z(1-z)Q_n'') < p$, $\deg((1-z)Q_n') < p$ alors $\deg(\mathcal{L}_p(Q_n(z))) < p$ et comme $0 = \mathcal{L}_p(\mathfrak{h}_{2|p}(z)) = \sum_{n \geq 0} z^{np} \mathcal{L}_p(Q_n(z))$, il suit que $\mathcal{L}_p(Q_n(z)) = 0$ pour tout $n \geq 0$. Comme \mathcal{L} est p -unipotent et $\text{Ker}(\mathbb{F}_p(z), \mathcal{L}_p) \neq 0$ car Q_0 est non nul, donc, d'après le lemme 3.5.5, $\dim_{\mathbb{F}_p(z^p)} \text{Ker}(\mathbb{F}_p(z), \mathcal{L}_p) = 1$. On vient de voir que $Q_0(z)$ et $Q_n(z)$ appartiennent à $\text{Ker}(\mathbb{F}_p(z), \mathcal{L}_p)$ et puisque pour tout $n \geq 0$ $\deg(Q_n(z)) < p$ et $Q_0(0) = 1$ alors $Q_n(z) = a_{np} Q_0(z)$ et ainsi

$$\mathfrak{h}_{2|p}(z) = Q_0(z) \sum_{n \geq 0} a_{np} z^{np} = Q_0(z) \Lambda_p(\mathfrak{h}_{2|p}(z))^p.$$

Donc, il découle de (3.22) que $P_{0,p}(z) = Q_0(z)$ et par conséquent $\mathcal{L}_p(P_{0,p}(z)) = 0$. Grâce à la proposition 2.2 de [50], $-\deg(P_{0,p})$ est congruent à $-1/2$ ou $1/2$ modulo p et comme $\deg(P_{0,p}) < p$ alors $\deg(P_{0,p}) = \frac{p-1}{2}$ ou $\deg(P_{0,p}) = \frac{p+1}{2}$. Raisonnons par l'absurde et supposons que $\deg(P_{0,p}(z)) = \frac{p+1}{2}$. Comme $P_{0,p}(z) = Q_0(z)$ alors $a_{\frac{p+1}{2}} = -\frac{1}{p} \left(\frac{p+1}{\frac{p+1}{2}} \right)^2 \pmod{p}$. Par suite du théorème de Lucas la valuation p -adique de $\left(\frac{p+1}{\frac{p+1}{2}} \right)^2$ est supérieure ou égale à 1, d'où la valuation p -adique de $\frac{1}{p} \left(\frac{p+1}{\frac{p+1}{2}} \right)^2$ est supérieure ou égale à 1 et, ainsi $a_{\frac{p+1}{2}} = 0$, contradiction. Alors $\deg(P_{0,p}) = \frac{p-1}{2}$ et par conséquent, $P_{0,p}(z) = \sum_{i=0}^{(p-1)/2} \left(-\frac{1}{2i-1} \binom{2i}{i}^2 \pmod{p} \right) z^i$. \square

Considérons la série hypergéométrique $\mathfrak{g}_2(z) = {}_2F_1(1/2, 1/2, 1, 16z) = \sum_{n \geq 0} \binom{2n}{n}^2 z^n$.

Lemme 3.6.2. *Pour tout $k \geq 1$ et tout nombre premier p , $\Lambda_p^k(\mathfrak{h}_{2|p}) = \mathfrak{g}_{2|p}$. En particulier, pour tout $k \geq 1$ et tout nombre premier $p \geq 3$, $\Lambda_p^k(\mathfrak{h}_{2|p}) \neq \mathfrak{h}_{2|p}$.*

Démonstration. Montrons d'abord que, pour tout nombre premier p , on a $\Lambda_p(\mathfrak{h}_{2|p}(z)) = \mathfrak{g}_{2|p}(z)$. En effet, d'après le théorème de Lucas, $\binom{2np}{np}^2 \equiv \binom{2n}{n}^2 \pmod{p}$ et, il est claire que $2np - 1 \equiv -1 \pmod{p}$. Donc, $\frac{-1}{2np-1} \binom{2np}{np}^2 \equiv \binom{2n}{n}^2 \pmod{p}$. D'où, $\Lambda_p(\mathfrak{h}_{2|p}(z)) = \mathfrak{g}_{2|p}(z)$. Finalement, comme $\mathfrak{g}_1(z)$ est p -Lucas pour tout nombre premier p , alors, pour tout entier k strictement positif et tout nombre premier p , $\Lambda_p^k(\mathfrak{g}_{2|p}(z)) = \mathfrak{g}_{2|p}$. Par suite, pour tout entier k strictement positif et tout $p \geq 3$, $\Lambda_p^k(\mathfrak{h}_{2|p}(z)) = \mathfrak{g}_{2|p}(z)$. \square

Grâce au lemme 3.6.2, on ne peut pas appliquer le deuxième point du théorème 1.7.6 à la série $\mathfrak{h}_2(z)$. Pour $p = 2$, on pose $P_{1,2}(z) = 1$ et pour $p \geq 3$ on pose $P_{1,p}(z) = \sum_{i=0}^{(p-1)/2} \left(\binom{2i}{i}^2 \pmod{p} \right) z^i$.

Lemme 3.6.3. *Pour tout nombre premier p , on a*

$$\mathfrak{h}_{2|p}(z) = \left(\frac{P_{1,p}(z)^p}{P_{0,p}(z)^{p-1}} \right) \mathfrak{h}_{2|p}(z)^p.$$

Notamment, la série $\mathfrak{h}_2(z)$ appartient à $\mathcal{L}^2(\mathcal{P})$.

Démonstration. Le lemme 3.6.2 et l'équation (3.22) entraînent que, pour tout nombre premier p , $\mathfrak{h}_{2|p}(z) = P_{0,p}(z)\mathfrak{g}_{2|p}(z^p)$. Maintenant, comme \mathfrak{g}_2 est p -Lucas pour tout nombre premier, alors, pour tout nombre premier p , on a $\mathfrak{g}_{2|p}(z) = P_{1,p}(z)\mathfrak{g}_{2|p}(z^p)$. Donc, pour tout nombre premier p , $\frac{\mathfrak{g}_{2|p}}{\mathfrak{h}_{2|p}} = \frac{P_{1,p}}{P_{0,p}}$ et,

$$\begin{aligned} \mathfrak{h}_{2|p}(z) &= P_0(z)\mathfrak{g}_{2|p}(z^p) = P_{0,p}(z) \left(\frac{\mathfrak{g}_{2|p}(z^p)}{\mathfrak{h}_{2|p}(z^p)} \right) \mathfrak{h}_{2|p}(z^p) \\ &= P_{0,p}(z) \left(\frac{P_{1,p}(z^p)}{P_{0,p}(z^p)} \right) \mathfrak{h}_{2|p}(z^p). \end{aligned}$$

Comme les degrés de $P_0(z)$ et $P_1(z)$ sont $\frac{p-1}{2}$, alors la hauteur de $\frac{P_{1,p}(z)^p}{P_{0,p}(z)^{p-1}}$ est inférieure ou égale à $p\frac{p-1}{2} < p^2$. \square

Nous allons montrer que pour tout nombre premier $p \geq 3$ les polynômes $P_{0,p}(z)$ et $P_{1,p}(z)$ sont premier entre eux.

Lemme 3.6.4. *Pour tout nombre premier p , nous avons $P_{0,p}(z) - 2zP'_{0,p}(z) = P_{1,p}(z)$*

Démonstration. Soit p un nombre premier différent de 2, on a

$$\begin{aligned} P_{0,p}(z) - 2zP'_{0,p}(z) &= 1 + \sum_{i=1}^{(p-1)/2} \frac{1}{1-2i} \binom{2i}{i}^2 z^i - \sum_{i=1}^{(p-1)/2} \frac{2i}{1-2i} \binom{2i}{i}^2 z^i \\ &= P_{1,p}(z). \end{aligned}$$

Pour $p = 2$ nous avons que $P_{0,2}(z) = 1 = P_{1,2}(z)$ d'où $P_{0,2}(z) - 2zP'_{0,2}(z) = P_{1,2}(z)$. \square

Lemme 3.6.5. *Pour tout nombre premier p , le polynôme $P_{0,p}(z)$ est séparable sur $\overline{\mathbb{F}_p}$. En particulier, $P_{0,p}$ et $P'_{0,p}$ n'ont pas de racine en commun.*

Démonstration. Pour $p = 2$, on a $P_{0,2}(z) = 1$. Donc, le polynôme $P_{0,2}(z)$ est séparable sur $\overline{\mathbb{F}_2}$. Soit p un nombre premier différent de 2 et soit $\mathcal{L} := z(1-16z)\frac{d}{dz^2} + (1-16z)\frac{d}{dz} + 4$. La série $\mathfrak{h}_2(z)$ annule \mathcal{L} . D'après le lemme 3.6.1, $\mathfrak{h}_{2|p}(z) = P_{0,p}(z)\Lambda_p(\mathfrak{h}_2(z))^p$. Par conséquent, $\mathcal{L}_p(P_{0,p}(z)) = 0$. Soit $\alpha_i \in \overline{\mathbb{F}_p}$ une racine de $P_{0,p}(z)$. Écrivons $P_{0,p}(z) = b_0(z - \alpha_i)^{m_i} + \dots + b_r(z - \alpha_i)^{\frac{p-1}{2}}$, où $b_0 \neq 0$. On veut montrer que $m_i = 1$. Le développement limité de $z(1-16z)$ en $z - \alpha_i$ nous donne l'égalité suivante

$$z(1-16z) = (\alpha_i - 16\alpha_i^2) + (1 - 32\alpha_i)(z - \alpha_i) - 16(z - \alpha_i)^2$$

et le développement limitée de $1 - 16z$ en $z - \alpha_i$ nous donne l'égalité suivante

$$1 - 16z = 1 - 16\alpha_i - 16(z - \alpha_i).$$

Comme $P_{0,p}(z)$ annule l'opérateur différentiel \mathcal{L}_p alors

$$\begin{aligned} [(\alpha_i - 16\alpha_i^2) + (1 - 32\alpha_i)(z - \alpha_i) - 16(z - \alpha_i)^2]P''_{0,p}(z) \\ + [1 - 16\alpha_i - 16(z - \alpha_i)]P'_{0,p}(z) + 4P_{0,p}(z) = 0. \end{aligned} \quad (3.23)$$

Mais,

$$P'_{0,p}(z) = b_0 m_1 (z - \alpha_i)^{m_i-1} + \dots + b_r \frac{p-1}{2} (z - \alpha_i)^{\frac{p-1}{2}-1}$$

et

$$P''_{0,p}(z) = b_0 m_i (m_i - 1) (z - \alpha_i)^{m_i-2} + b_1 m_i (m_i + 1) (z - \alpha_i)^{m_i-1} \\ + \dots + b_r \frac{p-1}{2} \left(\frac{p-1}{2} - 1 \right) (z - \alpha_i)^{\frac{p-1}{2}-2}.$$

Donc, il suit de (3.23) que,

$$a_{m_i-2} (z - \alpha_i)^{m_i-2} + a_{m_i-1} (z - \alpha_i)^{m_i-1} + \dots + a_{\frac{p-1}{2}} (z - \alpha_i)^{\frac{p-1}{2}} = 0, \quad (3.24)$$

où

$$a_{m_i-2} = (\alpha_i - 16\alpha_i^2) b_0 m_i (m_i - 1)$$

et

$$a_{m_i-1} = (\alpha_i - 16\alpha_i^2) b_1 m_i (m_i + 1) + (1 - 32\alpha_i) m_i (m_i - 1) b_0 + (1 - 16\alpha_i) m_i b_0.$$

Il suit de (3.24) que $a_{m_i-2} = 0$ et $a_{m_i-1} = 0$. Par conséquent,

$$(\alpha_i - 16\alpha_i^2) m_i (m_i - 1) b_0 = 0, \quad (3.25)$$

$$(\alpha_i - 16\alpha_i^2) b_1 m_i (m_i + 1) + (1 - 32\alpha_i) m_i (m_i - 1) b_0 + (1 - 16\alpha_i) m_i b_0 = 0. \quad (3.26)$$

Comme $m_i \neq 0$, $\alpha_i \neq 0$ (zéro n'est pas une racine de $P_{0,p}(z)$) et $b_0 \neq 0$ alors il suit de (3.25) que, $(1 - 16\alpha_i)(m_i - 1) = 0$. Si $\alpha_i \neq 1/16$ alors $m_i = 1$. Maintenant si $\alpha_i = 1/16$ alors l'égalité (3.26) entraîne que $-m_i(m_i - 1) = 0$. Par conséquent, $m_i = 1$. \square

Lemme 3.6.6. *Pour tout nombre premier $p \geq 3$ les polynômes $P_{0,p}(z)$ et $P_{1,p}(z)$ sont premiers entre eux.*

Démonstration. Soit p un nombre premier différent de 2. Montrons que $P_{0,p}(z)$ et $P_{1,p}(z)$ n'ont pas de racine en commun. Comme p est différent de 2, alors les polynômes $P_{0,p}(z)$ et $P_{1,p}(z)$ sont différents. Raisonnons par l'absurde, si $P_{0,p}(\alpha) = P_{1,p}(\alpha) = 0$, d'après le lemme 3.6.4, $P'_{0,p}(\alpha) = 0$. Ainsi α est une racine en commun de $P_{0,p}(z)$ et $P'_{0,p}(z)$ ce qui contredit le lemme 3.6.5. Donc, $P_{0,p}(z)$ et $P_{1,p}(z)$ n'ont pas de racine en commun et par conséquent, $P_{0,p}(z)$ et $P_{1,p}(z)$ sont premiers entre eux. \square

Lemme 3.6.7. *Soit \mathcal{S} un ensemble infini de nombres premiers. Alors la série $\mathfrak{h}_2(z)$ n'appartient pas à $\mathcal{L}(\mathcal{S})$.*

Démonstration. Soit p un nombre premier différent de 2. Nous posons $B_{0,p} = \frac{P_{1,p}^p}{P_{0,p}^{p-1}}$ et $B_{k,p} = B_0(z)B_0(z^p) \dots B_0(z^{p^k})$. D'après le lemme 3.6.3, il découle que

$$\mathfrak{h}_{2|p}(z) = B_k(z) \mathfrak{h}_{2|p}(z^{p^{k+1}}).$$

On vérifie facilement que $B_k = \frac{P_{1,p}^{p^2+p^2+\dots+p^{k+1}}}{P_{0,p}^{p^{k+1}-1}}$. Montrons que la hauteur de B_k est égale à $\frac{p}{2}(p^{k+1} - 1)$. Comme $P_{0,p}(z)$ et $P_{1,p}(z)$ sont premiers entre eux, alors la fraction B_k est réduite et sa hauteur est égale à $\frac{p-1}{2}(p + p^2 + \dots + p^{k+1}) = \frac{p-1}{2}p(1 + p + \dots + p^k) = \frac{p-1}{2} \frac{p}{p-1} (p^{k+1} - 1) = \frac{p}{2}(p^{k+1} - 1)$. Donc, pour tout nombre premier $p \geq 3$, il existe une fraction rationnelle $A_k \in \mathbb{F}_p(z)$ réduite de hauteur $\frac{p}{2}(p^k - 1)$ telle que $\mathfrak{h}_2(z) = A_k(z) \mathfrak{h}_2(z^{p^k})$. Par conséquent, $\mathfrak{h}_2(z) \notin \mathcal{L}(\mathcal{S})$. \square

3.7 Équations de Calabi-Yau

Dans [9] les auteurs donnent une liste de plus de 400 opérateurs de type Calabi-Yau. Ces opérateurs vérifient certaines conditions algébriques dont : zéro est un point singulier régulier et les exposants en zéro sont tous égaux à zéro et chaque opérateur admet une solution dans $\mathbb{Z}[[z]]$ dont le terme constant est égal à 1. Notamment, tous ces opérateurs sont MOM en zéro. Dans la plupart des cas, la série solution de ces opérateurs est donnée dans [9]. Grâce à la deuxième partie du théorème 1.7.6, nous avons montré dans la partie 3.3 que la série 210 de [9] appartient à $\mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{J} est un ensemble fini de nombres premiers. Nous soulignons que la stratégie utilisée pour montrer que la série 210 est dans $\mathcal{L}(\mathcal{P} \setminus \mathcal{J})$ peut être employée pour montrer que d'autres séries qui apparaissent dans [9] appartiennent à $\mathcal{L}(\mathcal{S})$, où \mathcal{S} est un ensemble de nombres premiers tel que $\mathcal{P} \setminus \mathcal{S}$ est fini. Illustrons encore une fois cette stratégie avec la série 26 de [9]. Cette série est donnée par

$$f(z) = \sum_{j \geq 0} \left(\binom{2j}{j} \left(\sum_{k=0}^j \binom{j}{k}^2 \binom{j+k}{k} \binom{2k}{j} \right) \right) z^j \in 1 + z\mathbb{Z}[[z]].$$

D'après le théorème 3.5 de [17], $f(z)$ est une diagonale d'une fraction rationnelle à coefficients dans \mathbb{Q} , alors de [25], la série $f(z)$ annule un opérateur différentiel $\mathcal{H} \in \mathbb{Q}(z)[d/dz]$ muni d'une structure de Frobenius forte pour presque tout p . De plus, comme on l'a déjà mentionné, l'opérateur annulé par $f(z)$ décrit dans [9] est MOM en zéro. Maintenant nous utilisons le théorème de Lucas pour montrer que pour tout nombre premier p , $\Lambda_p(f)|_p(z) = f|_p(z)$. En effet, d'après le théorème de Lucas $\binom{2jp}{jp} \equiv \binom{2j}{j} \pmod{p}$. Écrivons $k = s + lp$ avec $0 \leq l \leq j$ et $0 \leq s < p - 1$. Supposons $s > 0$, d'après le théorème de Lucas,

$$\binom{jp}{s+lp}^2 \binom{(j+l)p+s}{lp+s} \binom{2lp+2s}{pj} \equiv \binom{j}{l}^2 \binom{0}{s}^2 \binom{j+l}{l} \binom{s}{s} \binom{2lp+2s}{pj} \pmod{p} = 0$$

car $s > 0$. Dans le cas $s = 0$, d'après le théorème de Lucas on obtient,

$$\binom{jp}{lp}^2 \binom{(j+l)p}{lp} \binom{2lp}{pj} \equiv \binom{j}{l}^2 \binom{j+l}{l} \binom{2l}{j} \pmod{p}.$$

Ainsi,

$$\begin{aligned} \Lambda_p(f)|_p(z) &= \sum_{j \geq 0} \left(\binom{2jp}{jp} \left(\sum_{k=0}^{jp} \binom{jp}{k}^2 \binom{jp+k}{k} \binom{2k}{jp} \right) \pmod{p} \right) z^j \\ &= \sum_{j \geq 0} \left(\binom{2jp}{jp} \left(\sum_{s=0}^{p-1} \sum_{l=0}^j \binom{jp}{s+lp}^2 \binom{jp+s+lp}{s+lp} \binom{2lp+2s}{jp} \right) \pmod{p} \right) z^j \\ &= \sum_{j \geq 0} \left(\binom{2jp}{jp} \left(\sum_{l=0}^j \binom{jp}{lp}^2 \binom{jp+lp}{lp} \binom{2lp}{jp} \right) \pmod{p} \right) z^j \\ &= \sum_{j \geq 0} \left(\binom{2j}{j} \left(\sum_{l=0}^j \binom{j}{l}^2 \binom{j+l}{l} \binom{2l}{j} \right) \pmod{p} \right) z^j \\ &= f|_p(z). \end{aligned}$$

Donc, la deuxième partie du théorème 1.7.6 entraîne que la série $f(z) \in \mathcal{L}(\mathcal{P} \setminus \mathcal{J})$, où \mathcal{J} est un ensemble fini de nombres premiers. En appliquant la même stratégie dont nous nous sommes servis pour montrer que les séries 26 et 210 de [9] appartiennent à $\mathcal{L}(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers tel que $\mathcal{P} \setminus \mathcal{S}$ est fini, nous obtenons qu'entre

les séries qui apparaissent dans [9], il y en a 242 qui appartiennent à $\mathcal{L}(\mathcal{S})$, où $\mathcal{P} \setminus \mathcal{S}$ est fini. À savoir :

1-16, 18-25, **26-28**, 29, $\hat{1-14}$, 30, **32, 33**, 35-41, **42**, 43-46, 48-55, 57-60, 62-70, 75-82, 85-92, 94, 95, 99-108, **109**, 110-115, 119-122, **123**, 124-129, 131,132, 146-153, **154**, 156-158, 160-165, 185, **186, 189**, 190-192, **193-196**, 197, **198, 202**, 208, 209, **210, 212**, **213-219, 222, 223, 226**, 232, **234, 235**, 238-240, 243, **251**, 284, **286, 287**, 292, **293, 297, 298, 300, 301, 303, 304, 306, 307, 308-316, 318, 320-322, 323, 328, 329, 331-335, 336, 337, 338, 339, 341-345, 348, 349, 359, 367, 369-371, 373, 377, 378, 379, 380, 381, 385, 394-396, 398, 399-401**.

Les cas en italique représentent les cas montrés dans [2] et les autres sont les nouveaux cas.

