

Galois groups of reductions modulo p of D -finite series

Xavier Caruso, Florian Fürnsinn and Daniel Vargas-Montoya

April 13, 2025

Abstract

The aim of this paper is to investigate the algebraicity behavior of reductions of D -finite power series modulo prime numbers. For many classes of D -finite functions, such as diagonals of multivariate algebraic series or hypergeometric functions, it is known that their reductions modulo prime numbers, when defined, are algebraic. We formulate a conjecture that uniformizes the Galois groups of these reductions across different prime numbers.

We then focus on hypergeometric functions, which serves as a test case for our conjecture. Refining the construction of an annihilating polynomial for the reduction of a hypergeometric function modulo a prime number p , we extract information on the respective Galois groups and show that they behave nicely as p varies.

Contents

1	Introduction	1
2	A general picture of what we expect	5
2.1	Getting intuition by examples	5
2.2	The conjectures: weak and strong forms	13
2.3	The language of differential modules and Frobenius modules	19
3	Hypergeometric series and their reductions modulo p	27
3.1	Reductions of hypergeometric series modulo p	28
3.2	Algebraicity modulo p and Galois groups	36
3.3	The case of Gaussian hypergeometric functions	46

1 Introduction

The starting point of this paper is the observation that there exist many interesting series in $\mathbb{Q}[[x]]$ which are transcendental over $\mathbb{Q}(x)$ but whose reductions modulo p (when they exist) are algebraic over $\mathbb{F}_p(x)$ for a large set of primes p . A typical example is provided by “diagonals”. By definition, the *diagonal* of a multivariate series

$$f(t_1, \dots, t_k) = \sum_{n_1, \dots, n_k \in \mathbb{N}} a_{n_1, \dots, n_k} t_1^{n_1} \cdots t_k^{n_k}$$

is the univariate series

$$\Delta f(x) = \sum_{n \in \mathbb{N}} a_{n, \dots, n} x^n.$$

In characteristic zero, the diagonal construction usually does not preserve algebraicity. However this astonishing property does hold in positive characteristic: the diagonal of an algebraic function over $\mathbb{F}_p(t_1, \dots, t_k)$ is algebraic over $\mathbb{F}_p(x)$! This result was originally observed and proved by Furstenberg [Fur67] when f is a rational function; it was then extended by Deligne [Del84] to algebraic functions and reproved many times by different authors [Sal86; Sal87; DL87; Har88; SW88] throughout the years. Deligne's theorem shows that the diagonals exhibit the phenomenon we are interested in in this article: the diagonal $\Delta f(x)$ of an algebraic function $f(t_1, \dots, t_k) \in \mathbb{Q}[[t_1, \dots, t_k]]$ is usually transcendental but its reductions modulo the primes, when they are defined, are algebraic (since they agree with the diagonals of $f \bmod p$).

The community then got interesting in finding upper bounds on the degree of algebraicity of $\Delta f(x) \bmod p$. When f is a rational function, Furstenberg's original proof leads to a bound of the form p^n where n depends only on f . It turns out that Deligne's proof leads to a similar bound when $f(t_1, t_2)$ is a bivariate algebraic function. The general case was solved by Adamczewski and Bell [AB13] who obtained again a general bound of the form p^n where n only depends on f . In [ABC23], after providing sharper bounds on the exponent n , the authors observed that, not only $\Delta f(x) \bmod p$ is annihilated by a polynomial $Z_p(Y)$ of degree at most p^n , but that there always exists such an annihilating polynomial of the form

$$Z_p(Y) = c_0(x)Y + c_1(x)Y^p + \dots + c_n(x)Y^{p^n} \quad (c_i(x) \in \mathbb{F}_p[x]). \quad (1.1)$$

They noticed moreover (see Remark 5.3 of *loc. cit.*) that this property implies that all the Galois conjugates of $\Delta f(x) \bmod p$ lie in a $\mathbb{F}_p(x)$ -vector space of dimension n , which further shows that the Galois group of $\Delta f(x) \bmod p$ canonically embeds, up to conjugacy, into $\mathrm{GL}_n(\mathbb{F}_p)$. Going even further, they suggested that all those Galois groups could have a common origin living in characteristic zero.