3.8 Indépendance algébrique

Rappelons que $f_1(z), \dots, f_r(z) \in \mathbb{Q}[[z]]$ sont *algébriquement dépendantes* sur $\mathbb{Q}(z)$ s'il existe un polynôme non nul $P(x_1, \dots, x_r)$ à coefficients dans $\mathbb{Q}(z)$ tel que $P(f_1, \dots, f_r) = 0$. Et, $f_1(z), \dots, f_r(z)$ sont *algébriquement indépendantes* sur $\mathbb{Q}(z)$ si pour tout polynôme non nul $P(x_1, \dots, x_r)$ à coefficients dans $\mathbb{Q}(z)$, $P(f_1, \dots, f_r) \neq 0$. Notre but dans cette partie est de démontrer les deux théorèmes suivants.

Théorème 1. *Soit la famille $\mathfrak{F} = \left\{ \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n}^r z^n : r \geq 2 \right\}$. Alors tous les éléments de \mathfrak{F} sont algébriquement indépendants sur $\mathbb{Q}(z)$.*

Théorème 2. *Les séries*

$$h_2(z) = \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n}^2 z^n \quad \text{et} \quad a_1(z) = \sum_{n \geq 0} \left(\sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 \right) z^n$$

sont algébriquement indépendantes sur $\mathbb{Q}(z)$.

Nous avons montré dans la partie 3.6 que la série $h_2(z)$ n'appartient pas à $\mathcal{L}(\mathcal{P})$. Donc, le critère d'indépendance algébrique donné dans [2] ne peut pas être appliqué aux séries données dans les théorèmes 1 et 1.7.9. La démonstration de ces deux théorèmes repose sur la proposition 1.7.7. De plus, celle-ci nous fournit une stratégie pour montrer l'indépendance algébrique de certaines séries dans $\mathcal{L}^2(\mathcal{S})$.

Sous les hypothèses du théorème 1.7.7, le théorème 1.7.6 entraîne que pour chaque $i \in \{1, \dots, r\}$, il existe un ensemble $\mathcal{S}_i \subset \mathcal{S}$ infini tel que $f_i(z) \in \mathcal{L}^2(\mathcal{S}_i)$ et $\mathcal{S} \setminus \mathcal{S}_i$ est fini. Donc, si $\mathcal{S}' = \mathcal{S}_1 \cap \dots \cap \mathcal{S}_r$ alors l'ensemble \mathcal{S}' est infini, $\mathcal{S} \setminus \mathcal{S}'$ est fini et pour tout $i \in \{1, \dots, r\}$, $f_i(z) \in \mathcal{L}^2(\mathcal{S}')$. Une observation importante dans la proposition 1.7.7 est que les séries $g_1(z), \dots, g_r(z)$ sont dans $\mathcal{L}(\mathcal{S}_0)$, où $\mathcal{S}_0 \subset \mathcal{S}'$ est infini. Cette observation est montré dans le lemme 3.8.1 ci-dessous. Donc, la proposition 1.7.7 nous fournit un critère de transfert d'indépendance algébrique des séries qui appartiennent à $\mathcal{L}(\mathcal{S}_0)$ aux séries qui sont dans $\mathcal{L}^2(\mathcal{S}_0)$.

Lemme 3.8.1. *Soit \mathcal{S} un ensemble infini de nombres premiers et soient $f(z) \in \mathcal{F}(\mathcal{S})$ et $g(z) \in 1 + z\mathbb{Q}[[z]]$ tels que, pour tout $p \in \mathcal{S}$, $g(z) \in \mathbb{Z}_{(p)}[[z]]$. Supposons que $f(z)$ annule un opérateur différentiel MOM en zéro à coefficients dans $\mathbb{Q}(z)$. Si, pour tout $p \in \mathcal{S}$, il existe un entier strictement positif l_p tel que $\Lambda_p^{2l_p}(f|_p(z)) = g|_p(z) = \Lambda_p^{l_p}(f|_p(z))$ alors, il existe un ensemble infini $\mathcal{S}_0 \subset \mathcal{S}$ tel que l'ensemble $\mathcal{S} \setminus \mathcal{S}_0$ est fini et la série $g(z)$ appartient à $\mathcal{L}(\mathcal{S}_0)$. De plus, pour tout $p \in \mathcal{S}_0$, il existe une fraction rationnelle $B_p(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ telle que $f_p(z) = B_p(z)g|_p(z)$.*

Démonstration. Comme $f(z)$ est dans $\mathcal{F}(\mathcal{S})$ et annule un opérateur différentiel MOM en zéro à coefficients dans $\mathbb{Q}(z)$, d'après le lemme 3.4.2, il existe un ensemble infini $\mathcal{S}_0 \subset \mathcal{S}$ tel que : l'ensemble $\mathcal{S} \setminus \mathcal{S}_0$ est fini et pour tout $p \in \mathcal{S}_0$ et tout couple d'entiers positifs (i, m) , il existe une fraction rationnelle $A_{p,i,m}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^m telle que $\Lambda_p^i(f|_p(z)) = A_{p,i,m}(z)(\Lambda_p^{i+m}(f|_p(z)))^{p^m}$, où C ne dépend pas de p . En particulier, pour $p \in \mathcal{S}_0$ et les entiers strictement positifs $i = l_p = m$ il existe une fraction rationnelle $A_{p,l_p,l_p}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^{l_p} telle que $\Lambda_p^{l_p}(f|_p(z)) = A_{p,l_p,l_p}(z)(\Lambda_p^{2l_p}(f|_p(z)))^{p^{l_p}}$. Mais par hypothèse, $\Lambda_p^{2l_p}(f|_p(z)) = g|_p(z) = \Lambda_p^{l_p}(f|_p(z))$ donc, $g|_p(z) = A_{p,l_p,l_p}(z)g|_p(z)^{p^{l_p}}$. Par conséquent, la série $g(z)$ appartient à $\mathcal{L}(\mathcal{S}_0)$. Maintenant, d'après le lemme 3.4.2, pour $p \in \mathcal{S}_0$ il existe une fraction rationnelle $A_{p,0,l_p}(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ de hauteur inférieure ou égale à Cp^{l_p} telle que $f|_p(z) = A_{p,0,l_p}(z)(\Lambda_p^{l_p}(f|_p(z)))^{p^{l_p}}$. Mais par hypothèse, $\Lambda_p^{l_p}(f|_p(z)) = g|_p(z)$ alors $f|_p(z) = A_{p,0,l_p}(z)g|_p(z)^{p^{l_p}}$. Donc, $f|_p(z) = \frac{A_{p,0,l_p}(z)}{A_{p,l_p,l_p}(z)}g|_p(z)$. Le terme constant de $\frac{A_{p,0,l_p}(z)}{A_{p,l_p,l_p}(z)}$ est égal à 1 car le terme constant des séries $\Lambda_p^l(f|_p(z))$, $\Lambda_p^{2l_p}(f|_p(z))$ est 1. Donc, $\frac{A_{p,0,l_p}(z)}{A_{p,l_p,l_p}(z)} \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$. \square

Maintenant nous appliquerons le théorème 1.7.7 pour montrer les théorèmes 1.7.8 et 1.7.9.

Démonstration de 1.7.8. Pour chaque $r \geq 2$ on pose

$$\mathfrak{h}_r = \sum_{n \geq 0} \frac{-1}{2n-1} \binom{2n}{n} z^n \quad \text{et} \quad \mathfrak{g}_r = \sum_{n \geq 0} \binom{2n}{n} z^n.$$

Soit \mathcal{P} l'ensemble des nombres premiers. Remarquons d'abord que $\mathfrak{h}_r(z)$ et $\mathfrak{g}_r(z)$ appartiennent à $1 + z\mathbb{Z}[[z]]$. D'après le théorème de Lucas, pour tout nombre premier p et tout $r \geq 2$, $\Lambda_p(\mathfrak{h}_r(z))|_p = \mathfrak{g}_r|_p(z) = \Lambda_p^2(\mathfrak{h}_r(z))|_p$. Nous allons d'abord montrer que pour $r \geq 2$ la série $\mathfrak{h}_r(z)$ est dans $\mathcal{F}(\mathcal{P} \setminus \{2\})$. La série $\mathfrak{h}_r(z)$ annule l'opérateur différentiel

$$\mathcal{L}_r = \delta^r - 4^r z(\delta - 1/2)(\delta + 1/2)^{r-1},$$

où $\delta = z \frac{d}{dz}$. Grâce au théorème 6.1 de [73], l'opérateur \mathcal{L}_r est muni d'une structure de Frobenius forte pour tout nombre premier p différent de 2. Ainsi, $\mathfrak{h}_r(z) \in \mathcal{F}(\mathcal{P} \setminus \{2\})$. De plus, l'opérateur \mathcal{L}_r est MOM en zéro. Soit $l \geq 1$ et montrons que $\mathfrak{h}_1(z), \dots, \mathfrak{h}_l(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. Notons que $\mathfrak{h}_1(z), \dots, \mathfrak{h}_l(z) \in \mathcal{F}(\mathcal{P} \setminus \{2\})$ et, pour tout $p \in \mathcal{P} \setminus \{2\}$ et tout $r \in \{1, \dots, l\}$, on a que $\Lambda_p(\mathfrak{h}_r(z))|_p = \mathfrak{g}_r|_p(z) = \Lambda_p^2(\mathfrak{h}_r(z))|_p$. Donc, d'après la proposition 1.7.7, pour montrer que $\mathfrak{h}_1(z), \dots, \mathfrak{h}_l(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$, il suffit de montrer que $\mathfrak{g}_1(z), \dots, \mathfrak{g}_l(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. En effet, à la suite du théorème 2.1 de [2], les séries $\mathfrak{g}_1(z), \dots, \mathfrak{g}_l(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. Par conséquent, pour tout $l \geq 1$ les séries $\mathfrak{h}_1(z), \dots, \mathfrak{h}_l(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$, d'où tous les éléments de \mathfrak{F} sont algébriquement indépendants sur $\mathbb{Q}(z)$. \square

Avant de faire la démonstration du théorème 1.7.9 nous montrons que $\mathfrak{a}_1(z)$ est dans $\mathcal{F}(\mathcal{S})$, où \mathcal{S} est un ensemble infini de nombres premiers et, annule un opérateur différentiel MOM en zéro. D'après le théorème 3.5 de [17], la série $\mathfrak{a}_1(z)$ est la diagonale d'une fraction rationnelle, alors de [25], la série $\mathfrak{a}_1(z)$ annule un opérateur $\mathcal{H} \in \mathbb{Q}(z)[d/dz]$ muni d'une structure de Frobenius forte pour presque tout p . D'autre part, l'opérateur différentiel

$$\mathcal{D} : (1 - 34z + z^2)z^2 \frac{dz}{dz^3} + (3 - 153z + 6z^2)z \frac{d}{dz^2} + (1 - 112z + 7z^2) \frac{d}{dz} - 5 + z$$

est annulé par la série $\mathbf{a}_1(z)$. Cet opérateur est MOM en zéro.

Démonstration du théorème 1.7.9. Considérons $\mathbf{g}_2(z) = \sum_{n \geq 0} \binom{2n}{n}^2 z^n$. Donc pour tout $p \in \mathcal{P}$, $\Lambda_p(\mathfrak{h}_2(z))|_p = \mathfrak{g}_{2|p}(z) = \Lambda_p^2(\mathfrak{h}_2(z))|_p$ et, $\Lambda_p(\mathbf{a}_1(z))|_p = \mathbf{a}_1(z) = \Lambda_p^2(\mathbf{a}_1(z))|_p$. Alors, d'après la proposition 1.7.7, il suffit de montrer que $\mathbf{g}_2(z)$ et $\mathbf{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. Il découle du lemme 3.8.1 qu'il existe un ensemble infini \mathcal{S}'' de nombres premiers tel que $\mathbf{g}_2(z), \mathbf{a}_1(z) \in \mathcal{L}(\mathcal{S}'')$. À la suite du théorème 5.1 de [2], si $\mathbf{g}_2(z)$ et $\mathbf{a}_1(z)$ sont algébriquement dépendantes sur $\mathbb{Q}(z)$ il existe des entiers a, b non tous nuls et une fraction rationnelle $r(z) \in \mathbb{Q}(z)$ tels que $\mathbf{g}_2(z)^a \mathbf{a}_1(z)^b = r(z)$. Alors,

$$\mathbf{a}_1(z)^b = r(z) \mathbf{g}_2(z)^{-a}. \quad (3.27)$$

Comme $\mathbf{a}_1(z)$ annule l'opérateur différentiel \mathcal{D} alors le rayon de convergence de $\mathbf{a}_1(z)$ est égal à $\rho_{\mathbf{a}_1} = 17 - 12\sqrt{2}$ et le rayon de convergence de $\mathbf{g}_2(z)$ est égal à $\rho_{\mathbf{g}_2} = 1/16$ car elle annule l'opérateur $z(1 - 16z) \frac{d}{dz} + (1 - 32z) \frac{d}{dz} - 4$. Comme $\rho_{\mathbf{a}_1} < \rho_{\mathbf{g}_2}$ donc, d'après (3.27), la série $\mathbf{a}_1(z)^b$ est méromorphe au voisinage de $z_0 = 17 - 12\sqrt{2}$. Mais, il est montré dans [2, p. 555] que pour tout entier c différent de zéro la série $\mathbf{a}_1(z)^c$ n'admet pas une continuation méromorphe au voisinage de z_0 . Par conséquent, $b = 0$ et ainsi $\mathbf{g}_2(z)^a = r(z)$. Notamment, comme $a \neq 0$ alors $\mathbf{g}_2(z)$ est algébrique sur $\mathbb{Q}(z)$. Mais, d'après l'article [65] de Sharif et Woodcock, on sait que la série $\mathbf{g}_2(z)$ est transcendante sur $\mathbb{Q}(z)$. Ce qui nous amène à une contradiction. Alors $\mathbf{g}_2(z)$ et $\mathbf{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. Ainsi, la proposition 1.7.7 entraîne que $\mathfrak{h}_2(z)$ et $\mathbf{a}_1(z)$ sont algébriquement indépendantes sur $\mathbb{Q}(z)$. \square

Nous finissons cette partie en démontrant le théorème 1.7.7. Cette démonstration s'appuie fortement sur les techniques développées par Adamczewski, Bell et Delaygue dans [2].

3.9 Démonstration du théorème 1.7.7

Démonstration. D'après le théorème 1.7.6, pour chaque $i \in \{1, \dots, r\}$, la série $f_i \in \mathcal{L}^2(\mathcal{S}_i)$, où $\mathcal{S} \setminus \mathcal{S}_i$ est fini. Soit $\mathcal{S}' = \mathcal{S}_1 \cap \dots \cap \mathcal{S}_r$, alors \mathcal{S}' est infini et $f_1(z), \dots, f_r(z) \in \mathcal{L}^2(\mathcal{S}')$. Supposons que $f_1(z), \dots, f_r(z)$ sont algébriquement dépendantes sur $\mathbb{Q}(z)$. Donc, il existe un polynôme $P(x_1, \dots, x_r) \in \mathbb{Q}(z)[x_1, \dots, x_r]$ non nul de degré total d tel que $P(f_1, \dots, f_r) = 0$. D'après le lemme 3.8.1, pour chaque $i \in \{1, \dots, r\}$, la série $g_i(z) \in \mathcal{L}(\mathcal{S}'_i)$, où $\mathcal{S}' \setminus \mathcal{S}'_i$ est fini. Soit $\mathcal{S}'' = \mathcal{S}'_1 \cap \dots \cap \mathcal{S}'_r$, alors \mathcal{S}'' est infini et $g_1(z), \dots, g_r(z) \in \mathcal{L}(\mathcal{S}'')$. De plus, encore par le lemme 3.8.1, si $p \in \mathcal{S}''$ alors, il existe une fraction rationnelle $B_i(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ telle que $f_{i|p}(z) = B_i(z)g_{i|p}(z)$.

Soit $\mathcal{S}^{(3)} \subset \mathcal{S}''$ tel que pour tout $p \in \mathcal{S}^{(3)}$, le polynôme $P|_p$ est non nul. Remarquons que $P|_p$ est un élément de $\mathbb{F}_p[z][x_1, \dots, x_r]$. L'ensemble $\mathcal{S}^{(3)}$ est infini. Écrivons le polynôme $P|_p = \sum_{(i_1, \dots, i_r) \in \mathbb{N}^r} a_{(i_1, \dots, i_r)}(z) x_1^{i_1} \dots x_r^{i_r}$, où $a_{(i_1, \dots, i_r)}(z) \in \mathbb{F}_p[z]$. Mais, $f_{i|p}(z) = B_i(z)g_{i|p}(z)$, où $B_i(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$, alors $g_{1|p}(z), \dots, g_{r|p}(z)$ annulent le polynôme

$$\sum_{(i_1, \dots, i_r) \in \mathbb{N}^r} a_{(i_1, \dots, i_r)}(z) B_1(z)^{i_1} \dots B_r(z)^{i_r} x_1^{i_1} \dots x_r^{i_r}$$

dont le degré total est inférieur ou égal à d et $a_{(i_1, \dots, i_r)}(z) B_1(z)^{i_1} \dots B_r(z)^{i_r} \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$. Alors, pour tout $p \in \mathcal{S}^{(3)}$, les séries $g_{1|p}(z), \dots, g_{r|p}(z)$ annulent un polynôme non nul à coefficients dans $\mathbb{F}_p(z)$ de degré total inférieur ou égal à d . Puisque $\mathcal{S}^{(3)} \subset$

\mathcal{S}'' et $g_i(z) \in \mathcal{L}(\mathcal{S}'')$ pour tout $i \in \{1, \dots, r\}$, alors pour tout $p \in \mathcal{S}^{(3)}$ et tout $i \in \{1, \dots, r\}$, il existe $A_i(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ et un entier k_i strictement positif tel que $g_{i|p}(z) = A_i(z)g_{i|p}(z^{p^{k_i}})$, où la hauteur de $A_i(z)$ est inférieure ou égale à $C_i p^{k_i}$. Si $k = k_1 \cdots k_r$ et $C = 2 \max\{C_1, \dots, C_r\}$ alors, d'après la remarque 4.2 de [2], pour tout $i \in \{1, \dots, r\}$ il existe $Q_i(z) \in \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ tel que $g_{i|p}(z) = Q_i(z)g_{i|p}(z^{p^k})$, où la hauteur de $Q_i(z)$ est inférieure ou égale à Cp^k . Maintenant, nous allons appliquer la proposition 5.3 de [2] à L le corps de fractions de $\mathbb{F}_p[[z]]$, $M = \mathbb{F}_p(z)$ et l'endomorphisme injectif de L défini par $\sigma(g(z)) = g(z^{p^k}) = g(z)^{p^k}$. Alors la proposition 5.3 de [2] implique qu'il existe $m_1, \dots, m_r \in \mathbb{Z}$ non tous nuls et $r(z) \in \mathbb{F}_p(z)$ tels que

$$Q_1(z)^{m_1} \cdots Q_r(z)^{m_r} = \frac{r(z)^{p^k}}{r(z)} = r(z)^{p^k-1},$$

avec $|m_1 + \cdots + m_r| < d$ et $|m_i| < d$. Comme le terme constant des $Q_i(z)$ est 1 alors $Q_i(z)^{m_i} \in \mathbb{F}_p[[z]]$ et ainsi, $r(z) \in \mathbb{F}_p[[z]]$ et $r(0) = 1$. Notons que $Q_1(z), \dots, Q_r(z), r(z)$ et m_1, \dots, m_r dépendent de p . Comme les m_i appartiennent à un ensemble fini, le principe des tiroirs implique qu'il existe $\mathcal{S}^{(4)} \subset \mathcal{S}^{(3)}$ infini et des entiers t_1, \dots, t_r tels que, pour tout $p \in \mathcal{S}^{(4)}$, $m_i = t_i$ pour $i \in \{1, \dots, r\}$. Supposons que $p \in \mathcal{S}^{(4)}$ et écrivons $r(z) = \frac{a(z)}{b(z)}$, où $a(z), b(z) \in \mathbb{F}_p[z]$ sont premiers entre eux. Comme la hauteur de Q_i est inférieure ou égale à Cp^k alors la hauteur de $Q_1^{t_1} \cdots Q_r^{t_r}$ est inférieure ou égale à $Cp^k(|t_1| + \cdots + |t_r|)$. Et comme

$$Q_1^{t_1} \cdots Q_r^{t_r} = r(z)^{p^k-1}$$

alors la hauteur de $r(z)$ est inférieure ou égale à

$$C \frac{p^k}{p^k-1} (|t_1| + \cdots + |t_r|) < 2Crd.$$

D'où les degrés de $a(z)$ et $b(z)$ sont inférieurs ou égaux à $2Crd$. On pose

$$h(z) = g_1(z)^{-t_1} \cdots g_r(z)^{-t_r} \in \mathbb{Q}[[z]].$$

Donc, pour tout $p \in \mathcal{S}^{(4)}$ on a que

$$\begin{aligned} h_{|p}(z^{p^k}) &= g_{1|p}(z^{p^k})^{-t_1} \cdots g_{r|p}(z^{p^k})^{-t_r} \\ &= g_{1|p}(z)^{-t_1} \cdots g_{r|p}(z)^{-t_r} Q_1^{t_1} \cdots Q_r^{t_r} \\ &= h_{|p}(z) r(z)^{p^k-1}. \end{aligned}$$

Comme $h(0) = 1$ alors $h_{|p}(z)$ est non nul et ainsi $h_{|p}(z)^{p^k-1} = r(z)^{p^k-1}$. Par conséquent, $\frac{r(z)}{h_{|p}(z)}$ est solution du polynôme $x^{p^k-1} - 1$. Comme $r(0) = 1$ et $h_{|p}(0) = 1$ alors $\frac{r(z)}{h_{|p}(z)} = 1$. Maintenant, on sait que pour tout $p \in \mathcal{S}^{(4)}$, $a(z) = a_0 + a_1 z + \cdots + a_i z^i$ et $b(z) = b_0 + b_1 z + \cdots + b_j z^j$, où $0 \leq i, j \leq 2Crd$. Alors,

$$\sum_{j=0}^{2Crd} b_j z^j h_{|p}(z) - \sum_{i=0}^{2Crd} a_i z^i = 0.$$

Par conséquent, $h_{|p}, zh_{|p}(z), \dots, z^{2Crd} h_{|p}(z), z, \dots, z^{2Crd}$ sont linéairement dépendantes sur \mathbb{F}_p . Comme $\mathcal{S}^{(4)}$ est infini, d'après le lemme 5.4 de [2], les séries $zh(z), \dots, z^{2Crd} h(z), z, \dots, z^{2Crd}$ sont linéairement dépendantes sur \mathbb{Q} , d'où $h(z) \in \mathbb{Q}(z)$. Alors, les séries $g_1(z), \dots, g_r(z)$ sont algébriquement dépendantes sur $\mathbb{Q}(z)$. \square

Chapitre 4

Structure de Frobenius forte pour les opérateurs aux q -différences

Le but principal de ce chapitre est de proposer une nouvelle définition de la notion de structure de Frobenius forte pour les opérateurs aux q -différences¹ et d'expliquer comment cette notion aboutirait à des résultats sur les congruences modulo le polynôme cyclotomique associé à p .

4.1 Motivation

En mathématiques, de nombreux concepts élémentaires ont ce que l'on appelle des q -analogues, où q est une variable. L'intérêt des q -analogues est qu'en spécialisant q en 1 on récupère le concept habituel. Dans le cas particulier des entiers, nous disons que $P(q) \in \mathbb{Z}[q]$ est un q -analogue d'un entier n si $\mathbf{ev}(P(q)) = n$, où $\mathbf{ev} : \mathbb{Z}[q] \rightarrow \mathbb{Z}$ est l'homomorphisme donné par $\mathbf{ev}(P(q)) = P(1)$.

Par exemple, étant donné un entier n strictement positif, le polynôme

$$[n]_q := \frac{1 - q^n}{1 - q} = 1 + q + \cdots + q^{n-1} \in \mathbb{Z}[q]$$

est un q -analogue de n parce que $\mathbf{ev}([n]_q) = n$. Remarquons que $[n]_q$ n'est pas l'unique q -analogue de n car le polynôme constant n est aussi un q -analogue de n . Habituellement il est assumé dans la littérature que le q -analogue de n est le polynôme $[n]_q$. Par contre, le choix des q -analogues $[n]_q$ n'est pas fait de manière arbitraire car en quelque sorte, l'arithmétique de ces q -analogues est plus fine que l'arithmétique sur \mathbb{N} . En effet, pour chaque entier $n > 0$,

$$[n]_q = \prod_{d|n} \phi_d(q), \tag{4.1}$$

où $\phi_d(q)$ est le polynôme cyclotomique associé à d . Ainsi, $n = \prod_{d|n} \phi_d(1)$. Remarquons que $\phi_d(1) = 1$ si d est divisible par au moins deux nombres premiers et, pour tout nombre premier p et tout entier $k > 0$, $\phi_{p^k}(1) = p$. Alors, il suit de (4.1) que

$$n = \prod_{p|n} p^{v_p(n)}. \tag{4.2}$$

1. Dans [11] André et Divizio ont donné une autre définition de structure de Frobenius forte pour les opérateurs aux q -différences.

La décomposition (4.1) est plus fine que la décomposition (4.2).

Un q -analogue de $n!$ est défini comme suit :

$$[n]_q! := \prod_{i=1}^n [i]_q \in \mathbb{Z}[q].$$

Il n'est pas difficile de voir que $\mathbf{ev}([n]_q!) = n!$. Également, le coefficient binomial $\binom{n}{m}$ a un q -analogue qui est défini de la façon suivante :

$$\begin{bmatrix} n \\ m \end{bmatrix}_q := \frac{[n]_q!}{[m]_q! [n-m]_q!} \in \mathbb{Z}[q].$$

Il est clair que $\mathbf{ev} \left(\begin{bmatrix} n \\ m \end{bmatrix}_q \right) = \binom{n}{m}$.

Pour considérer des exemples élaborés nous introduisons les anneaux R et R_1 . L'anneau R est la clôture algébrique de $\mathbb{Q}(q)$ et $R_1 = R \cap \overline{\mathbb{Q}}[[q-1]]$. L'homomorphisme $\mathbf{ev} : \mathbb{Z}[q] \rightarrow \mathbb{Z}$ s'étend en l'homomorphisme $\mathbf{ev} : R_1 \rightarrow \overline{\mathbb{Q}}$ donné par $\mathbf{ev}(P(q)) = P(1)$. On dit qu'un élément $P(q) \in R_1$ est un q -analogue de $\gamma \in \overline{\mathbb{Q}}$ si $\mathbf{ev}(P(q)) = \gamma$.

Cela nous permet de définir un q -analogue de $(\alpha)_n$ (n est un entier positif) lorsque α est un nombre rationnel. Rappelons que $(\alpha)_0 = 1$ et $(\alpha)_n = \alpha(\alpha+1) \cdots (\alpha+n-1)$ pour $n > 0$. Le q -analogue de $(\alpha)_n$ est défini de la façon suivante :

$$[(\alpha)_n]_q := \frac{(1-q^\alpha) \cdots (1-q^{\alpha+n-1})}{(1-q)^n} \in R_1,$$

car $\lim_{q \rightarrow 1} [(\alpha)_n]_q = (\alpha)_n$.

Pour chaque $a \in R$, on a

$$(a, q)_n = \prod_{i=0}^{n-1} (1 - aq^i) \in R.$$

Ainsi, un q -analogue de $\frac{(\alpha)_n}{n!}$ est égal à $\frac{(q^\alpha, q)_n}{(q, q)_n} \in R_1$ parce que $\lim_{q \rightarrow 1} \frac{(q^\alpha, q)_n}{(q, q)_n} = \frac{(\alpha)_n}{n!}$.

4.1.1 Structure de Frobenius forte pour les opérateurs aux q -différences, une première motivation

Dans cette partie nous allons exposer notre première motivation pour proposer une nouvelle définition de la notion de structure de Frobenius forte pour les opérateurs aux q -différences.

Jusqu'ici on a vu que certains concepts élémentaires ont des q -analogues. Maintenant nous allons voir que des concepts plus élaborés ont aussi des q -analogues. Nous commençons par les *opérateurs q -hypergéométriques*.

Les opérateurs q -hypergéométriques sont définis de la manière suivante : étant donnés les vecteurs $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ et $\underline{\beta} = (\beta_1, \dots, \beta_{n-1}, 1) \in (\mathbb{Q} \setminus \mathbb{Z}_{\leq 0})^n$, l'opérateur q -hypergéométrique associé aux paramètres $\underline{\alpha}$ et $\underline{\beta}$ est l'opérateur,

$$\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta}) = \prod_{i=1}^n \left(q^{\beta_i-1} \delta_q + \frac{q^{\beta_i-1} - 1}{q-1} \right) - z \prod_{i=1}^n \left(q^{\alpha_i} \delta_q + \frac{q^{\alpha_i} - 1}{q-1} \right) \in R(z)[\delta_q],$$

où δ_q est l'automorphisme de $R(z)$ qui à $f(q, z)$ associe $\frac{f(q, qz) - f(q, z)}{q-1}$.

L'opérateur $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ est un q -analogue de l'opérateur différentiel hypergéométrique

$$\mathcal{H}(\underline{\alpha}, \underline{\beta}) = \prod_{i=1}^n (\delta + \beta_i - 1) - z \prod_{i=1}^n (\delta + \alpha_i) \in \mathbb{Z}[z][\delta], \quad \delta = z \frac{d}{dz}.$$

Cela signifie que lorsque nous remplaçons δ_q par δ et que nous faisons q égal à 1 dans $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ nous récupérons l'opérateur hypergéométrique $\mathcal{H}(\underline{\alpha}, \underline{\beta})$, c'est-à-dire

$$\mathcal{H}(\underline{\alpha}, \underline{\beta}) = \prod_{i=1}^n \left(\mathbf{ev}(q^{\beta_i-1})\delta + \mathbf{ev}\left(\frac{q^{\beta_i-1}-1}{q-1}\right) \right) - z \prod_{i=1}^n \left(\mathbf{ev}(q^{\alpha_i})\delta + \mathbf{ev}\left(\frac{q^{\alpha_i}-1}{q-1}\right) \right).$$

Or, si $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$ et si p est un nombre premier tel que la norme p -adique de α_i et β_j est inférieure ou égale à 1 pour tout $i, j \in \{1, \dots, n\}$ alors, d'après le théorème 1.4.11, l'opérateur différentiel hypergéométrique $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ est muni d'une structure de Frobenius forte pour p . Nous venons de voir que l'opérateur q -hypergéométrique $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ est un q -analogue de l'opérateur différentiel $\mathcal{H}(\underline{\alpha}, \underline{\beta})$. Ainsi, un problème intéressant est de savoir s'il existe une notion de structure de Frobenius forte pour les opérateurs aux q -différences telle que si l'opérateur $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ est muni d'une telle structure alors nous pouvons retrouver la structure de Frobenius forte de l'opérateur différentiel $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ lorsque nous faisons $q = 1$.

Rappelons que dans le cas où n est un entier positif, nous privilégions le choix de $[n]_q$ comme q -analogue de n pour des raisons arithmétiques que nous avons décrites au début de cette partie. Dans le cas de la notion de structure de Frobenius forte pour les opérateurs aux q -différences, nous voulons donc définir une notion qui ait les deux propriétés suivantes : premièrement, que l'on puisse retrouver le résultat arithmétique établi dans le théorème 1.4.6 lorsque nous faisons $q = 1$ et, deuxièmement, qu'elle nous permette de retrouver la structure de Frobenius forte d'un opérateur différentiel quand nous faisons $q = 1$. À présent nous allons détailler ces propriétés à travers les questions 5 et 6 suivantes.

4.1.2 Structure de Frobenius forte pour les opérateurs aux q -différences : arithmétique et spécialisation

Dans certaines situations, les congruences modulo p (p un nombre premier) ont aussi des q -analogues. Par exemple, il suit de [47, 61, 70] que, pour tout nombre premier p , tout entier $r \geq 1$, tout entier $n \geq 1$ et tout $m \in \{0, 1, \dots, p-1\}$, on a la congruence suivante :

$$\left[\begin{matrix} 2(np+m) \\ np+m \end{matrix} \right]_q^r \equiv \left[\begin{matrix} 2n \\ n \end{matrix} \right]_q^r \binom{2m}{m} \pmod{[p]_q \mathbb{Z}[q]}. \quad (4.3)$$

Cette congruence est un q -analogue de la congruence $\binom{2(np+m)}{np+m}^r \equiv \binom{2n}{n}^r \binom{2m}{m}^r \pmod{p\mathbb{Z}}$. Considérons maintenant, pour tout entier $r \geq 1$, la série

$$\mathfrak{g}_r(q, z) = \sum_{n \geq 0} \left[\begin{matrix} 2n \\ n \end{matrix} \right]_q^r z^n.$$

Remarquons que $\mathfrak{g}_r(1, z) = \sum_{n \geq 0} \binom{2n}{n}^r z^n$. Il suit de l'égalité (4.3) que, pour tout nombre premier p et tout entier $r \geq 1$,

$$\mathfrak{g}_r(q, z) \equiv \left(\sum_{n=0}^{p-1} \left[\begin{matrix} 2n \\ n \end{matrix} \right]_q^r z^n \right) \mathfrak{g}_r(1, z^p) \pmod{[p]_q \mathbb{Z}[q][[z]]}.$$

Par conséquent, en faisant $q = 1$ on a

$$\mathfrak{g}_r(1, z) \equiv \left(\sum_{n=0}^{p-1} \binom{2n}{n}^r z^n \right) \mathfrak{g}_r(1, z^p) \pmod{p\mathbb{Z}[[z]]}.$$

La série $\mathfrak{g}_r(q, z)$ fait partie d'une famille de séries étudiées dans [3]. En effet, il a été démontré dans [3] qu'il y a de nombreuses séries $f(q, z)$ appartenant à $1 + z\mathbb{Z}[q][[z]]$ telles que pour tout nombre p , il existe un polynôme $A_p(q, z)$ dans $\mathbb{Z}[q][z]$ de degré en z inférieur ou égal à $p-1$ tel que $f(q, z) \equiv A_p(q, z)f(1, z^p) \pmod{[p]_q\mathbb{Z}[q][[z]]}$. Remarquons que $q^p \equiv 1 \pmod{[p]_q}$, alors

$$f(q, z) \equiv A_p(q, z)f(q^p, z^p) \pmod{[p]_q\mathbb{Z}[q][[z]]}. \quad (4.4)$$

Par conséquent, en faisant $q = 1$ on a que, pour tout nombre premier p ,

$$f(1, z) \equiv A_p(1, z)f(1, z^p) \pmod{p\mathbb{Z}[[z]]}. \quad (4.5)$$

Ainsi, la congruence $f(1, z) \equiv A_p(1, z)f(1, z^p) \pmod{p\mathbb{Z}[[z]]}$ est obtenue après avoir fait $q = 1$ en $f(q, z) \equiv A_p(q, z)f(q^p, z^p) \pmod{[p]_q\mathbb{Z}[q][[z]]}$.

Il se trouve que parmi les séries $f(q, z) \in 1 + z\mathbb{Z}[q][[z]]$ étudiées dans [3], il y en a beaucoup vérifiant que $f(1, z)$ annule un opérateur différentiel muni d'une structure de Frobenius forte pour presque tout nombre premier p . Comme cela, d'après le théorème 1.4.6, pour presque tout nombre premier p , la série $f|_p(1, z) \in \mathbb{F}_p[[z]]$ est algébrique sur $\mathbb{F}_p(z)$ de degré inférieur ou égal à $n^2 h_p$, où n est l'ordre de l'opérateur différentiel et h_p est la période de la structure de Frobenius pour p . Plus précisément, pour presque tout nombre premier p , il existe des polynômes $a_0(z), \dots, a_j(z) \in \mathbb{Z}[z]$ avec $j \leq n^2$ tels que leurs réductions modulo p ne sont pas tous nuls et

$$a_0(z)f(1, z) + a_1(z)f(1, z^{p^{h_p}}) + \dots + a_j(z)f(1, z^{p^{j h_p}}) \equiv 0 \pmod{p\mathbb{Z}[[z]]}. \quad (4.6)$$

En suivant la situation exposée par les égalités (4.4) et (4.5) on a la question suivante :

Question 5. La congruence (4.6) découle-t-elle d'une congruence de la forme

$$\sum_{i=0}^j d_i(q, z)f(q^{p^{i h_p}}, z^{p^{i h_p}}) \equiv 0 \pmod{[p]_q\mathbb{Z}[q][[z]]} \quad ?$$

Par analogie avec le théorème 1.4.6 on s'attendrait à ce qu'à partir de la définition que nous proposons de structure de Frobenius forte on ait le résultat suivant : si la série $f(q, z)$ annule un opérateur aux q -différence d'ordre n muni d'une structure de Frobenius forte pour p de période h_p , alors

$$\sum_{i=0}^j d_i(q, z)f(q^{p^{i h_p}}, z^{p^{i h_p}}) \equiv 0 \pmod{[p]_q\mathbb{Z}[q][[z]]}, \quad (4.7)$$

où $d_i(q, z) \in \mathbb{Z}[q][[z]]$ sont tels que : $d_1(q, z) \pmod{[p]_q}, \dots, d_j(q, z) \pmod{[p]_q}$ ne sont pas tous nuls et $d_1(1, z)|_p, \dots, d_j(1, z)|_p$ appartiennent à $\mathbb{F}_p(z)$. Si tel est le cas, on devrait donc retrouver la congruence (4.6) après avoir fait $q = 1$ en (4.7).

Maintenant, afin de détailler la deuxième propriété espérée d'une structure de Frobenius forte pour les opérateurs aux q -différences, nous commençons par esquisser la définition que nous proposerions de structure de Frobenius forte pour un premier p d'un opérateur aux q -différences. Étant donné un nombre premier p , il faudrait d'abord construire un

anneau ultramétrique de fonctions $E_{\mathbb{Z},q,p}^2$. Cet anneau devrait être muni des automorphismes σ_q et δ_q , où $\sigma_q(f(q, z)) = f(q, qz)$ et $\delta_q(f(q, z)) = \frac{f(q, qz) - f(q, z)}{q-1}$ et également d'un automorphisme de Frobenius \mathbf{F}_q tel que $\mathbf{F}_q(q) = q^p$. Finalement, cet anneau aurait les propriétés suivantes : l'anneau $\mathbb{Z}[q][z]$ est contenu dans $E_{\mathbb{Z},q,p}$ et il existe un homomorphisme continu d'anneaux $\mathbf{ev} : E_{\mathbb{Z},q,p} \rightarrow E_p$, où E_p est l'anneau des éléments analytiques tel que $\mathbf{ev}(P(q, z)) = P(1, z)$ pour tout $P(q, z) \in \mathbb{Z}[q][z]$. L'homomorphisme \mathbf{ev} représenterait dans notre contexte l'opération de spécialiser la variable q en 1.

Considérons maintenant l'opérateur aux q -différence d'ordre n

$$L_{\delta_q} := \delta_q^n + b_1(z)\delta_q^{n-1} + \cdots + b_{n-1}(z)\delta_q + b_n(z) \in E_{\mathbb{Z},q,p}[\delta_q]. \quad (4.8)$$

Nous posons $\mathbf{ev}(L_{\delta_q}) = \delta^n + \mathbf{ev}(b_1(z))\delta^{n-1} + \cdots + \mathbf{ev}(b_{n-1}(z))\delta + \mathbf{ev}(b_n(z))$ et nous disons que L_{δ_q} est un q -analogue de l'opérateur différentiel $\mathbf{ev}(L_{\delta_q})$. On devrait avoir $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta}) \in E_{\mathbb{Z},q,p}[\delta_q]$ et $\mathbf{ev}(\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})) = \mathcal{H}(\underline{\alpha}, \underline{\beta})$. Nous associons à L_{δ_q} la matrice

$$B_q = \begin{pmatrix} 1 & (q-1) & 0 & \cdots & 0 \\ 0 & 1 & (q-1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & (q-1) \\ -(q-1)b_n(z) & -(q-1)b_{n-1}(z) & -(q-1)b_{n-2}(z) & \cdots & -(q-1)b_1 + 1 \end{pmatrix}.$$

Nous posons $B_q^{\mathbf{F}_q^h}$ la matrice obtenue après avoir appliqué h -fois l'automorphisme \mathbf{F}_q à chaque entrée de B_q . Nous appelons la matrice B_q la *matrice associée* à L_{δ_q} . La définition que nous proposerions de *structure de Frobenius forte pour un nombre premier p pour les opérateurs aux q -différence* serait alors la suivante :

Définition 4.1.1. Soient p un nombre premier, $L_q \in E_{\mathbb{Z},q,p}[\delta_q]$ et B_q la matrice associée à L_q . Nous disons que L_q possède une *structure de Frobenius forte* pour p de période h s'il existe une matrice $H_q \in \mathrm{GL}_n(E_{\mathbb{Z},q,p})$ telle que

$$\sigma_q(H_q)B_q^{\mathbf{F}_q^h} = B_qH_q. \quad (4.9)$$

La matrice H_q est appelée une *matrice de passage de Frobenius* pour p de l'opérateur L_{δ_q} .

L'égalité (4.9) signifie que les σ_q -modules définis par les matrices $B_q^{\mathbf{F}_q^h}$ et B_q sont isomorphes en tant que σ_q -modules à coefficients dans $E_{\mathbb{Z},q,p}$.

Sous cette définition, nous espérons avoir la *confluence* de la structure de Frobenius forte des opérateurs q -hypergéométriques vers la structure de Frobenius des opérateurs différentiels hypergéométriques. Nous précisons cela dans la question suivante :

Question 6. Supposons que $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ est muni d'une structure de Frobenius forte pour p de période h et H_q est une matrice de passage de Frobenius pour p de cet opérateur. Soient B la matrice compagnon de $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ et $\mathbf{ev}(H_q)$ la matrice obtenue après avoir appliqué \mathbf{ev} à chaque entrée de H_q . A-t-on l'égalité $\delta(\mathbf{ev}(H_q)) = B\mathbf{ev}(H_q) - p^h\mathbf{ev}(H_q)B(z^{p^h})$?

Remarquons que l'égalité $\delta(\mathbf{ev}(H_q)) = B\mathbf{ev}(H_q) - p^h\mathbf{ev}(H_q)B(z^{p^h})$ signifie que $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ a une structure de Frobenius forte pour p de période h . Si la question 6 a une réponse affirmative alors elle nous dit que nous pouvons retrouver la structure de Frobenius forte de l'opérateur différentiel $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ à partir de la structure de Frobenius forte de l'opérateur aux q -différences $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ puisque $\delta(\mathbf{ev}(H_q)) = B\mathbf{ev}(H_q) - p^h\mathbf{ev}(H_q)B(z^{p^h})$.