In the present article, we explore this question in slightly different contexts. To start with, we consider the class of D -finite functions. By definition the series $f(x) \in \mathbb{Q}[[x]]$ is called D -finite if it is a solution of a linear differential equation of the form

$$f^{(r)}(x) + a_{r-1}(x)f^{(r-1)}(x) + \dots + a_1(x)f'(x) + a_0(x)f(x) = 0 \quad (1.2)$$

where the coefficients $a_i(x)$ are rational functions. It is a standard fact that diagonals are D -finite but it turns out that the class of D -finite series is much larger; for instance, it includes the function $f(x) = \exp(\arctan(x))$ whose reduction modulo p only makes sense for primes p which are congruent to 1 modulo 4 (whereas diagonals can always be reduced modulo p for almost all primes p).

In Section 2, we formulate several hypothesis predicting the behavior of the Galois groups of $f(x) \bmod p$ when $f(x)$ is D -finite. Roughly speaking, if n denotes the minimal order of a differential equation satisfied by $f(x)$, what we expect is the existence of a number field K and a finite family G_1, \dots, G_t of subgroups of $\mathrm{GL}_n(K)$ with the following property: for any prime \mathfrak{p} of K for which $f(x) \bmod \mathfrak{p}$ is well defined and algebraic over $\mathbb{F}_p(x)$, there exists an integer $i \in \{1, \dots, t\}$ such that

$$\mathrm{Gal}(f(x) \bmod p \mid \bar{\mathbb{F}}_p(x)) \simeq \mathrm{image}(G_i \cap \mathrm{GL}_n(\mathcal{O}_{(\mathfrak{p})}) \rightarrow \mathrm{GL}_n(k_{\mathfrak{p}})).$$

Here $\mathcal{O}_{(\mathfrak{p})}$ denotes the localization of the ring of integer of K at \mathfrak{p} , that is the ring consisting of fractions of the form $\frac{a}{b}$ with $b \notin \mathfrak{p}$, and $k_{\mathfrak{p}}$ is the residue field. We refer to Conjecture 2.2.6 in the body of the text for a more precise statement.

We then elaborate further on this conjecture, trying to predict what could be the field K , the groups G_i , and the dependence of the index i with respect to p . This leads us to formulate stronger forms (see Conjectures 2.2.8 and 2.2.11) which, despite being technical, capture all what

we have glimpsed at so far. Finally, in Subsection 2.3.5, we investigate a possible relationship between the groups G_i and the differential Galois group of the differential equation (1.2).

In Section 3, we provide evidence towards our conjectures by studying in more details the special case of hypergeometric functions. We recall that, given two tuples $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_m)$ of rational numbers which are not nonpositive integers, the corresponding *hypergeometric function* is

$${}_nF_m(\alpha, \beta; x) := \sum_{k=0}^{\infty} \frac{(\alpha_1)_k (\alpha_2)_k \cdots (\alpha_n)_k}{(\beta_1)_k (\beta_2)_k \cdots (\beta_m)_k} \cdot \frac{x^k}{k!}$$

where $(\alpha)_k := \alpha \cdot (\alpha + 1) \cdots (\alpha + k - 1)$ is the *Pochhammer symbol*. It is a standard fact that hypergeometric functions are D -finite (but not necessarily diagonals). In Subsection 3.1, refining a former result of Christol, we classify the primes p for which the series ${}_nF_{n-1}(\alpha, \beta; x)$ reduces properly modulo p . In Subsection 3.2, we move to the main interest of this article and, following the strategy introduced in [Var24], we exhibit an annihilating polynomial for the function ${}_nF_{n-1}(\alpha, \beta; x) \bmod p$ (when it is defined) and study the corresponding Galois group. More precisely, we prove the following theorem.

Theorem 1.1. *Let n be a positive integer. Let $\alpha = (\alpha_1, \dots, \alpha_n)$ and $\beta = (\beta_1, \dots, \beta_{n-1})$ be tuples of rational numbers with $\alpha_i, \beta_j \notin -\mathbb{N}$ for all i, j . Let d be the smallest common denominator of the α_i and β_i and let $\mathbb{Q}(\zeta_d)$ be the d -th cyclotomic extension of \mathbb{Q} . Let K be the subextension of $\mathbb{Q}(\zeta_d)$ corresponding under Galois correspondence to the group*

$$D := \left\{ \lambda \in (\mathbb{Z}/d\mathbb{Z})^\times : \lambda \cdot \alpha \equiv \alpha \pmod{\mathbb{Z}} \text{ and } \lambda \cdot \beta \equiv \beta \pmod{\mathbb{Z}} \text{ as sets} \right\} \\ \subseteq (\mathbb{Z}/d\mathbb{Z})^\times \simeq \text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}).$$