2. L'anneau $E_{\mathbb{Z},q,p}$ jouerait le rôle analogue que joue le corps des éléments analytiques E_p dans le contexte des opérateurs différentiels.

4.2 Structure de Frobenius forte pour les opérateurs aux q -différences

Dans cette partie nous allons définir la structure de Frobenius forte pour les opérateurs aux q -différences. Considérons l'anneau $\mathbb{Z}[q]$, où q est une variable et l'homomorphisme $\mathbf{ev} : \mathbb{Z}[q] \rightarrow \mathbb{Z}$ donné par $\mathbf{ev}(P(q)) = P(1)$. Dans la suite nous fixons le nombre premier p et l'idéal $\mathfrak{m} = (p, 1 - q)\mathbb{Z}[q]$.

Remarque 4.2.1. L'idéal \mathfrak{m} est un idéal maximal de $\mathbb{Z}[q]$ parce que \mathfrak{m} est le noyau de l'homomorphisme surjectif $\pi \circ \mathbf{ev} : \mathbb{Z}[q] \rightarrow \mathbb{F}_p$, où $\pi : \mathbb{Z} \rightarrow \mathbb{F}_p$ est l'homomorphisme de réduction modulo p .

Comme l'anneau $\mathbb{Z}[q]$ est noethérien et $\mathfrak{m} \neq (1)$ alors, d'après le corollaire 10.18 de [13], $\bigcap_{n \geq 0} \mathfrak{m}^n = \{0\}$. Par conséquent, si $x \in \mathbb{Z}[q]$ est non nul, alors il existe un unique entier n supérieur ou égal à zéro tel que $x \in \mathfrak{m}^n$ et $x \notin \mathfrak{m}^{n+1}$. Nous posons

$$|x|_{\mathfrak{m}} = \frac{1}{p^n}.$$

Une observation important est que $|\cdot|_{\mathfrak{m}}$ définit une valeur absolue ultramétrique sur $\mathbb{Z}[q]$, c'est-à-dire que, pour tout $x, y \in \mathbb{Z}[q]$, $|x|_{\mathfrak{m}} = 0$ si et seulement si $x = 0$, $|x + y|_{\mathfrak{m}} \leq \max\{|x|_{\mathfrak{m}}, |y|_{\mathfrak{m}}\}$ et $|xy|_{\mathfrak{m}} = |x|_{\mathfrak{m}}|y|_{\mathfrak{m}}$. Ainsi, l'anneau $\mathbb{Z}[q]$ est muni d'une norme ultramétrique que nous appelons la norme \mathfrak{m} -adique.

Proposition 4.2.2. *Munissons $\mathbb{Z}[q]$ de la norme \mathfrak{m} -adique et \mathbb{Z} de la norme p -adique. Alors l'homomorphisme $\mathbf{ev} : \mathbb{Z}[q] \rightarrow \mathbb{Z}$ est continu et, pour tout $P(q) \in \mathbb{Z}[q]$, $|\mathbf{ev}(P(q))|_p \leq |P(q)|_{\mathfrak{m}}$.*

Démonstration. Soit $P(q) \in \mathbb{Z}[q]$. Supposons que $|P(q)|_{\mathfrak{m}} = 1/p^n$ alors, $P(q) \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. Or \mathfrak{m}^n est engendré par la famille $\{p^{n-i}(1-q)^i\}_{0 \leq i \leq n}$. Par conséquent, $P(q) = \sum_{i=0}^n a_i(q)p^{n-i}(1-q)^i$ où les $a_i(q)$ appartiennent à $\mathbb{Z}[q]$. Ainsi, $\mathbf{ev}(P(q)) = P(1) = a_0(1)p^n$ et $|P(1)|_p \leq 1/p^n$. Alors, pour tout $P(q) \in \mathbb{Z}[q]$,

$$|\mathbf{ev}(P(q))|_p \leq |P(q)|_{\mathfrak{m}}. \quad (4.10)$$

Puisque \mathbf{ev} est un homomorphisme d'anneaux alors cette dernière inégalité implique que \mathbf{ev} est continu. \square

Maintenant soit $\mathbf{F}_q : \mathbb{Z}[q] \rightarrow \mathbb{Z}[q]$ l'automorphisme de $\mathbb{Z}[q]$ donné par $\mathbf{F}_q(P(q)) = P(q^p)$.

Proposition 4.2.3. *L'automorphisme $\mathbf{F}_q : \mathbb{Z}[q] \rightarrow \mathbb{Z}[q]$ est un automorphisme de Frobenius et, pour tout $P(q) \in \mathbb{Z}[q]$, $|\mathbf{F}_q(P(q))|_{\mathfrak{m}} \leq |P(q)|_{\mathfrak{m}}$.*

Démonstration. Montrons que \mathbf{F}_q est continu. Remarquons que, pour tout entier $n > 0$, $\mathbf{F}_q(\mathfrak{m}^n \mathbb{Z}[q]) \subset \mathfrak{m}^n \mathbb{Z}[q]$ car $\mathbf{F}_q(\mathfrak{m} \mathbb{Z}[q]) \subset \mathfrak{m} \mathbb{Z}[q]$ et \mathbf{F}_q est un automorphisme d'anneaux. Alors,

$$|\mathbf{F}_q(P(q))|_{\mathfrak{m}} = |P(q^p)|_{\mathfrak{m}} \leq |P(q)|_{\mathfrak{m}}.$$

De cette dernière inégalité suit que \mathbf{F}_q est continu parce que \mathbf{F}_q est un automorphisme d'anneaux.

Montrons que $|\mathbf{F}_q(x) - x^p|_{\mathfrak{m}} < 1$ pour tout $x \in \mathbb{Z}[q]$. Soit $x = P(q) \in \mathbb{Z}[q]$, alors

$$\mathbf{F}_q(x) - x^p = P(q^p) - P(q)^p.$$

Comme $\pi_p \circ \mathbf{ev}(P(q^p) - P(q)^p) = 0$ alors, d'après la remarque 4.2.1, $P(q^p) - P(q)^p \in \mathfrak{m}$. Ainsi,

$$|\mathbf{F}_q(x) - x^p|_{\mathfrak{m}} < 1.$$

□

Le corps des fractions de $\mathbb{Z}[q]$ est l'anneau $\mathbb{Q}(q)$, alors la norme \mathfrak{m} -adique définie sur $\mathbb{Z}[q]$ s'étend de manière unique à $\mathbb{Q}(q)$. Elle s'étend de la manière suivante : soit $x \in \mathbb{Q}(q)$, alors il existe $x_1, x_2 \in \mathbb{Z}[q]$ tels que $x = \frac{x_1}{x_2}$. Nous posons $|x|_{\mathfrak{m}} = \frac{|x_1|_{\mathfrak{m}}}{|x_2|_{\mathfrak{m}}}$. La valeur de $|x|_{\mathfrak{m}}$ ne dépend pas de l'écriture de x . Ainsi, nous avons muni $\mathbb{Q}(q)$ de la norme ultramétrique \mathfrak{m} -adique. Nous venons de montrer que $\mathbf{F}_q : \mathbb{Z}[q] \rightarrow \mathbb{Z}[q]$ est un automorphisme de Frobenius. Une question naturelle est de savoir si \mathbf{F}_q s'étend en un automorphisme de Frobenius de $\mathbb{Q}(q)$. Malheureusement, ce n'est pas le cas. En effet, montrons que si τ est un automorphisme de $\mathbb{Q}(q)$ tel que τ étend \mathbf{F}_q alors τ n'est pas un automorphisme de Frobenius. Si τ étend \mathbf{F}_q alors $\tau\left(\frac{P(q)}{R(q)}\right) = \frac{P(q^p)}{R(q^p)}$. Puisque $1 - q$ et p appartiennent à $\mathfrak{m} \setminus \mathfrak{m}^2$ alors la norme \mathfrak{m} -adique de $x = \frac{1-q}{p}$ est égale à 1 tandis que la norme \mathfrak{m} -adique de $1 - q^p$ est égale à $1/p^2$ car $1 - q^p = (1 - q)[p]_q$ et ainsi, la norme \mathfrak{m} -adique de $\tau(x) = \frac{1-q^p}{p}$ est égale à $1/p$. Puisque la norme est ultramétrique, alors la norme de $\tau(x) - x^p$ est égale à 1. Par conséquent, τ n'est pas un automorphisme de Frobenius. En conséquence, le corps $\mathbb{Q}(q)$ n'est pas muni d'un automorphisme de Frobenius tel que $q \mapsto q^p$. Par contre, nous pouvons étendre l'automorphisme \mathbf{F}_q en un automorphisme de Frobenius à un sous-anneau de $\mathbb{Q}(q)$. Ce sous anneau est l'anneau $\mathbb{Z}[q]_{\mathfrak{m}}$ qui est la localisation de $\mathbb{Z}[q]$ en l'idéal \mathfrak{m} . Rappelons que $\mathbb{Z}[q]_{\mathfrak{m}}$ est l'ensemble constitué des fractions $\frac{P(q)}{Q(q)}$ telles que $P(q), Q(q) \in \mathbb{Z}[q]$ et $Q(q) \notin \mathfrak{m}$.

Remarque 4.2.4. Soit $Q(q) \in \mathbb{Z}[q]$. Il suit de la définition de la norme \mathfrak{m} -adique que $Q(q) \notin \mathfrak{m}$ si et seulement si $|Q(q)|_{\mathfrak{m}} = 1$. De plus, la remarque 4.2.1 entraîne que $Q(q) \notin \mathfrak{m}$ si et seulement si $Q(1) \notin (p)$, d'où $|Q(q)|_{\mathfrak{m}} = 1$ si et seulement si $|Q(1)|_p = 1$.

Cette remarque entraîne que les applications $\mathbf{ev} : \mathbb{Z}[q]_{\mathfrak{m}} \rightarrow \mathbb{Z}_{(p)}$ et $\mathbf{F}_q : \mathbb{Z}[q]_{\mathfrak{m}} \rightarrow \mathbb{Z}[q]_{\mathfrak{m}}$ données par $\mathbf{ev}\left(\frac{P(q)}{Q(q)}\right) = \frac{P(1)}{Q(1)}$ et $\mathbf{F}_q\left(\frac{P(q)}{Q(q)}\right) = \frac{P(q^p)}{Q(q^p)}$ sont bien définies. La proposition 4.2.5 et la remarque 4.2.4 impliquent la proposition suivante.

Proposition 4.2.5. *L'homomorphisme $\mathbf{ev} : \mathbb{Z}[q]_{\mathfrak{m}} \rightarrow \mathbb{Z}_{(p)}$ donné par $\mathbf{ev}\left(\frac{P(q)}{Q(q)}\right) = \frac{P(1)}{Q(1)}$ est continu et, pour tout $x \in \mathbb{Z}[q]_{\mathfrak{m}}$, $|\mathbf{ev}(x)|_p \leq |x|_{\mathfrak{m}}$.*

La proposition suivante montre que l'anneau $\mathbb{Z}[q]_{\mathfrak{m}}$ possède un automorphisme de Frobenius.

Proposition 4.2.6. *L'automorphisme $\mathbf{F}_q : \mathbb{Z}[q]_{\mathfrak{m}} \rightarrow \mathbb{Z}[q]_{\mathfrak{m}}$ donné par $\mathbf{F}_q\left(\frac{P(q)}{Q(q)}\right) = \frac{P(q^p)}{Q(q^p)}$ est un automorphisme de Frobenius et, pour tout $x \in \mathbb{Z}[q]_{\mathfrak{m}}$, $|\mathbf{F}_q(x)|_{\mathfrak{m}} \leq |x|_{\mathfrak{m}}$.*

Démonstration. La proposition 4.2.3 et la remarque 4.2.4 impliquent que pour tout $x = \frac{P(q)}{Q(q)} \in \mathbb{Z}[q]_{\mathfrak{m}}$,

$$|\mathbf{F}_q(x)|_{\mathfrak{m}} = \frac{|P(q^p)|_{\mathfrak{m}}}{|Q(q^p)|_{\mathfrak{m}}} = |P(q^p)|_{\mathfrak{m}} \leq |P(q)|_{\mathfrak{m}} = \frac{|P(q)|_{\mathfrak{m}}}{|Q(q)|_{\mathfrak{m}}} = |x|_{\mathfrak{m}}.$$

De cette dernière inégalité suit que \mathbf{F}_q est continu car \mathbf{F}_q est un automorphisme d'anneaux.

Montrons que pour tout $x \in \mathbb{Z}[q]_{\mathfrak{m}}$, $|\mathbf{F}_q(x) - x^p|_{\mathfrak{m}} < 1$. Soit $x = \frac{P(q)}{Q(q)} \in \mathbb{Z}[q]_{\mathfrak{m}}$, où $Q(q) \notin \mathfrak{m}$. Alors, on a

$$\mathbf{F}_q(x) - x^p = \frac{P(q^p)Q(q)^p - P(q)^pQ(q^p)}{Q(q)^pQ(q^p)}.$$

Comme $Q(q) \notin \mathfrak{m}$, la remarque 4.2.4 entraîne que $Q(q^p) \notin \mathfrak{m}$ et puisque \mathfrak{m} est un idéal maximal de $\mathbb{Z}[q]$ alors $Q(q)^p Q(q^p) \notin \mathfrak{m}$. De plus,

$$\pi_p \circ \mathbf{ev}(P(q^p)Q(q)^p - P(q)^p Q(q^p)) = 0.$$

Donc, d'après la remarque 4.2.1, $P(q^p)Q(q)^p - P(q)^p Q(q^p) \in \mathfrak{m}$. Ainsi,

$$|\mathbf{F}_q(x) - x^p|_{\mathfrak{m}} < 1.$$

□

Définition 4.2.7. L'anneau $\mathbb{Z}_{q,p}$ est le complété de $\mathbb{Z}[q]_{\mathfrak{m}}$ pour la norme \mathfrak{m} -adique.

Remarque 4.2.8. L'anneau $\mathbb{Z}_{q,p}$ a les propriétés suivantes :

- (1) Tout élément de $\mathbb{Z}_{q,p}$ a une norme inférieure ou égale à 1 parce que $\mathbb{Z}_{q,p}$ est le complété de $\mathbb{Z}[q]_{\mathfrak{m}}$, la norme est ultramétrique et tout élément de $\mathbb{Z}[q]_{\mathfrak{m}}$ a une norme inférieure ou égale à 1.
- (2) L'anneau $\mathbb{Z}_{q,p}$ est un anneau local dont le corps résiduel est l'anneau \mathbb{F}_p . L'anneau $\mathbb{Z}_{q,p}$ est local parce qu'il est complet pour la norme ultramétrique \mathfrak{m} -adique. Maintenant remarquons que l'anneau résiduel de $\mathbb{Z}[q]_{\mathfrak{m}}$ est \mathbb{F}_p parce que $\mathbb{Z}[q]_{\mathfrak{m}}/\mathfrak{m}\mathbb{Z}[q]_{\mathfrak{m}} = \mathbb{F}_p$. Comme $\mathbb{Z}_{q,p}$ est le complété de $\mathbb{Z}[q]_{\mathfrak{m}}$ pour la norme \mathfrak{m} -adique alors l'anneau résiduel de $\mathbb{Z}_{q,p}$ et celui de $\mathbb{Z}[q]_{\mathfrak{m}}$ sont égaux, d'où l'anneau résiduel de $\mathbb{Z}_{q,p}$ est \mathbb{F}_p .

Remarque 4.2.9. D'après la proposition 4.2.5, l'homomorphisme $\mathbf{ev} : \mathbb{Z}[q]_{\mathfrak{m}} \rightarrow \mathbb{Z}_{(p)}$ est continu. Alors, par continuité il s'étend en un homomorphisme continu $\mathbf{ev} : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_p$. De même, d'après la proposition 4.2.6, l'automorphisme $\mathbf{F}_q : \mathbb{Z}[q]_{\mathfrak{m}} \rightarrow \mathbb{Z}[q]_{\mathfrak{m}}$ est continu. Alors, par continuité il s'étend en un automorphisme $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$.

La proposition suivante découle de la construction des homomorphismes \mathbf{ev} et \mathbf{F}_q .

Proposition 4.2.10. L'automorphisme $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$ est un automorphisme de Frobenius de $\mathbb{Z}_{q,p}$ et $\mathbf{ev} \circ \mathbf{F}_q = \mathbf{ev}$, où $\mathbf{ev} : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_p$.

Nous appelons l'automorphisme $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$, l'automorphisme de Frobenius de $\mathbb{Z}_{q,p}$.

Munissons l'anneau $\mathbb{Z}_{q,p}[[z]]$ de la norme de Gauss, $|\sum_{n \geq 0} a(n)z^n|_{\mathcal{G}} = \sup\{|a(n)|_{\mathfrak{m}}\}_{n \geq 0}$. L'anneau $\mathbb{Z}_{q,p}[[z]]$ est complet pour la norme de Gauss car $\mathbb{Z}_{q,p}$ est complet et l'anneau résiduel de $\mathbb{Z}_{q,p}[[z]]$ est l'anneau $\mathbb{F}_p[[z]]$ parce que l'anneau résiduel de $\mathbb{Z}_{q,p}$ est \mathbb{F}_p . Maintenant nous allons construire un sous anneau de $\mathbb{Z}_{q,p}[[z]]$ dont le corps résiduel est contenu dans $\mathbb{F}_p(z)$.

Définition 4.2.11. Soient $S = \{P(z) \in \mathbb{Z}_{q,p}[z] : |P(0)|_{\mathfrak{m}} = 1\}^3$ et $\mathbb{Z}_{q,p}[z]_S$ la localisation de $\mathbb{Z}_{q,p}[z]$ en S . L'anneau $E_{\mathbb{Z}_{q,p}}$ est le complété de $\mathbb{Z}_{q,p}[z]_S$ dans $\mathbb{Z}_{q,p}[[z]]$ pour la norme de Gauss.

Soit $\mathbf{F} : \mathbb{Z}_p[[z]] \rightarrow \mathbb{Z}_p[[z]]$ l'automorphisme donné par $\mathbf{F}(\sum_{n \geq 0} a_n z^n) = \sum_{n \geq 0} a_n z^{np}$. L'automorphisme \mathbf{F} est l'automorphisme de Frobenius de $\mathbb{Z}_p[[z]]$.

Dans la proposition suivante nous énonçons quelques propriétés de l'anneau $E_{\mathbb{Z}_{q,p}}$.

3. L'ensemble S est un ensemble multiplicatif, c'est-à-dire, que pour tout $P(z), Q(z) \in S$, on a $P(z)Q(z) \in S$.

Proposition 4.2.12. (1) L'anneau $E_{\mathbb{Z},q,p}$ est contenu dans $\mathbb{Z}_{q,p}[[z]]$ et son anneau résiduel est contenu dans $\mathbb{F}_p(z)$.

(2) L'anneau $E_{\mathbb{Z},q,p}$ est muni d'un automorphisme continu σ_q donné par

$$\sigma_q\left(\sum_{n \geq 0} a_n z^n\right) = \sum_{n \geq 0} a_n q^n z^n$$

et d'une application continue δ_q donnée par

$$\delta_q(f(z)) = \frac{\sigma_q(f) - f}{q - 1}.$$

(3) L'automorphisme $\mathbf{F}_q : E_{\mathbb{Z},q,p} \rightarrow E_{\mathbb{Z},q,p}$ donné par

$$\mathbf{F}_q\left(\sum_{n \geq 0} a_n z^n\right) = \sum_{n \geq 0} \mathbf{F}_q(a_n) z^{np}$$

est un automorphisme de Frobenius.

(4) On a l'homomorphisme continu $\mathbf{ev} : E_{\mathbb{Z},q,p} \rightarrow E_p \cap \mathbb{Z}_p[[z]]$ donné par

$$\mathbf{ev}\left(\sum_{n \geq 0} a_n z^n\right) = \sum_{n \geq 0} \mathbf{ev}(a_n) z^n,$$

où E_p est le corps des éléments analytiques.

(5) Pour tout entier $h > 0$, on a $\mathbf{ev} \circ \mathbf{F}_q^h = \mathbf{F}_q^h \circ \mathbf{ev}$.

Le lecteur trouvera la démonstration de cette proposition à la fin de cette partie. Considérons l'opérateur aux q -différences d'ordre n

$$L_q := \sigma_q^n + a_1(z)\sigma_q^{n-1} + \cdots + a_{n-1}(z)\sigma_q + a_n(z) \in E_{\mathbb{Z},q,p}[\sigma_q]. \quad (4.11)$$

La matrice compagnon de L_q est la matrice

$$A_q = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & \cdots & -a_1 \end{pmatrix}.$$

Nous posons $A_q^{\mathbf{F}_q^h}$ comme la matrice obtenue après avoir appliqué h -fois l'automorphisme \mathbf{F}_q à chaque entrée de A_q .