Let $p > 2d \cdot \max\{|\alpha_i| + 1, |\beta_j| + 1\}$ be a prime number such that ${}_nF_{n-1}(\alpha, \beta; x) \in \mathbb{Z}_{(p)}[[x]]$. Then, letting $k_{\mathfrak{p}}$ be the residue field of K at a place \mathfrak{p} above p and writing $q := \text{Card}(k_{\mathfrak{p}})$, the function ${}_nF_{n-1}(\alpha, \beta; x) \bmod p$ is annihilated by a nonzero polynomial of the form

$$Z_p(Y) = c_0(x)Y + c_1(x)Y^q + \cdots + c_n(x)Y^{q^n} \quad \text{with } c_i(x) \in k_{\mathfrak{p}}(x).$$

In particular, the Galois group of ${}_nF_{n-1}(\alpha, \beta; x) \bmod p$ over $k_{\mathfrak{p}}(x)$ embeds into $\text{GL}_n(k_{\mathfrak{p}})$.

We notice in particular the emergence of a number field K , which is perfectly in line with our formulation of Conjecture 2.2.6. Moreover, we underline that the integer n appearing in $\text{GL}_n(k_{\mathfrak{p}})$, say the *embedding dimension*, is truly the same as the integer n we started with, which is also the order of the differential equation satisfied by ${}_nF_{n-1}(\alpha, \beta; x)$. Again, this is in perfect accordance with Conjecture 2.2.6. We mention nevertheless that, in this special case, the embedding dimension can even be lowered and looks more closely related to the dimension of the space of solutions of the hypergeometric equation in characteristic p .

Finally, in Subsection 3.3, we consider the special case of Gaussian hypergeometric functions ${}_2F_1(\alpha, (1); x)$ with $\alpha = (\alpha_1, \alpha_2) \in (\mathbb{Q} \setminus (-\mathbb{N}))^2$. In this situation, two important facts occur. Firstly, keeping the notation and assumptions of Theorem 1.1, the hypergeometric series ${}_2F_1(\alpha, (1); x)$ can be reduced modulo p for all prime p not dividing d . Secondly, the Galois group of ${}_2F_1(\alpha, (1); x) \bmod p$ over $k_{\mathfrak{p}}(x)$ always embeds into $\text{GL}_1(k_{\mathfrak{p}}) = k_{\mathfrak{p}}^\times$; in particular, it is commutative. The following theorem exhibits explicit subgroups of $\text{GL}_1(K) = K^\times$, which are serious candidates for uniformizing the above Galois groups when p varies.

Theorem 1.2. *We keep the notation and assumptions of Theorem 1.1 and assume moreover that $n = 2$, $\alpha_1, \alpha_2 \notin \mathbb{Z}$ and $\beta_1 = 1$. We set $K^+ := K \cap \mathbb{R}$, we let m be the denominator of an irreducible fraction representing $\alpha_1 + \alpha_2$, and we define the subgroup G of $\mathrm{GL}_1(K)$ by*

$$G := \begin{cases} \mathrm{GL}_1(K) & \text{if } K = K^+ \\ \mathrm{GL}_1(K^+) \cdot \langle \xi - \bar{\xi} \rangle & \text{if } K \neq K^+ \text{ and } m = 2 \\ \mathrm{GL}_1(K^+) \cdot \langle 1 + \zeta_m \rangle & \text{if } K \neq K^+ \text{ and } m \neq 2 \end{cases}$$

where ξ is an element of $K \setminus K^+$, $\bar{\xi}$ is its complex conjugate, $\zeta_m = \exp(2i\pi/m)$ is a primitive m -th root of unity and the notation $\langle \cdot \rangle$ stands for the generated subgroup.

Then, for any prime number p which does not divide d and any prime \mathfrak{p} of K above p , we have

$$\mathrm{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \bmod p \mid k_{\mathfrak{p}}(x)) \subseteq \mathrm{image}(G \cap \mathrm{GL}_1(\mathcal{O}_{(p)}) \rightarrow \mathrm{GL}_1(k_{\mathfrak{p}})),$$

where $\mathcal{O}_{(\mathfrak{p})}$ is the localization of the ring of integers of K at \mathfrak{p} .