Définition 4.2.13 (*Structure de Frobenius forte*). Soient $L_q \in E_{\mathbb{Z},q,p}[\sigma_q]$ défini comme en (4.11) et A_q la matrice compagnon de L_q . Nous disons que L_q possède une structure de Frobenius forte de période h s'il existe une matrice $H_q \in \mathrm{GL}_n(E_{\mathbb{Z},q,p})$ telle que

$$\sigma_q(H_q)A_q^{\mathbf{F}_q^h} = A_q H_q. \quad (4.12)$$

Si $L_q \in E_{\mathbb{Z},q,p}[\sigma_q]$ possède une structure de Frobenius forte de période h , nous disons qu'une matrice $H_q \in \mathrm{GL}_n(E_{\mathbb{Z},q,p})$ est une *matrice de passage de Frobenius* de L_q si H_q vérifie l'égalité (4.12). En général, nous disons que le système aux q -différences $\sigma_q X = A_q X$

avec $A_q \in \mathcal{M}_n(E_{\mathbb{Z},q,p})$ possède une structure de Frobenius forte de période h s'il existe une matrice $H_q \in \text{GL}_n(E_{\mathbb{Z},q,p})$ telle que $\sigma_q(H_q)A_q^{\mathbf{F}_q^h} = A_qH_q$.

Nous obtenons par récurrence sur $i > 0$ que, $\sigma_q^i = \sum_{j=0}^i \binom{i}{j} (q-1)^j \delta_q^j$, où $\delta_q = \frac{\sigma_q - 1}{q-1}$. Soit L_q défini comme en (4.11). Donc, si nous réécrivons $\frac{1}{(q-1)^n} L_q$ en fonction de δ_q , nous obtenons le nouvel opérateur

$$L_{\delta_q} = \delta_q^n + b_1(z)\delta_q^{n-1} + \cdots + b_{n-1}(z)\delta_q + b_n(z), \quad (4.13)$$

où, pour $i \in \{1, \dots, n\}$, on a

$$b_i(z) = \frac{1}{(q-1)^i} \sum_{k=n-i}^n \binom{k}{n-i} a_{n-k}(z).$$

Considérons le système $\delta_q X = C_q X$, où C_q est la matrice compagnon de L_{δ_q} . Nous voulons définir la notion de structure de Frobenius pour ce système. Précédemment, nous avons défini la structure de Frobenius forte pour les systèmes de la forme $\sigma_q X = A_q X$. Puisque $\delta_q = \frac{\sigma_q - 1}{q-1}$, alors à partir du système $\delta_q X = C_q X$, nous avons que $\sigma_q X = ((q-1)C_q + Id)X$, où Id est la matrice identité de taille n . Soit $B_q = (q-1)C_q + Id$. Donc, nous dirons que le système $\delta_q X = C_q X$ possède une structure de Frobenius forte si B_q est une matrice à coefficients dans $E_{\mathbb{Z},q,p}$ et si le système $\sigma_q X = B_q X$ possède une structure de Frobenius forte. La matrice B_q est appelée *la matrice associée à L_{δ_q}* .

Définition 4.2.14. Soient $L_{\delta_q} \in E_{\mathbb{Z},q,p}[\delta_q]$ défini comme en (4.13) et C_q la matrice compagnon de L_{δ_q} . L'opérateur différentiel L_{δ_q} possède une structure de Frobenius forte si le système $\delta_q X = C_q X$ a une structure de Frobenius forte.

Nous finissons cette partie en démontrant la proposition 4.2.12.

Démonstration de la proposition 4.2.12. Rappelons que $S = \{P(z) \in \mathbb{Z}_{q,p}[z] : |P(0)|_{\mathfrak{m}} = 1\}$.

Démonstration de (1).

Soit x un élément de $E_{\mathbb{Z},q,p}$, alors $x = \lim_{n \rightarrow \infty} x_n$, où $x_n \in \mathbb{Z}_{q,p}[z]_S$. Pour chaque entier $n > 0$, écrivons $x_n = P_n(z)/Q_n(z)$ avec $P_n(z), Q_n(z) \in \mathbb{Z}_{q,p}[z]$ et $Q_n(z) \in S$. Par définition de l'ensemble S , $|Q_n(0)|_{\mathfrak{m}} = 1$. Puisque $\mathbb{Z}_{q,p}$ est un anneau local complet alors $1/Q_n(0) \in \mathbb{Z}_{q,p}$ et ainsi, $1/Q_n(z) \in \mathbb{Z}_{q,p}[[z]]$. Par conséquent, pour chaque $n > 0$, $x_n = P_n(z)/Q_n(z) \in \mathbb{Z}_{q,p}[[z]]$. Comme $\mathbb{Z}_{q,p}[[z]]$ est complet pour la norme de Gauss, alors $x \in \mathbb{Z}_{q,p}[[z]]$, d'où $E_{\mathbb{Z},q,p} \subset \mathbb{Z}_{q,p}[[z]]$.

Montrons maintenant que l'anneau résiduel de $E_{\mathbb{Z},q,p}$ est contenu dans $\mathbb{F}_p(z)$. Rappelons que pour $a \in \mathbb{Z}_{q,p}$ nous notons par \bar{a} la réduction de a modulo l'idéal maximal de $\mathbb{Z}_{q,p}$. Puisque $E_{\mathbb{Z},q,p}$ est le complété de $\mathbb{Z}_{q,p}[z]_S$ alors l'anneau résiduel de $E_{\mathbb{Z},q,p}$ est justement l'anneau résiduel de $\mathbb{Z}_{q,p}[z]_S$. Donc, il suffit de voir que l'anneau résiduel de $\mathbb{Z}_{q,p}[z]_S$ est contenu dans $\mathbb{F}_p(z)$. Soit $\xi : \mathbb{Z}_{q,p}[z]_S \rightarrow \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ donné par

$$\xi \left(\frac{\sum_{i=0}^n a_i z^i}{\sum_{j=0}^m b_j z^j} \right) = \frac{\sum_{i=0}^n \bar{a}_i z^i}{\sum_{j=0}^m \bar{b}_j z^j}.$$

Notons que ξ est bien défini car $|b_0|_{\mathfrak{m}} = 1$ et par conséquent $\bar{b}_0 \neq 0$. De plus, ξ est un homomorphisme d'anneaux. L'idéal maximal de $\mathbb{Z}_{q,p}[z]_S$ est constitué des éléments qui ont une norme inférieure à 1, et $\xi(x_1(z)/x_2(z)) = 0$ si et seulement si, $|x_1(z)/x_2(z)|_{\mathcal{G}} < 1$, ce qui revient à dire que $x_1(z)/x_2(z)$ appartient à l'idéal maximal de $\mathbb{Z}_{q,p}[z]_S$. Ainsi, si A est

l'anneau résiduel de $\mathbb{Z}_{q,p}[z]_S$ on a l'homomorphisme injectif $\bar{\xi} : A \rightarrow \mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$ donné par $\bar{\xi}\left(\frac{x_1(z)}{x_2(z)}\right) = \xi(x_1(z)/x_2(z))$. D'où l'anneau résiduel de $E_{\mathbb{Z},q,p}$ est contenu dans $\mathbb{F}_p(z) \cap \mathbb{F}_p[[z]]$.

Démonstration de (2).

Soit $\sigma_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ donné par $\sigma_q(\sum_{n \geq 0} a_n z^n) = \sum_{n \geq 0} a_n q^n z^n$. Remarquons d'abord que σ_q est un homomorphisme d'anneaux et qu'il est continu pour la norme de Gauss car $|q|_m = 1$. Montrons maintenant que $\sigma_q(E_{\mathbb{Z},q,p}) \subset E_{\mathbb{Z},q,p}$. Pour montrer cela, il suffit de montrer que $\sigma_q(\mathbb{Z}_{q,p}[z]_S) \subset \mathbb{Z}_{q,p}[z]_S$ parce que σ_q est continu pour la norme de Gauss et $E_{\mathbb{Z},q,p}$ est le complété de $\mathbb{Z}_{q,p}[z]_S$ pour la norme de Gauss. En effet, il est clair que si $Q(z) \in S$ alors $Q(qz) \in S$, d'où si $\frac{P(z)}{Q(z)} \in \mathbb{Z}_{q,p}[z]_S$ alors $\sigma_q\left(\frac{P(z)}{Q(z)}\right) = \frac{P(qz)}{Q(qz)} \in \mathbb{Z}_{q,p}[z]_S$. Par conséquent, $\sigma_q(\mathbb{Z}_{q,p}[z]_S) \subset \mathbb{Z}_{q,p}[z]_S$ et ainsi, $\sigma_q(E_{\mathbb{Z},q,p}) \subset E_{\mathbb{Z},q,p}$, d'où l'automorphisme $\sigma_q : E_{\mathbb{Z},q,p} \rightarrow E_{\mathbb{Z},q,p}$ donné par $\sigma_q(\sum_{n \geq 0} a_n z^n) = \sum_{n \geq 0} a_n q^n z^n$ est continu.

Maintenant, soit $\delta_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ donné par $\delta_q(f) = \frac{\sigma_q(f) - f}{q-1}$. Montrons d'abord que δ_q est bien défini, c'est-à-dire que, pour tout $\sum_{n \geq 0} a_n z^n \in \mathbb{Z}_{q,p}[[z]]$, $\delta_q(\sum_{n \geq 0} a_n z^n) \in \mathbb{Z}_{q,p}[[z]]$. En effet, on a

$$\begin{aligned} \delta_q\left(\sum_{n \geq 0} a_n z^n\right) &= \frac{\sum_{n \geq 0} a_n q^n z^n - \sum_{n \geq 0} a_n z^n}{q-1} \\ &= \sum_{n \geq 0} \frac{q^n - 1}{q-1} a_n z^n \\ &= \sum_{n \geq 1} (1 + q + \dots + q^{n-1}) a_n z^n. \end{aligned}$$

D'où $\delta_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ est bien défini et de plus, il suit que δ_q est continu pour la norme de Gauss car, pour tout entier $n > 0$, $|1 + q + \dots + q^{n-1}|_m \leq 1$. Maintenant, montrons que $\delta_q(E_{\mathbb{Z},q,p}) \subset E_{\mathbb{Z},q,p}$. Pour montrer cela il suffit de montrer que $\delta_q(\mathbb{Z}_{q,p}[z]_S) \subset \mathbb{Z}_{q,p}[z]_S$ parce que δ_q est continu pour la norme de Gauss et $E_{\mathbb{Z},q,p}$ est le complété de $\mathbb{Z}_{q,p}[z]_S$ pour la norme de Gauss. En effet, si $x(z) = \frac{\sum_{i=0}^n a_i z^i}{\sum_{j=0}^m b_j z^j} \in \mathbb{Z}_{q,p}[z]_S$, alors

$$\begin{aligned} \delta_q(x(z)) &= \frac{x(qz) - x(z)}{q-1} = \frac{1}{q-1} \frac{\sum_{i=0}^n a_i q^i z^i \sum_{j=0}^m b_j z^j - \sum_{i=0}^n a_i z^i \sum_{j=0}^m b_j q^j z^j}{\sum_{i=0}^m b_j z^j \sum_{j=0}^m b_j q^j z^j} \\ &= \frac{1}{q-1} \frac{\sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j (q^i - q^j)\right) z^k}{\sum_{i=0}^m b_j z^j \sum_{j=0}^m b_j q^j z^j} \\ &= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \frac{(q^i - q^j)}{q-1}\right) z^k \cdot \frac{1}{\sum_{i=0}^m b_j z^j \sum_{j=0}^m b_j q^j z^j}. \end{aligned}$$

Remarquons que $\sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \frac{(q^i - q^j)}{q-1}\right) z^k \in \mathbb{Z}_{q,p}[z]$ car, pour tout couple $(i, m) \in \mathbb{Z}_{\geq 0}^2$, $\frac{(q^i - q^j)}{q-1} \in \mathbb{Z}[q]$ et puisque S est multiplicatif, $\sum_{i=0}^n b_j z^j$ et $\sum_{i=0}^n b_j q^j z^j$ appartiennent à S alors $\sum_{i=0}^n b_j z^j \sum_{j=0}^m b_j q^j z^j \in S$. Donc, $\delta_q(x(z)) \in \mathbb{Z}_{q,p}[z]_S$. Par conséquent, on a $\delta_q(\mathbb{Z}_{q,p}[z]_S) \subset \mathbb{Z}_{q,p}[z]_S$, d'où l'application $\delta_q : E_{\mathbb{Z},q,p} \rightarrow E_{\mathbb{Z},q,p}$ donnée par $\delta_q(f) = \frac{\sigma_q(f) - f}{q-1}$ est continue.

Démonstration de (3).

Soit $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ donné par $\mathbf{F}_q(\sum_{n \geq 0} a_n z^n) = \sum_{n \geq 0} \mathbf{F}_q(a_n) z^{np}$, où $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$ est l'automorphisme de Frobenius de $\mathbb{Z}_{q,p}$. Alors, $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ est un automorphisme d'anneaux.

Montrons maintenant que $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ est un automorphisme de Frobenius. Remarquons d'abord que $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ est continu pour la norme de Gauss car $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$ est continu. Montrons maintenant que, pour tout $\sum_{n \geq 0} a_n z^n \in \mathbb{Z}_{q,p}[[z]]$, $|\mathbf{F}_q(\sum_{n \geq 0} a_n z^n) - (\sum_{n \geq 0} a_n z^n)^p|_{\mathcal{G}} < 1$. Rappelons que cela revient à montrer que $\mathbf{F}_q(\sum_{n \geq 0} a_n z^n) \equiv (\sum_{n \geq 0} a_n z^n)^p \pmod{\mathfrak{m}_{\mathbb{Z}_{q,p}} \mathbb{Z}_{q,p}[[z]]}$, où $\mathfrak{m}_{\mathbb{Z}_{q,p}}$ est l'idéal maximal de $\mathbb{Z}_{q,p}$. Comme $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$ est l'automorphisme de Frobenius de $\mathbb{Z}_{q,p}$ et le corps résiduel de $\mathbb{Z}_{q,p}$ est de caractéristique p alors,

$$\begin{aligned} \mathbf{F}_q \left(\sum_{n \geq 0} a_n z^n \right) &= \sum_{n \geq 0} \mathbf{F}_q(a_n) z^{np} \\ &\equiv \sum_{n \geq 0} a_n^p z^{np} \pmod{\mathfrak{m}_{\mathbb{Z}_{q,p}} \mathbb{Z}_{q,p}[[z]]} \\ &\equiv \left(\sum_{n \geq 0} a_n z^n \right)^p \pmod{\mathfrak{m}_{\mathbb{Z}_{q,p}} \mathbb{Z}_{q,p}[[z]]}. \end{aligned}$$

Maintenant, montrons que $\mathbf{F}_q(E_{\mathbb{Z},q,p}) \subset E_{\mathbb{Z},q,p}$. Pour montrer cela il suffit de montrer que $\mathbf{F}_q(\mathbb{Z}_{q,p}[z]_S) \subset \mathbb{Z}_{q,p}[z]_S$ car \mathbf{F}_q est continu pour la norme de Gauss et $E_{\mathbb{Z},q,p}$ est le complété de $\mathbb{Z}_{q,p}[z]_S$ pour la norme de Gauss. En effet, soit $P(z)/Q(z) \in \mathbb{Z}_{q,p}[z]_S$, où $P(z) \in \mathbb{Z}_{q,p}[z]$ et $Q(z) \in S$. Par définition de l'ensemble S , $|Q_n(0)|_{\mathfrak{m}} = 1$. Puisque $\mathbb{Z}_{q,p}$ est un anneau local complet alors $1/Q_n(0) \in \mathbb{Z}_{q,p}$ et ainsi, $1/Q_n(z) \in \mathbb{Z}_{q,p}[[z]]$ et comme $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ est un automorphisme d'anneaux alors, $\mathbf{F}_q \left(\frac{P(z)}{Q(z)} \right) = \frac{\mathbf{F}_q(P(z))}{\mathbf{F}_q(Q(z))}$. Il est clair que $\mathbf{F}_q(P(z)) \in \mathbb{Z}_{q,p}[z]$. Montrons maintenant que $\mathbf{F}_q(Q(z)) \in S$. Écrivons $Q(z) = \sum_{j=0}^m b_j z^j$ alors $|b_0|_{\mathfrak{m}} = 1$ car $Q(z) \in S$ et $\mathbf{F}_q(Q(z)) = \sum_{j=0}^m \mathbf{F}_q(b_j) z^{jp}$. D'une part, comme $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$ est l'automorphisme de Frobenius de $\mathbb{Z}_{q,p}$, alors $|\mathbf{F}_q(b_0) - b_0^p|_{\mathfrak{m}} < 1$ et d'autre part, comme $|b_0^p|_{\mathfrak{m}} = 1$ et la norme est ultramétrique, alors on a

$$|\mathbf{F}_q(b_0)|_{\mathfrak{m}} = |\mathbf{F}_q(b_0) - b_0^p + b_0^p|_{\mathfrak{m}} = \max\{|\mathbf{F}_q(b_0) - b_0^p|_{\mathfrak{m}}, |b_0^p|_{\mathfrak{m}}\} = 1.$$

Par conséquent, $\mathbf{F}_q(Q(z)) \in S$ et ainsi $\mathbf{F}_q \left(\frac{P(z)}{Q(z)} \right) \in \mathbb{Z}_{q,p}[z]_S$. C'est pourquoi $\mathbf{F}_q(\mathbb{Z}_{q,p}[z]_S) \subset \mathbb{Z}_{q,p}[z]_S$, et ainsi l'automorphisme $\mathbf{F}_q : E_{\mathbb{Z},q,p} \rightarrow E_{\mathbb{Z},q,p}$ donné par $\mathbf{F}_q \left(\sum_{n \geq 0} a_n z^n \right) = \sum_{n \geq 0} \mathbf{F}_q(a_n) z^{np}$ est un automorphisme de Frobenius de $E_{\mathbb{Z},q,p}$.

Démonstration de (4).

Soit $\mathbf{ev} : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_p[[z]]$ donné par $\mathbf{ev}(\sum_{n \geq 0} a_n z^n) = \sum_{n \geq 0} \mathbf{ev}(a_n) z^n$, où $\mathbf{ev} : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_p$ est l'homomorphisme continu construit dans la remarque 4.2.9. Montrons d'abord que l'homomorphisme $\mathbf{ev} : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_p[[z]]$ est tel que $\mathbf{ev}(\mathbb{Z}_{q,p}[z]_S) \subset E_p \cap \mathbb{Z}_p[[z]]$. Soit $P(z)/Q(z) \in \mathbb{Z}_{q,p}[z]_S$, où $P(z) \in \mathbb{Z}_{q,p}[z]$ et $Q(z) \in S$. Écrivons $Q(z) = \sum_{j=0}^m b_j z^j$ et comme $Q(z) \in S$, alors $|b_0|_{\mathfrak{m}} = 1$. Rappelons que $\mathbb{Z}_{q,p}$ est le complété de $\mathbb{Z}[q]_{\mathfrak{m}}$ pour la norme \mathfrak{m} -adique. Donc $b_0 = \lim_{n \rightarrow \infty} x_n$, où $x_n \in \mathbb{Z}[q]_{\mathfrak{m}}$. Notamment, pour $\epsilon > 0$ assez petit, il existe un entier $N > 0$ tel que, pour tout $n \geq N$, $|b_0 - x_n|_{\mathfrak{m}} < \epsilon$. Comme la norme est ultramétrique et $|b_0|_{\mathfrak{m}} = 1$ alors, pour tout $n \geq N$, $|x_n|_{\mathfrak{m}} = 1$. Écrivons $x_n = R_n(q)/T_n(q) \in \mathbb{Z}[q]_{\mathfrak{m}}$, où $R_n(q), T_n(q) \in \mathbb{Z}[q]$ et $T_n(q) \notin \mathfrak{m}$. Puisque, pour tout $n \geq N$, $|x_n|_{\mathfrak{m}} = 1$ et $|T_n(q)|_{\mathfrak{m}} = 1$, alors $|R_n(q)|_{\mathfrak{m}} = 1$. Par conséquent, pour tout $n \geq N$, $R_n(q)$ et $T_n(q)$ n'appartiennent pas à \mathfrak{m} . Il suit donc de la remarque 4.2.1 que, pour tout

$n \geq N$, $\mathbf{ev}(R_n(q))$ et $\mathbf{ev}(T_n(q))$ n'appartiennent pas $p\mathbb{Z}$, d'où $|\mathbf{ev}(x_n)|_p = 1$ pour tout $n \geq N$. Par construction de $\mathbf{ev} : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_p$ on a que, $\mathbf{ev}(b_0) = \lim_{n \rightarrow \infty} \mathbf{ev}(x_n)$. Puisque la norme est ultramétrique et, pour tout $n \geq N$, $|\mathbf{ev}(x_n)|_p = 1$ alors $|\mathbf{ev}(b_0)|_p = 1$. Par conséquent, $1/\mathbf{ev}(Q(z)) \in \mathbb{Z}_p[[z]]$. Finalement, il est clair que $\mathbf{ev}(P(z)) \in \mathbb{Z}_p[[z]]$ et que $\mathbf{ev}(P(z))/\mathbf{ev}(Q(z)) \in E_p$ puisque $\mathbb{Q}_p(z) \subset E_p$ et $\mathbf{ev}(P(z))/\mathbf{ev}(Q(z)) \in \mathbb{Q}_p(z)$. Alors on a

$$\mathbf{ev} \left(\frac{P(z)}{Q(z)} \right) = \frac{\mathbf{ev}(P(z))}{\mathbf{ev}(Q(z))} \in E_p \cap \mathbb{Z}_p[[z]].$$

Ainsi on a l'homomorphisme d'anneaux $\mathbf{ev} : \mathbb{Z}_{q,p}[z]_S \rightarrow E_p \cap \mathbb{Z}_p[[z]]$ qui est continu pour la norme de Gauss car $\mathbf{ev} : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_p$ est continu. Il s'étend alors par continuité en $\mathbf{ev} : E_{\mathbb{Z},q,p} \rightarrow E_p \cap \mathbb{Z}_p[[z]]$.

Démonstration de (5).

D'une part, rappelons que d'après la remarque 4.2.9 on a l'automorphisme continu $\mathbf{F}_q : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_{q,p}$ et l'homomorphisme continu $\mathbf{ev} : \mathbb{Z}_{q,p} \rightarrow \mathbb{Z}_p$ et, d'après la proposition 4.2.10, pour tout $a \in \mathbb{Z}_{q,p}$, on a

$$\mathbf{ev}(\mathbf{F}_q(a)) = \mathbf{ev}(a). \quad (4.14)$$

D'autre part, nous avons l'automorphisme $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ défini par

$$\mathbf{F}_q \left(\sum_{n \geq 0} a_n z^n \right) = \sum_{n \geq 0} \mathbf{F}_q(a_n) z^{np}$$

et $\mathbf{ev} \left(\sum_{n \geq 0} a_n z^n \right) = \sum_{n \geq 0} \mathbf{ev}(a_n) z^n$. Nous voulons voir que pour ces deux derniers homomorphismes on a l'égalité $\mathbf{ev} \circ \mathbf{F}_q^h = \mathbf{F}^h \circ \mathbf{ev}$, où $\mathbf{F} : \mathbb{Z}_p[[z]] \rightarrow \mathbb{Z}_p[[z]]$ est tel que $\mathbf{F}(z) = z^p$. Soit $\sum_{n \geq 0} a_n z^n \in \mathbb{Z}_{q,p}$. Alors on a

$$\mathbf{ev} \left(\mathbf{F}_q^h \left(\sum_{n \geq 0} a_n z^n \right) \right) = \sum_{n \geq 0} \mathbf{ev}(\mathbf{F}_q^h(a_n)) z^{np^h}$$

et

$$\mathbf{F}^h \left(\mathbf{ev} \left(\sum_{n \geq 0} a_n z^n \right) \right) = \sum_{n \geq 0} \mathbf{ev}(a_n) z^{np^h}.$$

Donc, $\mathbf{ev} \left(\mathbf{F}_q^h \left(\sum_{n \geq 0} a_n z^n \right) \right) = \mathbf{F}^h \left(\mathbf{ev} \left(\sum_{n \geq 0} a_n z^n \right) \right)$ si et seulement si, pour tout entier $n \geq 0$, $\mathbf{ev}(\mathbf{F}_q^h(a_n)) = \mathbf{ev}(a_n)$. Mais il suit de (4.14) que, pour tout entier $n \geq 0$, $\mathbf{ev}(\mathbf{F}_q^h(a_n)) = \mathbf{ev}(a_n)$. D'où on obtient que

$$\mathbf{ev} \left(\mathbf{F}_q^h \left(\sum_{n \geq 0} a_n z^n \right) \right) = \mathbf{F}^h \left(\mathbf{ev} \left(\sum_{n \geq 0} a_n z^n \right) \right).$$

□

4.3 Résultats principaux

Le théorème suivant est une réponse à la question 6.

Théorème 4.3.1. Soient p un nombre premier, $L_{\delta_q} = \delta_q^n + b_1(z)\delta_q^{n-1} + \dots + b_{n-1}(z)\delta_q + b_n(z) \in E_{\mathbb{Z},q,p}[\delta_q]$ et $\mathbf{ev}(L_{\delta_q}) = \delta^n + \mathbf{ev}(b_1(z))\delta^{n-1} + \dots + \mathbf{ev}(b_{n-1}(z))\delta + \mathbf{ev}(b_n(z)) \in E_p[\delta]$. Si L_{δ_q} possède une structure de Frobenius forte de période h , alors l'opérateur différentiel $\mathbf{ev}(L_{\delta_q})$ possède une structure de Frobenius forte de période h . De plus, si H_q est une matrice de passage de Frobenius de l'opérateur L_{δ_q} alors la matrice $\mathbf{ev}(H_q)$ est une matrice de passage de Frobenius pour p de l'opérateur différentiel $\mathbf{ev}(L_{\delta_q})$, c'est-à-dire $\delta(\mathbf{ev}(H_q)) = B\mathbf{ev}(H_q) - p^h\mathbf{ev}(H_q)B(z^{p^h})$, où B est la matrice compagnon de $\mathbf{ev}(L_{\delta_q})$.

Démonstration. Nous allons montrer que l'opérateur différentiel

$$\mathbf{ev}(L_{\delta_q}) := \delta^n + \mathbf{ev}(b_1(z))\delta^{n-1} + \dots + \mathbf{ev}(b_1(z))\delta + \mathbf{ev}(b_n(z)) \in E_p[\delta]$$

est muni d'une structure de Frobenius forte de période h . Par définition la matrice associée à L_{δ_q} est

$$B_q = \begin{pmatrix} 1 & (q-1) & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & (q-1) \\ -(q-1)b_n(z) & -(q-1)b_{n-1}(z) & \dots & -(q-1)b_1(z) + 1 \end{pmatrix}.$$

Alors,

$$\frac{B_q - I_n}{q-1} = \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ -b_n(z) & -b_{n-1}(z) & \dots & -b_1(z) \end{pmatrix}.$$

Ainsi, $B := \mathbf{ev}\left(\frac{B_q - I_n}{q-1}\right)$ est la matrice compagnon de l'opérateur différentiel $\mathbf{ev}(L_{\delta_q})$. Notons que la matrice B est à coefficients dans l'anneau $E_p \cap \mathbb{Z}_p[[z]]$. Par hypothèse, il existe $G_q \in \mathrm{GL}_n(E_{\mathbb{Z},q,p})$ telle que

$$\sigma_q(G_q)B_q^{\mathbf{F}_q^h} = B_qG_q. \quad (4.15)$$

Il suit de l'égalité (4.15) que

$$\begin{aligned} \sigma_q(G_q)B_q^{\mathbf{F}_q^h} = B_qG_q &\iff \sigma_q(G_q)B_q^{\mathbf{F}_q^h} - I_n = B_qG_q - I_n \\ &\iff \sigma_q(G_q)B_q^{\mathbf{F}_q^h} - \sigma_q(G_q) + \sigma_q(G_q) - I_n = B_qG_q - G_q + G_q - I_n \\ &\iff \sigma_q(G_q)[B_q^{\mathbf{F}_q^h} - I_n] + \sigma_q(G_q) - Id_n = [B_q - Id_n]G_q + G_q - I_n \\ &\iff \sigma_q(G_q) \cdot \frac{B_q^{\mathbf{F}_q^h} - I_n}{q-1} + \frac{\sigma_q(G_q) - I_n}{q-1} = \frac{B_q - I_n}{q-1} \cdot G_q + \frac{G_q - I_n}{q-1} \\ &\iff \frac{\sigma_q(G_q) - I_n}{q-1} - \frac{G_q - I_n}{q-1} = \frac{B_q - I_n}{q-1} \cdot G_q - \sigma_q(G_q) \cdot \frac{B_q^{\mathbf{F}_q^h} - I_n}{q-1}. \end{aligned}$$

De cette dernière égalité on obtient que

$$\frac{\sigma_q(G_q) - G_q}{q-1} = \left(\frac{B_q - I_n}{q-1}\right) G_q - \sigma_q(G_q) \left(\frac{B_q^{\mathbf{F}_q^h} - I_n}{q-1}\right). \quad (4.16)$$

Remarquons que pour $\sum_{i \geq 0} a_i z^i \in \mathbb{Z}_{q,p}[[z]]$ on a

$$\begin{aligned} \mathbf{ev} \left(\sigma_q \left(\sum_{i \geq 0} a_i z^i \right) \right) &= \mathbf{ev} \left(\sum_{i \geq 0} a_i q^i z^i \right) \\ &= \sum_{i \geq 0} \mathbf{ev}(a_i q^i) z^i \\ &= \sum_{i \geq 0} \mathbf{ev}(a_i) z^i \\ &= \mathbf{ev} \left(\sum_{i \geq 0} a_i z^i \right) \end{aligned}$$

car $\mathbf{ev}(q) = 1$.

Par conséquent, $\mathbf{ev}(\sigma_q(G_q)) = \mathbf{ev}(G_q)$. Maintenant, soit $\sum_{i \geq 0} a_i z^i \in \mathbb{Z}_{q,p}[[z]]$ alors, on a

$$\begin{aligned} \frac{\sigma_q(\sum_{i \geq 0} a_i z^i) - \sum_{i \geq 0} a_i z^i}{q-1} &= \frac{\sum_{i \geq 0} a_i q^i z^i - \sum_{i \geq 0} a_i z^i}{q-1} \\ &= \frac{\sum_{i \geq 1} (q^i - 1) a_i z^i}{q-1} \\ &= \sum_{i \geq 1} (1 + q \cdots + q^{i-1}) a_i z^i \in \mathbb{Z}_{q,p}[[z]]. \end{aligned}$$

Puisque pour tout $i \geq 1$, $\mathbf{ev}(1 + q \cdots + q^{i-1}) = i$ alors,

$$\mathbf{ev} \left(\frac{\sigma_q(\sum_{i \geq 0} a_i z^i) - \sum_{i \geq 0} a_i z^i}{q-1} \right) = \sum_{i \geq 1} i \mathbf{ev}(a_i) z^i = \delta \mathbf{ev} \left(\sum_{i \geq 0} a_i z^i \right),$$

où $\delta = z \frac{d}{dz}$. Ainsi, $\mathbf{ev} \left(\frac{\sigma_q(G_q) - G_q}{q-1} \right) = \delta \mathbf{ev}(G_q)$. Notons que

$$\frac{B_q^{\mathbf{F}_q^h} - I_n}{q-1} = \begin{pmatrix} 0 & \frac{(q^{p^h}-1)}{q-1} & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \frac{(q^{p^h}-1)}{q-1} \\ -\frac{(q^{p^h}-1)}{q-1} \mathbf{F}_q(b_n(z)) & -\frac{(q^{p^h}-1)}{q-1} \mathbf{F}_q(b_{n-1}(z)) & \cdots & -\frac{(q^{p^h}-1)}{q-1} \mathbf{F}_q(b_1(z)) \end{pmatrix}.$$

Notons que $\mathbf{ev} \left(\frac{q^{p^h}-1}{q-1} \right) = p^h$. Posons, pour chaque $i \in \{1, \dots, n\}$, $b_i(z) = \sum_{j \geq 0} b_{j,i} z^j$.

Alors on a $\mathbf{F}_q^h(\sum_{j \geq 0} b_{j,i} z^j) = \sum_{j \geq 0} \mathbf{F}_q^h(b_{j,i}) z^{jp^h}$. Donc, d'après le point 5 de la proposition 4.2.12, $\mathbf{ev}(\mathbf{F}_q^h(\sum_{j \geq 0} b_{j,i} z^j)) = \mathbf{ev}(\sum_{j \geq 0} b_{j,i} z^{jp^h})$. Par conséquent,

$$\mathbf{ev} \left(\frac{B_q^{\mathbf{F}_q^h} - I_n}{q-1} \right) = p^h \mathbf{ev} \left(\frac{B_q - I_n}{q-1} \right) (z^{p^h}) = p^h B(z^{p^h}) = p^h B^{\mathbf{F}_q^h},$$

où $\mathbf{F} : \mathbb{Z}_p[[z]] \rightarrow \mathbb{Z}_p[[z]]$ est l'automorphisme de Frobenius de $\mathbb{Z}_p[[z]]$. Donc, en appliquant \mathbf{ev} à l'égalité (4.16), on obtient que

$$\delta(\mathbf{ev}(G_q)) = \mathbf{Bev}(G_q) - \mathbf{ev}(G_q)p^h B^{\mathbf{F}^h}. \quad (4.17)$$

Puisque $G_q \in \mathrm{GL}_n(\mathbb{E}_{\mathbb{Z},q,p})$, alors $\mathbf{ev}(G_q) \in \mathrm{GL}_n(\mathbb{E}_p)$. Il suit donc de l'égalité (4.17) que l'opérateur différentiel $\mathbf{ev}(L_{\delta_q})$ est muni d'une structure de Frobenius forte de période h . \square

Voici notre deuxième résultat qui répond à la question 5.

Théorème 4.3.2. *Soient $L_q \in E_{\mathbb{Z},q,p}[\sigma_q]$ d'ordre n et $f(q, z) \in \mathbb{Z}_{q,p}[[z]]$ solution de L_q . Supposons que L_q possède une structure de Frobenius forte de période h . Il existe donc $d_0(q, z), \dots, d_{n^2}(q, z) \in \vartheta_{\mathrm{Frac}(\mathbb{Z}_{q,p})}[[z]]$ et une constante $c \in \mathbb{Z}_{q,p}$ non nulle telles que le polynôme $d_0(q, z)Y_0 + d_1(q, z)Y_1 + \dots + d_{n^2}(q, z)Y_{n^2} \pmod{[p]_q \vartheta_{\mathrm{Frac}(\mathbb{Z}_{q,p})}}$ est non nul, $cd_0(z), \dots, cd_{n^2}(z) \in E_{\mathbb{Z},q,p}$ et*

$$\sum_{i=0}^{n^2} d_i(q, z) \mathbf{F}_q^{ih}(f(q, z)) \equiv 0 \pmod{[p]_q \vartheta_{\mathrm{Frac}(\mathbb{Z}_{q,p})}[[z]]}. \quad (4.18)$$

La démonstration de ce théorème repose sur plusieurs propositions que nous énonçons et démontrons dans la partie suivante.

4.3.1 Propositions auxiliaires

Étant donné $L_q \in E_{\mathbb{Z},q,p}[\sigma_q]$, soient A_q la matrice compagnon de L_q et $N(A_q)$ l'ensemble des solutions de $\sigma_q X = A_q X$ dans $\mathbb{Z}_{q,p}[[z]]^n$. Cet ensemble est un $\mathbb{Z}_{q,p}$ -module pour l'opération $c \cdot (f_1, \dots, f_n)^t = (cf_1, \dots, cf_n)^t$. Soit $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ donné par $\mathbf{F}_q(\sum_{i \geq 0} a_i z^i) = \sum_{i \geq 0} \mathbf{F}_q(a_i) z^{ip}$. Dans la proposition suivante, nous allons décrire l'action de Frobenius sur l'ensemble $N(A_q)$.

Proposition 4.3.3. *Soient $L_q \in E_{\mathbb{Z},q,p}[\sigma_q]$ un opérateur aux q -différences d'ordre n et A_q la matrice compagnon de L_q . Si L_q possède une structure de Frobenius forte de période h avec H_q une matrice de passage de Frobenius de L_q , alors l'application $\psi : N(A_q) \rightarrow N(A_q)$ donnée par*

$$\psi((f_1, \dots, f_n)^t) = H_q(\mathbf{F}_q^h(f_1), \dots, \mathbf{F}_q^h(f_n))^t$$

est une application semi linéaire par rapport à l'automorphisme \mathbf{F}_q^h de $\mathbb{Z}_{q,p}$.

Démonstration. Comme L_q possède une structure de Frobenius forte et $H_q \in \mathrm{GL}_n(\mathbb{E}_{\mathbb{Z},q,p})$ est une matrice de passage de Frobenius de L_q , alors on a

$$\sigma_q(H_q) A_q^{\mathbf{F}_q^h} = A_q H_q. \quad (4.19)$$

Nous posons $\psi : N(A_q) \rightarrow N(A_q)$ définie par $\psi((f_1, \dots, f_n)^t) = H_q((\mathbf{F}_q^h(f_1), \dots, \mathbf{F}_q^h(f_n))^t)$. Montrons d'abord que ψ est bien définie. C'est-à-dire montrons que si $(f_1, \dots, f_n)^t \in N(A_q)$ alors $H_q(\mathbf{F}_q^h(f_1), \dots, \mathbf{F}_q^h(f_n))^t \in N(A_q)$. En effet, comme $(f_1, \dots, f_n)^t$ est solution de $\sigma_q y = A_q y$ alors

$$\begin{pmatrix} \sigma_q f_1 \\ \sigma_q f_2 \\ \vdots \\ \sigma_q f_n \end{pmatrix} = A_q \begin{pmatrix} f_1 \\ f_2 \\ \vdots \\ f_n \end{pmatrix}. \quad (4.20)$$

Remarquons que la restriction de $\mathbf{F}_q : \mathbb{Z}_{q,p}[[z]] \rightarrow \mathbb{Z}_{q,p}[[z]]$ à $E_{\mathbb{Z},q,p}$ donne l'automorphisme de Frobenius de $E_{\mathbb{Z},q,p}$ considéré dans le point 3 de la proposition 4.2.12. Alors, en appliquant \mathbf{F}_q^h à l'égalité (4.20) on a que,

$$\begin{pmatrix} \mathbf{F}_q^h(\sigma_q f_1) \\ \vdots \\ \mathbf{F}_q^h(\sigma_q f_n) \end{pmatrix} = A_q^{\mathbf{F}_q^h} \begin{pmatrix} \mathbf{F}_q^h(f_1) \\ \vdots \\ \mathbf{F}_q^h(f_n) \end{pmatrix}. \quad (4.21)$$

Écrivons $f_j = \sum_{i \geq 0} a_{i,j} z^i$, donc $\mathbf{F}_q^h(f_j) = \sum_{i \geq 0} \mathbf{F}_q^h(a_{i,j}) z^{ip^h}$ et ainsi, on a

$$\begin{aligned} \mathbf{F}_q^h(\sigma_q f_j) &= \mathbf{F}_q^h \left(\sum_{i \geq 0} a_{i,j} q^i z^i \right) = \sum_{i \geq 0} \mathbf{F}_q^h(a_{i,j}) \mathbf{F}_q^h(q^i) z^{ip^h} \\ &= \sum_{i \geq 0} \mathbf{F}_q^h(a_{i,j}) q^{ip^h} z^{ip^h} \\ &= \sigma_q(\mathbf{F}_q^h(f_j)). \end{aligned}$$

Donc, d'après l'égalité (4.21) on obtient que

$$\begin{pmatrix} \sigma_q(\mathbf{F}_q^h(f_1)) \\ \vdots \\ \sigma_q(\mathbf{F}_q^h(f_n)) \end{pmatrix} = A_q^{\mathbf{F}_q^h} \begin{pmatrix} \mathbf{F}_q^h(f_1) \\ \vdots \\ \mathbf{F}_q^h(f_n) \end{pmatrix}.$$

Ainsi, $(\mathbf{F}_q^h(f_1), \dots, \mathbf{F}_q^h(f_n))^t$ est une solution du système $\sigma_q X = A_q^{\mathbf{F}_q^h} X$. Donc, à la suite de (4.19) on a que

$$H_q \begin{pmatrix} \mathbf{F}_q^h(f_1) \\ \vdots \\ \mathbf{F}_q^h(f_n) \end{pmatrix}$$

est solution du système $\sigma_q X = A_q X$. Comme $H_q \in \mathrm{GL}_n(E_{\mathbb{Z},q,p})$ et, d'après le point 1 de la proposition 4.2.12, on a $E_{\mathbb{Z},q,p} \subset \mathbb{Z}_{q,p}[[z]]$, alors cette solution appartient à $N(A_q)$. Par conséquent, ψ est bien définie. Notons que pour tout $c \in \mathbb{Z}_{q,p}$ et tout $(f_1, \dots, f_n)^t \in N(A_q)$, $\psi(c \cdot (f_1, \dots, f_n)^t) = \mathbf{F}_q^h(c) \cdot \psi((f_1, \dots, f_n)^t)$. \square

Étant donné $L_q \in \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]][\sigma_q]$ soit $\mathrm{Ker}(L_q, \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]])$ l'ensemble de solutions de L_q dans $\mathrm{Frac}(\mathbb{Z}_{q,p})[[z]]$.

Proposition 4.3.4. *Soient $L_q \in \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]][\sigma_q]$ un opérateur aux q -différences d'ordre n . L'ensemble $\mathrm{Ker}(L_q, \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]])$ est un $\mathrm{Frac}(\mathbb{Z}_{q,p})$ -espace vectoriel de dimension inférieure ou égale à n .*

Cette proposition est un cas particulier du lemme 1.2.1 de [36] mais on en donne néanmoins une preuve ici par soucis de complétude.

Démonstration. Soit $C = \{f \in \mathrm{Frac}(\mathbb{Z}_{q,p})((z)) : \sigma_q(f) = f\}$. Autrement dit, C est le sous-anneau de $\mathrm{Frac}(\mathbb{Z}_{q,p})((z))$ qui contient les éléments invariants sous l'action de σ_q . On constate facilement que $C = \mathrm{Frac}(\mathbb{Z}_{q,p})$. Ainsi, $\mathrm{Ker}(L_q, \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]])$ est un C -espace vectoriel car $\mathrm{Ker}(L_q, \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]])$ est un $\mathrm{Frac}(\mathbb{Z}_{q,p})$ -espace vectoriel sous l'action $c \cdot (\sum_{i \geq 0} a_i z^i) = \sum_{i \geq 0} ca_i z^i$. Montrons que la dimension de $\mathrm{Ker}(L_q, \mathrm{Frac}(\mathbb{Z}_{q,p})[[z]])$

comme C -espace vectoriel est inférieure ou égale à n . Soient f_1, \dots, f_{n+1} éléments de $\text{Ker}(L_q, \text{Frac}(\mathbb{Z}_{q,p})[[z]])$ et

$$L_q = \sigma_q^n + a_1(z)\sigma_q^{n-1} + \dots + a_{n-1}(z)\sigma_q + a_n(z) \in \text{Frac}(\mathbb{Z}_{q,p})[[z]][\sigma_q].$$

Alors, pour tout $i \in \{1, \dots, n+1\}$, on a

$$\sigma_q^n(f_i) + a_1(z)(\sigma_q^{n-1}f_i) + \dots + a_{n-1}(z)(\sigma_q f_i) + a_n(z)f_i = 0.$$

D'où les vecteurs

$$y_1 = \begin{pmatrix} f_1 \\ \sigma_q f_1 \\ \vdots \\ \sigma_q^n f_1 \end{pmatrix}, y_2 = \begin{pmatrix} f_2 \\ \sigma_q f_2 \\ \vdots \\ \sigma_q^n f_2 \end{pmatrix}, \dots, y_{n+1} = \begin{pmatrix} f_{n+1} \\ \sigma_q f_{n+1} \\ \vdots \\ \sigma_q^n f_{n+1} \end{pmatrix}$$

sont linéairement dépendants sur $\text{Frac}(\mathbb{Z}_{q,p})((z))$ car $\text{Frac}(\mathbb{Z}_{q,p})[[z]] \subset \text{Frac}(\mathbb{Z}_{q,p})((z))$. Par conséquent, si r est le rang de la matrice dont les colonnes sont les vecteurs y_1, \dots, y_{n+1} alors $r \leq n$. Ainsi, il existe $v_1, \dots, v_r \in \{y_1, \dots, y_{n+1}\}$ linéairement indépendants sur $\text{Frac}(\mathbb{Z}_{q,p})((z))$ tels que y_1, \dots, y_{n+1} appartiennent au $\text{Frac}(\mathbb{Z}_{q,p})((z))$ -espace vectoriel engendré par v_1, \dots, v_r . Sans perdre en généralité nous supposons que $v_1 = y_1, \dots, v_r = y_r$. Donc, pour chaque $j \in \{r+1, \dots, n+1\}$, il existe $c_{1,j}, \dots, c_{r,j} \in \text{Frac}(\mathbb{Z}_{q,p})((z))$ tels que $y_j = c_{1,j}y_1 + \dots + c_{r,j}y_r$. C'est pourquoi, pour tout $j \in \{r+1, \dots, n+1\}$, on a

$$\begin{pmatrix} f_1 & \dots & f_r \\ \sigma_q f_1 & \dots & \sigma_q f_r \\ \vdots & \dots & \vdots \\ \sigma_q^n f_1 & \dots & \sigma_q^n f_r \end{pmatrix} \begin{pmatrix} c_{1,j} \\ c_{2,j} \\ \vdots \\ c_{r,j} \end{pmatrix} = \begin{pmatrix} f_j \\ \sigma_q f_j \\ \vdots \\ \sigma_q^n f_j \end{pmatrix}. \quad (4.22)$$

Nous allons montrer que, pour tout $j \in \{r+1, \dots, n+1\}$, $c_{1,j}, \dots, c_{r,j} \in C$. En effet, en appliquant σ_q à (4.22) nous obtenons que

$$\begin{pmatrix} \sigma_q f_1 & \dots & \sigma_q f_r \\ \sigma_q^2 f_1 & \dots & \sigma_q^2 f_r \\ \vdots & \dots & \vdots \\ \sigma_q^{n+1} f_1 & \dots & \sigma_q^{n+1} f_r \end{pmatrix} \begin{pmatrix} \sigma_q c_{1,j} \\ \sigma_q c_{2,j} \\ \vdots \\ \sigma_q c_{r,j} \end{pmatrix} = \begin{pmatrix} \sigma_q f_j \\ \sigma_q^2 f_j \\ \vdots \\ \sigma_q^{n+1} f_j \end{pmatrix}. \quad (4.23)$$

Il suit de (4.22) et (4.23) que

$$\begin{pmatrix} \sigma_q f_1 & \dots & \sigma_q f_r \\ \sigma_q^2 f_1 & \dots & \sigma_q^2 f_r \\ \vdots & \dots & \vdots \\ \sigma_q^n f_1 & \dots & \sigma_q^n f_r \end{pmatrix} \begin{pmatrix} \sigma_q c_{1,j} - c_{1,j} \\ \sigma_q c_{2,j} - c_{2,j} \\ \vdots \\ \sigma_q c_{r,j} - c_{r,j} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Le rang de cette dernière matrice est égal à r car les vecteurs v_1, \dots, v_r sont linéairement indépendants. Ainsi, pour tout $j \in \{r+1, \dots, n+1\}$ et tout $i \in \{1, \dots, r\}$, $\sigma_q c_{i,j} = c_{i,j}$. D'où $c_{i,j} \in C$ pour $j \in \{r+1, \dots, n+1\}$ et $i \in \{1, \dots, r\}$. Par conséquent, les vecteurs y_1, \dots, y_{n+1} sont linéairement dépendants sur C et ainsi, f_1, \dots, f_{n+1} sont linéairement dépendants sur C . Il découle donc que la dimension de $\text{Ker}(L_q, \text{Frac}(\mathbb{Z}_{q,p})[[z]])$ comme C -espace vectoriel est inférieure ou égale à n . \square

4.3.2 Démonstration du théorème 4.3.2

Maintenant nous démontrons le théorème 4.3.2.

Démonstration. D'après la proposition 4.3.4, l'ensemble $\text{Ker}(L_q, \text{Frac}(\mathbb{Z}_{q,p})[[z]])$ est un $\text{Frac}(\mathbb{Z}_{q,p})$ -espace vectoriel de dimension inférieure ou égale à n . Soient A_q la matrice compagnon de L_q et $\widehat{N}(A_q)$ l'ensemble des solutions de $\sigma_q X = A_q X$ dans $\text{Frac}(\mathbb{Z}_{q,p})[[z]]^n$. Cet ensemble est un $\text{Frac}(\mathbb{Z}_{q,p})$ -espace vectoriel pour l'action $c \cdot (f_1, \dots, f_n)^t = (cf_1, \dots, cf_n)^t$. Les ensembles $\text{Ker}(L_q, \text{Frac}(\mathbb{Z}_{q,p})[[z]])$ et $\widehat{N}(A_q)$ sont isomorphes en tant que $\text{Frac}(\mathbb{Z}_{q,p})$ -espaces vectoriels sous l'homomorphisme $\widehat{N}(A_q) \rightarrow \text{Ker}(L_q, \text{Frac}(\mathbb{Z}_{q,p})[[z]])$ donné par $(f_1, \dots, f_n)^t \mapsto f_1$. Ainsi, $\dim_{\text{Frac}(\mathbb{Z}_{q,p})} \widehat{N}(A_q) \leq n$. Soit $N(A_q)$ l'ensemble des solutions de $\sigma_q X = A_q X$ dans $\mathbb{Z}_{q,p}[[z]]^n$. Il est clair que $N(A_q) \subset \widehat{N}(A_q)$. Soit H_q une matrice de passage de Frobenius de L_q . D'après la proposition 4.3.3, on a l'application semi-linéaire $\psi : N(A_q) \rightarrow N(A_q)$ donné par $\psi((f_1, \dots, f_n)^t) = H_q((\mathbf{F}_q^h(f_1)), \dots, \mathbf{F}_q^h(f_n))^t$. Soit $\mathbf{f} = (f, \sigma_q(f), \dots, \sigma_q^{n-1}(f))^t$. Comme par hypothèse f est solution de L_q et $f \in \mathbb{Z}_{q,p}[[z]]$, alors $\mathbf{f} \in N(A_q)$ et par conséquent, pour tout entier $i > 0$, $\psi^i(\mathbf{f}) \in N(A_q)$. Puisque $N(A_q) \subset \widehat{N}(A_q)$ et $\dim_{\text{Frac}(\mathbb{Z}_{q,p})} \widehat{N}(A_q) \leq n$ alors, il existe $r_1, \dots, r_n \in \text{Frac}(\mathbb{Z}_{q,p})$ non tous nuls tels que $\psi^n(\mathbf{f}) + r_1 \psi^{n-1}(\mathbf{f}) + \dots + r_{n-1} \psi(\mathbf{f}) + r_n \mathbf{f} = 0$. Alors, il existe $s_0 \in \mathbb{Z}_{q,p}$ non nul et $s_1, \dots, s_n \in \mathbb{Z}_{q,p}$ non tous nuls tels que

$$s_0 \psi^n(\mathbf{f}) + s_1 \psi^{n-1}(\mathbf{f}) + \dots + s_{n-1} \psi(\mathbf{f}) + s_n \mathbf{f} = 0. \quad (4.24)$$

Posons Z comme le $\text{Frac}(E_{\mathbb{Z},q,p})$ -espace vectoriel engendré par $\{\mathbf{F}_q^{jh}(\sigma_q^i(f)) : j \in \mathbb{Z}_{\geq 0}, i \in \{0, 1, \dots, n-1\}\}$. Il suit de (4.24) que Z , en tant que $\text{Frac}(E_{\mathbb{Z},q,p})$ -espace vectoriel, est engendré par $\{\mathbf{F}_q^{rh}(\sigma_q^i(f)) : r, i \in \{0, 1, \dots, n-1\}\}$ et par conséquent, $\dim_{\text{Frac}(E_{\mathbb{Z},q,p})} Z \leq n^2$. Maintenant notons que $f, \mathbf{F}_q^h(f), \dots, \mathbf{F}_q^{n^2 h}(f) \in Z$. Donc, il existe $b_0(q, z), b_1(q, z), \dots, b_{n^2}(q, z) \in E_{\mathbb{Z},q,p}$, non tous nuls, tels que

$$b_0(q, z)f + b_1(q, z)\mathbf{F}_q^h(f) + \dots + b_{n^2}(q, z)\mathbf{F}_q^{n^2 h}(f) = 0.$$

Soit $i_0 \in \{0, \dots, n^2\}$ tel que $|b_{i_0}(q, z)|_{\mathcal{G}} = \max\{|b_0(q, z)|_{\mathcal{G}}, \dots, |b_{n^2}(q, z)|_{\mathcal{G}}\}$. Comme $b_{i_0}(q, z)$ appartient à $E_{\mathbb{Z},q,p}$ est non nul et la norme est ultramétrique alors il existe $P(z)/Q(z)$ dans $\mathbb{Z}_{q,p}[z]_{\mathcal{S}}$ telle que $|b_{i_0}(q, z)|_{\mathcal{G}} = |P(z)/Q(z)|_{\mathcal{G}}$. Mais $|P(z)/Q(z)|_{\mathcal{G}} = |P(z)|_{\mathcal{G}}$ car $Q(z) \in \mathcal{S}$.

Soit $c \in \mathbb{Z}_{q,p}$ le coefficient de $P(z)$ tel que $|P(z)|_{\mathcal{G}} = |c|_{\mathfrak{m}}$. Par conséquent, on a $|c|_{\mathfrak{m}} = \max\{|b_0(q, z)|_{\mathcal{G}}, \dots, |b_{n^2}(q, z)|_{\mathcal{G}}\}$. c est non nul car les $b_i(q, z)$ ne sont pas tous nuls. Posons pour chaque $i \in \{0, 1, \dots, n^2\}$, $d_i(q, z) = \frac{b_i(q, z)}{c}$.

Ainsi, $1 = \max\{|d_0(q, z)|_{\mathcal{G}}, \dots, |d_{n^2}(q, z)|_{\mathcal{G}}\}$ et

$$d_0(q, z)f + d_1(q, z)\mathbf{F}_q^h(f) + \dots + d_{n^2}(q, z)\mathbf{F}_q^{n^2 h}(f) = 0. \quad (4.25)$$

D'après le point 1 de la proposition 4.2.12, $E_{\mathbb{Z},q,p} \subset \mathbb{Z}_{q,p}[[z]]$. Ainsi, $b_0(q, z), b_1(q, z), \dots, b_{n^2}(q, z) \in \mathbb{Z}_{q,p}[[z]]$ et $d_0(q, z), d_1(q, z), \dots, d_{n^2}(q, z) \in \text{Frac}(\mathbb{Z}_{q,p})[[z]]$. Puisque, pour tout $i \in \{0, 1, \dots, n^2\}$, $|d_i(q, z)|_{\mathcal{G}} \leq 1$ alors $d_0(q, z), d_1(q, z), \dots, d_{n^2}(q, z) \in \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]$. Donc, il suit de (4.25) que

$$d_0(q, z)f + d_1(q, z)\mathbf{F}_q^h(f) + \dots + d_{n^2}(q, z)\mathbf{F}_q^{n^2 h}(f) \equiv 0 \pmod{[p]_q \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]}$$

et le polynôme $d_0(q, z)Y_0 + \dots + d_{n^2}(q, z)Y_{n^2} \pmod{[p]_q \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}}$ est non nul car $1 = \max\{|d_i(q, z)|_{\mathcal{G}}, \dots, |d_{n^2}(q, z)|_{\mathcal{G}}\}$. \square

Remarque 4.3.5. Soit k l'anneau résiduel de $\vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}$. Notons que k est un corps car $\text{Frac}(\mathbb{Z}_{q,p})$ est un corps. Soit \mathfrak{n} l'idéal maximal de $\vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}$. Nous venons de montrer que, sous les hypothèses du théorème 4.3.2, il existe $d_0(z), \dots, d_{n^2}(z) \in \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]$ et une constante $c \in \mathbb{Z}_{q,p}$ non nulle telles que le polynôme $d_0(q, z)Y_0 + d_1(z)Y_1 + \dots + d_{n^2}(q, z)Y_{n^2} \pmod{[p]_q \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}}$ est non nul, $cd_0(q, z), \dots, cd_{n^2}(q, z) \in E_{\mathbb{Z}, q, p}$ et

$$d_0(q, z)f(z) + d_1(q, z)\mathbf{F}_q^h(f) + \dots + d_{n^2}(q, z)\mathbf{F}_q^{n^2 h}(f) \equiv 0 \pmod{[p]_q \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]}.$$

Pour chaque $i \in \{0, 1, \dots, n^2\}$, soit $d_i|_{\mathfrak{n}}(q, z)$ la série à coefficients dans k obtenue après avoir réduit chaque coefficient de $d_i(q, z)$ modulo l'idéal \mathfrak{n} . Dans cette remarque nous allons montrer que, pour tout $i \in \{0, 1, \dots, n^2\}$, $d_i|_{\mathfrak{n}}(q, z) \in k(z)$.

En effet, comme $b_i(q, z) \in E_{\mathbb{Z}, q, p}$, alors $b_i(q, z) = \lim_{n \rightarrow \infty} x_n(z)$, où $x_n(z) \in \mathbb{Z}_{q,p}[z]_S$ pour tout $n \geq 0$. Ainsi, $d_i(q, z) = \lim_{n \rightarrow \infty} \frac{x_n(z)}{c}$ et par conséquent, il existe N tel que $|d_i(q, z) - \frac{x_N(z)}{c}|_{\mathcal{G}} < 1$. Comme la norme est ultramétrique alors $\left| \frac{x_N(z)}{c} \right|_{\mathcal{G}} \leq 1$. Écrivons

$$x_N(z) = \frac{\sum_{i=0}^l a_{N,i} z^i}{\sum_{j=0}^t b_{N,j} z^j},$$

où $\sum_{i=0}^l a_{N,i} z^i \in \mathbb{Z}_{q,p}[z]$ et $\sum_{j=0}^t b_{N,j} z^j \in S$.

Soit i_0 tel que $|a_{N,i_0}|_{\mathfrak{m}} = \max\{|a_{N,0}|_{\mathfrak{m}}, \dots, |a_{N,l}|_{\mathfrak{m}}\}$. Puisque $\sum_{j=0}^t b_{N,j} z^j \in S$, alors $1 = |b_{N,0}|_{\mathfrak{m}} = \max\{|b_{N,0}|_{\mathfrak{m}}, \dots, |b_{N,t}|_{\mathfrak{m}}\}$ et

$$x_N(z) = \frac{a_{N,i_0} P(z)}{b_{N,0} Q(z)}, \quad \text{où } P(z) = \sum_{i=0}^l \frac{a_{N,i}}{a_{N,i_0}} z^i, \quad Q(z) = \sum_{j=0}^t \frac{b_{N,j}}{b_{N,0}} z^j,$$

$|P(z)|_{\mathcal{G}} = 1$ et $|Q(z)|_{\mathcal{G}} = 1$. Ainsi, $P(z), Q(z) \in \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[z]$. Comme $|b_{N,0}|_{\mathfrak{m}} = 1$ alors $\frac{1}{b_{N,0}} \in \mathbb{Z}_{q,p}$ car $\mathbb{Z}_{q,p}$ est un anneau local complet et ainsi $\frac{a_{N,i_0}}{b_{N,0}} \in \mathbb{Z}_{q,p}$. Puisque $\frac{X_N(z)}{c} = \frac{a_{N,i_0} P(z)}{cb_{N,0} Q(z)}$, $|P(z)/Q(z)|_{\mathcal{G}} = 1$ et $|x_N(z)/c|_{\mathcal{G}} \leq 1$ alors $|a_{N,i_0}/cb_{N,0}|_{\mathfrak{m}} \leq 1$, d'où $a_{N,i_0}/cb_{N,0} \in \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}$. Donc, si $\frac{X_N(z)}{c}|_{\mathfrak{n}}$ désigne la série obtenue après avoir réduit les coefficients de $\frac{X_N(z)}{c}$ modulo l'idéal maximal \mathfrak{n} alors,

$$\frac{X_N(z)}{c} \Big|_{\mathfrak{n}} = \left(\frac{a_{N,i_0}}{cb_{N,0}} \pmod{\mathfrak{n}} \right) \frac{\sum_{i=0}^l \left(\frac{a_{N,i}}{a_{N,i_0}} \pmod{\mathfrak{n}} \right) z^i}{\sum_{j=0}^t \left(\frac{b_{N,j}}{b_{N,0}} \pmod{\mathfrak{n}} \right) z^j} \in k(z).$$

Puisque $|d_i(q, z) - \frac{x_N(z)}{c}|_{\mathcal{G}} < 1$ alors, $d_i|_{\mathfrak{n}}(q, z) = \frac{X_N(z)}{c} \Big|_{\mathfrak{n}}$ et ainsi, $d_i|_{\mathfrak{n}}(q, z) \in k(z)$. Finalement, puisque $1 = \max\{|d_0(q, z)|_{\mathcal{G}}, \dots, |d_{n^2}(q, z)|_{\mathcal{G}}\}$, alors $d_0|_{\mathfrak{n}}(q, z), \dots, d_{n^2}|_{\mathfrak{n}}(q, z)$ ne sont pas toutes nulles.

4.3.3 Réponse à la question 5

Soit $f(q, z) \in \mathbb{Z}[q][[z]]$, alors $\mathbf{F}_q(f(q, z)) = f(q^p, z^p)$ et $\mathbf{ev}(f(q, z)) = f(1, z)$. Supposons que $f(q, z) \in \mathbb{Z}[q][[z]]$ annule un opérateur aux q -différences L_q d'ordre n muni d'une structure de Frobenius forte de période h . Par conséquent, d'après le théorème 4.3.2, il existe $d_0(z), \dots, d_{n^2}(z) \in \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]$ et une constante $c \in \mathbb{Z}_{q,p}$ non nulle telles que le polynôme $d_0(q, z)Y_0 + d_1(z)Y_1 + \dots + d_{n^2}(q, z)Y_{n^2} \pmod{[p]_q \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}}$ est non nul, $cd_0(q, z), \dots, cd_{n^2}(q, z) \in E_{\mathbb{Z}, q, p}$ et

$$\sum_{i=0}^{n^2} d_i(q, z) f(q^{p^{ih}}, z^{p^{ih}}) \equiv 0 \pmod{[p]_q \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]}. \quad (4.26)$$

Soit \mathfrak{n} l'idéal maximal de $\vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}$. Remarquons que $\mathfrak{m} \subset \mathfrak{n}$ parce que $\mathfrak{m} \subset \mathbb{Z}[q] \subset \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}$ et tout élément de \mathfrak{m} a une norme inférieure à 1. Par conséquent, pour tout $i \geq 0$, $q^{p^{ih}} \equiv 1 \pmod{\mathfrak{n}}$ car $q^{p^{ih}} \equiv 1 \pmod{\mathfrak{m}}$ et $q \equiv 1 \pmod{\mathfrak{n}}$ car $q \equiv 1 \pmod{\mathfrak{m}}$. De plus, $[p]_q \in \mathfrak{n}$ puisque $[p]_q \in \mathfrak{m}$. Il suit donc de l'équation (4.26) que

$$\sum_{i=0}^{n^2} d_i(1, z) f(1, z^{p^{ih}}) = 0 \pmod{\mathfrak{n} \vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}[[z]]}. \quad (4.27)$$

Remarquons que $d_i(1, z) \equiv d(q, z) \pmod{\mathfrak{n}}$ car $q \equiv 1 \pmod{\mathfrak{n}}$ et d'après la remarque 4.3.5, la réduction des séries $d_0(q, z), \dots, d_{n^2}(q, z)$ modulo l'idéal maximal \mathfrak{n} sont des fractions rationnelles non toutes nulles à coefficients dans le corps $\vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}/\mathfrak{n}$. Remarquons que pour tout entier $i \geq 0$, $f(1, z^{p^{ih}}) \pmod{\mathfrak{n}} \in \mathbb{F}_p[[z]]$ car le corps résiduel de $\mathbb{Z}[q]$ est \mathbb{F}_p et $f(1, z^{p^{ih}}) \in \mathbb{Z}[q][[z]]$. Finalement, $\vartheta_{\text{Frac}(\mathbb{Z}_{q,p})}/\mathfrak{n}$ est une extension de \mathbb{F}_p , alors le lemme 2.1.2 et l'équation (4.27) entraînent qu'il existe des polynômes $a_0(z), \dots, a_{n^2}(z) \in \mathbb{Z}[z]$ tels que leurs réductions modulo p ne sont pas toutes nulles et

$$\sum_{i=0}^{n^2} a_i(z) f(1, z^{p^{ih}}) \equiv 0 \pmod{p\mathbb{Z}[[z]]}.$$

Par conséquent, nous obtenons ainsi une réponse à la question 5.

4.4 Question ouverte

Motivée par les résultats des théorèmes 4.3.1 et 4.3.2, une question naturelle est de savoir si, étant donné un nombre premier p , l'opérateur q -hypergéométrique $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$, où $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$, $\underline{\beta} = (\beta_1, \dots, \beta_n) \in (\mathbb{Q} \setminus \mathbb{Z}_{\leq 0})^n$, a une structure de Frobenius forte pour p .

Rappelons que d'après le théorème 1.4.11, si $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$ et si la norme p -adique de α_i et β_j est inférieure ou égale à 1 pour tout $i, j \in \{1, \dots, n\}$, alors l'opérateur différentiel hypergéométrique $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ a une structure de Frobenius forte pour p . Ainsi, on s'attend à ce que $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ soit muni d'une structure de Frobenius pour p lorsque $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$.

La démonstration du théorème 1.4.11 repose essentiellement sur la rigidité de l'opérateur $\mathcal{H}(\underline{\alpha}, \underline{\beta})$. Dans [60] Roques donne une définition de rigidité pour les opérateurs aux q -différences et il démontre que sous cette définition l'opérateur q -hypergéométrique $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ est rigide. Une piste éventuelle serait d'utiliser cette notion de rigidité pour démontrer que $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ est muni d'une structure de Frobenius pour presque tout nombre premier lorsque $\alpha_i - \beta_j \notin \mathbb{Z}$ pour tout $i, j \in \{1, \dots, n\}$.

4.5 Les travaux d'André et Di Vizio

Dans [11], André et Di Vizio ont donné une définition de structure de Frobenius forte pour les opérateurs aux q -différences lorsque q est un élément d'un corps ultramétrique vérifiant certaines conditions. Notre but ici est de voir que cette définition et les résultats de [11], bien que profonds, ne semblent pas adéquats pour répondre aux questions 5 et 6.

Soient K un corps de caractéristique zéro complet pour la norme ultramétrique $|\cdot|$ et k le corps résiduel de K de caractéristique $p > 0$. Étant donné $0 < \epsilon < 1$, soient I_ϵ

l'intervalle $(1 - \epsilon, 1)$ et

$$\mathcal{A}_K(I_\epsilon) = \left\{ \sum_{i \in \mathbb{Z}} a_i z^i : \text{tel que } a_i \in K, \lim_{i \rightarrow \pm\infty} |a_i| r^i = 0, \text{ pour tout } r \in I_\epsilon \right\}.$$

L'anneau de Robba est l'anneau $\mathcal{R}_K = \bigcup_{\epsilon > 0} \mathcal{A}_K(I_\epsilon)$. Soient $q \in K$ tel que q n'est pas une racine de l'unité, $|1 - q| < 1$ et τ un automorphisme de Frobenius de K tel que $\tau(q) = q$. Dans [11], André et Di Vizio ont défini une notion de structure de Frobenius forte pour les σ_q -modules à coefficients dans \mathcal{R}_K . Ils ont noté par $\sigma_q\text{-Mod}_{\mathcal{R}_K}^{(\phi)}$ la catégorie des σ_q -modules à coefficients dans \mathcal{R}_K qui sont munis d'une structure de Frobenius forte et par $d\text{-Mod}_{\mathcal{R}_K}^{(\phi)}$ la catégorie des modules différentiels à coefficients dans \mathcal{R}_K qui sont munis d'une structure de Frobenius forte. Ils ont montré un théorème de monodromie locale qui s'avère être le q -analogue de la conjecture de quasi-unipotence de Crew. Cela leur permet de montrer que lorsque k est algébriquement clos, il y a un foncteur $\text{Conf} : \sigma_q\text{-Mod}_{\mathcal{R}_K}^{(\phi)} \rightarrow d\text{-Mod}_{\mathcal{R}_K}^{(\phi)}$ qui est une équivalence.

Ensuite, Pulita [58] a montré que le foncteur Conf peut être étendu à la catégorie des modules *admissibles*, ce qui montre que la construction faite par André et Di Vizio ne dépend pas *a posteriori* de la structure de Frobenius forte. De plus, grâce à la construction faite par Pulita, nous obtenons que Conf envoie un opérateur aux q -différences à coefficients dans $\widetilde{\mathcal{R}_K}$ sur un opérateur différentiel à coefficients dans \mathcal{R}_K ayant les mêmes solutions dans $\widetilde{\mathcal{R}_K}[\text{Log}z]$, où $\widetilde{\mathcal{R}_K}$ est une extension de \mathcal{R}_K , c'est-à-dire que Conf préserve les solutions.

Le fait que ce foncteur préserve les solutions est un empêchement pour répondre à la question 6 parce que d'une part, cela implique que les structures de Frobenius fortes de M et $\text{Conf}(M)$ sont les mêmes, c'est-à-dire que les matrices de passage de M et $\text{Conf}(M)$ sont les mêmes et d'autre part, même si on ne sait pas si l'opérateur $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ possède une structure de Frobenius forte sous la définition proposée dans [11], on aura *a posteriori* que $\text{Conf}(\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})) \neq \mathcal{H}(\underline{\alpha}, \underline{\beta})$ parce que $\mathcal{H}_{\delta_q}(\underline{\alpha}, \underline{\beta})$ et $\mathcal{H}(\underline{\alpha}, \underline{\beta})$ n'ont pas les mêmes solutions. Par conséquent, en utilisant cette approche, nous ne pouvons pas répondre à la question 6.

Bibliographie

- [1] B. ADAMCZEWSKI, AND J. P. BELL, *Diagonalization and rationalization of algebraic Laurent series*, Ann. Sci. Éc. Norm. Supér **46** (2013), 963–1004.
- [2] B. ADAMCZEWSKI, J. P. BELL, E. DELAYGUE, *Algebraic independence of G -functions and congruences "à la lucas"*, preprint 2016, arXiv1603.04187, 50 pp.
- [3] B. ADAMCZEWSKI, J. BELL, E. DELAYGUE AND F. JOUHET, *Congruences modulo cyclotomic polynomials and algebraic independence for q -series* Sémin. Lothar. Combin **78B** (2017), 12 pp.
- [4] B. ADAMCZEWSKI ET E. DELAYGUE, communication personnelle 2019.
- [5] B. ADAMCZEWSKI, J. P. BELL, AND E. DELAYGUE, *Algebraic independence of G -functions and congruences "à la lucas"*, Ann. Sci. Éc. Norm. Supér **52** (2019), 515–559.
- [6] B. ADAMCZEWSKI, *Mahler's method*, Doc. Math Extra Volume Mahler Selecta (2019), 95–122.
- [7] B. ADAMCZEWSKI AND R. YASSAWI, *A note on Christol's theorem*, preprint 2019, arXiv :1906.08703, 14 pp.
- [8] J-P. ALLOUCHE, D.GOUYOU-BEAUCHAMPS, G. SKORDEV, *Transcendence of binomial and Lucas' formal power series*. J. Algebra **210** (1998), 577–592.
- [9] G. ALMKVIST, C. VAN ECKENVORT, D. VAN STRATEN, AND W. ZUDILIN. *Tables of Calbi-Yau equations*, preprint 2010, arXiv :0507430 130 pp.
- [10] Y. ANDRÉ, *G-functions and geometry*, Aspects of Mathematics **E13**, Friedr. Vieweg & Sohn, Braunschweig, 1989.
- [11] Y. ANDRÉ AND L. DI VIZIO, *q -difference equations and p -adic local monodromy*, Astérisque **296** (2004), 55–111.
- [12] R. APÉRY. *Irrationalité de $\xi(2)$ et $\xi(3)$* , Astérisque **61** (1979), 11–13.
- [13] M. F. ATIYAH AND I. G. MACDONALD, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, 1969.
- [14] F. BEUKERS, AND G. HECKMAN, *Monodromy for the hypergeometric fonction ${}_nF_{n-1}$* , Invent. Math **95** (1989), 325–354.
- [15] E. BOMBIERI, *On G -functions*, Recent progress in analytic number theory, Vol. 2 (Durham, 1979), pp. 1–67, Academic Press, London-New York, 1981.
- [16] A.BOSTAN AND E. SCHOST, *Fast algorithms for differential equations in positive characteristic*, ISSAC 2009 (Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation) pp. 47–54, ACM, New York, 2009.
- [17] A. BOSTAN, P. LAIREZ, B. SALVY, *Multiple binomial sums*, J. Symbolic Comput **80** (2017), 351–386.
- [18] M. BOUSQUET-MÉLOU, *Rational and algebraic series in combinatorial enumeration*, in International Congress of Mathematicians. Vol. III, Eur. Math. Soc., 2006, 789–826.

- [19] G. CHRISTOL, *Éléments analytiques uniformes et multiformes*, Séminaire Delange-Pisot-Poitou, Théorie des nombres **15** (1973-1974), Exp. No 6, 18 pp.
- [20] G. CHRISTOL, *Ensembles presque périodiques k -reconnaissables*, Theoret. Compt. Sci **9** (1979), 141-145.
- [21] G. CHRISTOL, *Décomposition des matrices en facteurs singuliers. Applications aux équations différentielles*, Study Group on Ultrametric Analysis **7-8** (1979-1981), Exp No 5, 17 pp.
- [22] G. CHRISTOL, *Systèmes différentiels linéaires p -adiques, structures de Frobenius faible*, Bull. Soc. Math. France **109** (1981), 83-122.
- [23] G. CHRISTOL, *Modules différentiels et équations différentielles p -adiques*, Queen's Papers in Pure and Applied Mathematics, **66**, Queen's University, Kingston, 1983.
- [24] G. CHRISTOL, *Un théorème de transfert pour les disques singuliers réguliers*, Astérisque **119-120** (1984), 151-168.
- [25] G. CHRISTOL, *Diagonales de fractions rationnelles et équations de Picard-Fuchs*, Study group on ultrametric analysis **12** (1984/85), Exp No 13, 12 pp.
- [26] G. CHRISTOL, *Fonctions et éléments algébriques*, Pacific J. of Math. **125** (1986), 1-37.
- [27] G. CHRISTOL, *Fonctions hypergéométriques bornées*, Study group on ultrametric analysis **14** (1986-1987), Exp No 8, 16 pp.
- [28] G. CHRISTOL, *Globally bounded solutions of differential equations*, in *Analytic number theory (Tokyo 1988)*, pp. 45-64, Lectures Notes in Math **1434**, Springer, Berlin, 1990.
- [29] D. CLARK, *A note on the p -adic convergence of solutions of linear differential equations*, P Proc. Amer. Math. Soc **17** (1966), 262-269.
- [30] T. CLUZEAU, *Algorithmique modulaire des équations différentielles linéaires*, thèse de doctorat, Université de Limoges, 2004.
- [31] A. COBHAM, *Uniform tag sequences*, Math. Systems Theory **6** (1972) 164-192.
- [32] R. CREW, *Rigidity and Frobenius Structure*, Doc. Math **22** (2017), 287-296.
- [33] P. DELIGNE, *Théorie de Hodge II*, Inst. Hautes Études Sci. Publ. Math **40** (1971) 5-57.
- [34] P. DELIGNE, *Intégration sur un cycle évanescant*, Invent. Math **76** (1983), 129-143.
- [35] J. DENEFF, AND L. LIPSHITZ, *Algebraic power series and diagonals*, J. Number Theory **26** (1987) 46-67.
- [36] L. DI VIZIO, *On the arithmetic theory of q -difference equations. The q -analogue of the Grothendieck-Katz's conjecture on p -curvatures*, Invent. Math **150** (2002), 517-578.
- [37] B.M. DWORK, *p -adic cycles*, Inst. Hautes Études Sci. Publ. Math **37** (1969), 27-115.
- [38] B.M DWORK, *On p -adic differential equations I. The Frobenius structure of differential equations*, Bull. Soc. Math. France **39-40** (1974), 27-37.
- [39] B.M. DWORK, *Arithmetic theory of differential equations*, Symposia Mathematica, Vol. XXIV (Rome, 1979), pp. 225-243, Academic Press, London-New York, 1981.
- [40] B.M DWORK, *On Apery's differential operator*, tudy group on ultrametric analysis, **7-8** (1979-1981), Exp No 25, 6 pp.
- [41] B.M. DWORK, *Lectures on p -adic differential equations*, Grundlehren der Math. Wissens-chaften **253**, Spring-Verlag, New York, 1982.

- [42] B. DWORK, G. GEROTTO, AND F. SULLIVAN, A introduction to G-functions, Annals of Mathematics Studies **133**, Princeton University Press, 1994.
- [43] S. EILENBERG, Automata, languages, and machines Vol. A, Pure and Applied Mathematics **58**, Academic Press, New York, 1974.
- [44] H. ESNAULT, AND M. GROECHENIG, *Rigid connections and F-isocrystals*, preprint 2020, arXiv :1707.00752, 44 pp.
- [45] N. J. FINE, *Binomial coefficients modulo a prime*, Amer. Math. Monthly **54** (1947), 589–592.
- [46] P. FLAJOLET, *Analytic models and ambiguity of context-free languages*, Theoret. Comput. Sci. **49** (1987), 283–309.
- [47] R. D. FRAY, *Congruence properties of ordinary and q-binomial coefficients*, Duke Math. J **34** (1967), 467–480.
- [48] H. FURSTENBERG, *Algebraic functions over finite fields*, J. Algebra **7** (1967) 271–277.
- [49] I. GESSEL, *Some congruences for Apéry numbers*, J. Number Theory **14** (1982), 362–368.
- [50] T. HONDA, *Algebraic differential equations*. Symposia Mathematica, Vol. XXIV (Rome, 1979), pp. 169-204, Academic Press, London-New York, 1981.
- [51] N. KATZ, *Algebraic solutions of differential equations (p-curvature and the Hodge filtration)*, Invent. Math **18** (1972), 1–118.
- [52] N. KATZ, *Rigid Local Systems*, Annals of Math. Studies **139**, Princeton Univ. Pres, 1996.
- [53] E. R. KOLCHIN, *Algebraic groups and algebraic dependence*, Amer. J. Math **90** (1968), 1151–1164.
- [54] K. KEDLAYA, *p-adic differential equations*, Cambridge studies in advanced mathematics **125**, Cambridge University Press, 2010.
- [55] E. LUCAS, *Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques suivant un module premier*, Bull. Soc. Math. France **6** (1878), 49–54.
- [56] A. MALIK AND A. STRAUB, *Divisibility properties of sporadic Apéry-like numbers*, Res. Number theory **2** (2016), 26 pp.
- [57] R. MESTROVIC, *Lucas theorem its generalizations, extensions and applications (1878–2014)*, preprint 2014, arXiv :1409.3820v1, 51 pp.
- [58] A. PULITA, *p-Adic Confluence of q-Difference Equations*, Compos. Math **144** (2008), 867–919.
- [59] T. RIVOAL, *Les E-fonctions et G-fonctions de Siegel*, prépublication (2019), 76 pp.
- [60] J. ROQUES, *Birkhoff matrices, residues and rigidity for q-difference equations.*, J. Reine Angew. Math **706** (2015), 215–244.
- [61] B. E. SAGAN, *Congruence properties of q-analogs*, Adv. Math **95** (1992), 127–143.
- [62] A. SALINIER, *Structure de Frobenius forte de l'équation différentielle hypergéométrique*, C. R. Acad. Sci. Paris **305** (1987), 393–396.
- [63] O. SALON, *Suites automatiques à multi-indices et algébricité*, C. R. Acad. Sci. Paris **305** (1987), 501–504.
- [64] O. SALON, *Suites automatiques à multi-indices*, Séminaire de Théorie des Nombre de Bordeaux, 1986/1987.

- [65] H. SHARIF AND C. F. WOODCOCK *On the transcendence of certain series*, J. Algebra **121** (1989), 364–369.
- [66] C. SIEGEL, *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen Akad. Berlin 1929.
- [67] M. F. SINGER, *Introduction to the Galois theory of linear differential equations*, London Math. Soc. Lecture Note Ser **357** (2009), 1–82.
- [68] R. P. STANLEY, *Differentiably finite power series*, European J. Combin **1** (1980), 175–188.
- [69] R. P. STANLEY, *Enumerative combinatorics Vol. 2*, Cambridge Studies in Advanced Mathematics **62**, Cambridge University Press, Cambridge, 1999.
- [70] V. STREHL, *Zum q-Analogon der Kongruenz von Lucas*, Séminaire Lotharingien de Combinatoire, 5-ième Session. Institut de Recherche Mathématique Avancée, 1982, pp. 102–104.
- [71] A. J. VAN DER POORTEN, *Power series representing algebraic functions*, Séminaire de Théorie des Nombres Paris, 1990–91, pp. 241–262, Progr. Math **108**, Birkhäuser Boston, Boston, 1993.
- [72] M. VAN DER PUT, AND M. F. SINGER *Galois theory of linear differential equations*, Grundlehren der Mathematischen Wissenschaften **328**, Springer-Verlag, Berlin, 2003.
- [73] D. VARGAS-MONTOYA, *Algébricité modulo p , séries hypergéométriques et structure de Frobenius forte*. à paraître au Bull. Soc. Math France (2021), 40 pp.

Algébricité modulo p et structure de Frobenius forte

Résumé : Cette thèse se situe à l'interface entre la théorie des nombres et la théorie des équations différentielles. Elle est consacrée à l'étude de l'algébricité modulo p des séries formelles à coefficients dans le corps des nombres rationnels \mathbb{Q} . Etant donné un nombre premier p , une série formelle $f(z) \in \mathbb{Q}[[z]]$ est algébrique modulo p si l'on peut réduire ses coefficients modulo p et si la série formelle obtenue est algébrique sur $\mathbb{F}_p(z)$, où \mathbb{F}_p désigne le corps à p éléments. L'outil principal utilisé dans cette thèse afin d'étudier cette problématique est la notion de structure de Frobenius forte associée à un opérateur différentiel à coefficients dans $\mathbb{Q}_p(z)$.

Dans un premier temps, nous montrons que si l'on peut réduire $f(z)$ modulo p et si $f(z)$ est solution d'un opérateur différentiel $L \in \mathbb{Q}(z)[d/dz]$ d'ordre n qui, vu dans $\mathbb{Q}_p(z)[d/dz]$, est muni d'une structure de Frobenius forte de période h , alors f est algébrique modulo p et le degré de sa réduction est majoré par p^{n^2h} . Nous démontrons ensuite que si L est un opérateur fuchsien dont les exposants sont rationnels et dont le groupe de monodromie est rigide, alors L possède, pour presque tout nombre premier p , une structure de Frobenius forte de période h , où h est majorée explicitement et indépendamment de p . Nous appliquons ces deux résultats pour résoudre une conjecture d'Adamczewski et Delaygue dans le cas des séries hypergéométriques généralisées.

La deuxième partie de la thèse est consacrée à certaines applications combinatoires et arithmétiques de l'algébricité modulo p . Etant donné un ensemble infini de nombres premiers \mathcal{S} , nous considérons des séries formelles $f(z)$ pouvant être réduite modulo p et annulant un opérateur différentiel L muni d'une structure de Frobenius forte, pour tout $p \in \mathcal{S}$. Nous montrons que si une telle série annule également un opérateur différentiel MUM en zéro, alors pour presque tout $p \in \mathcal{S}$, la réduction de f modulo p annule un polynôme de la forme $X - A_p(z)X^{p^l}$, où $A_p(z) \in \mathbb{F}_p(z)$. D'après des travaux récents d'Adamczewski, Bell et Delaygue, les coefficients de telles séries satisfont à des congruences dites « à la Lucas » qui peuvent être utilisées pour démontrer l'indépendance algébrique de G -fonctions au sens de Siegel. Nous donnons quelques applications de nos résultats dans cette direction.

Dans la dernière partie de la thèse, nous proposons une nouvelle définition de la notion de structure de Frobenius forte pour les opérateurs aux q -différences. Nous montrons que l'existence de telles structures impliquent certains résultats de confluence et d'algébricité modulo les p -ièmes polynômes cyclotomiques.

Mots clés : Algébricité modulo p , structure de Frobenius forte, congruences « à la Lucas » et indépendance algébrique.

Image en couverture : Photo du parc de la Feyssine prise par l'auteur de la thèse.