Moreover, the above inclusion is an equality when $d \in \{2, 3, 4, 6, 8, 12, 24\}$.

We actually expect that the inclusion of Theorem 1.2 is (almost) always an equality but, unfortunately, we were not able to prove it in full generality. If our expectation is correct, this would say that the group G of Theorem 1.2 uniformizes the Galois groups of ${}_2F_1(\boldsymbol{\alpha}, (1); x) \bmod p$. For this reason, it appears as a very important invariant attached to the hypergeometric function ${}_2F_1(\boldsymbol{\alpha}, (1); x)$. Nonetheless, it remains quite mysterious to us: it looks like it is built from several pieces of different nature but, so far, we do not have a clear understanding of where these parts come from.

Notation. Throughout the article, we let \mathbb{Z} , \mathbb{Q} , \mathbb{R} and \mathbb{C} denote the set of integers, rational numbers, real numbers and complex numbers respectively. We also write \mathbb{N} for the set of nonnegative integers, and we denote accordingly the set of nonpositive integers by $-\mathbb{N}$. Besides, we choose and fix once for all a square root of -1 in \mathbb{C} , that we denote by the bold letter \mathbf{i} .

If a is an element in a ring A and I is an ideal of A , we use the notation $a \bmod I$ to denote the image of a in the quotient of A/I . We will often abuse notation and simply write $a \bmod d$ for $a \bmod dA$ when d is an element of A .

If g_1, \dots, g_n are some elements in a group G , we write $\langle g_1, \dots, g_n \rangle$ for the subgroup they generate in G . In particular, if a and d are two coprime integers, the notation $\langle a \bmod d \rangle$ will refer to the *multiplicative* subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by a .

Acknowledgements. The authors thank Alin Bostan and Gilles Christol for their interest in this work and helpful comments.

The second-named author was funded by the Austrian Science Fund FWF, grant [10.55776/P34765](#), and a DOC Fellowship (27150) of the [Austrian Academy of Sciences](#) at the University of Vienna. Further he thanks [Fédération MARGAUX](#) for supporting a one month research stay at the University of Bordeaux and the French–Austrian project EAGLES (ANR-22-CE91-0007 & FWF grant [10.55776/I6130](#)) for financial support.

The authors thank [Austria’s Agency for Education and Internationalisation \(OeAD\)](#) and Campus France for providing funding for research stays via WTZ collaboration project/Amadeus project FR02/2024.

2 A general picture of what we expect

In this section, we consider the general class of D -finite series $f(x)$ and aim at drawing a general picture of the behavior of the Galois groups of $f(x) \bmod p$ (when it is defined) when p varies. Let us first recall from the introduction that a series $f(x) \in \mathbb{Q}[[x]]$ is D -finite (or *differentially finite*) if it is solution of a linear differential equation of the form

$$f^{(r)}(x) + a_{r-1}(x)f^{(r-1)}(x) + \cdots + a_1(x)f'(x) + a_0(x)f(x) = 0 \quad (2.0.1)$$

with $a_i(x) \in \mathbb{Q}(x)$ for all i . It is a standard fact that D -finiteness translates to a recurrence relation on the coefficients of $f(x)$. It is also well known that the class of D -finite series is closed under sums and products; in other words, it forms a subring of $\mathbb{Q}[[x]]$ [Sta80].

On the Galois side, we introduce the following notation.

Definition 2.0.1. Let K be a field and let K^{sep} be a separable closure of K . For an element $a \in K^{\text{sep}}$, we set $\text{Gal}(a | K) := \text{Gal}(L/K)$ where L denotes the extension of K generated by a and its Galois conjugates.

From now on, we fix a separable closure $\mathbb{F}_p(x)^{\text{sep}}$ of $\mathbb{F}_p(x)$. Since the extension $\mathbb{F}_p((x))/\mathbb{F}_p(x)$ is itself separable, any algebraic series $f(x) \in \mathbb{F}_p[[x]]$ is automatically separable over $\mathbb{F}_p(x)$ and thus can be considered (noncanonically) as an element of $\mathbb{F}_p(x)^{\text{sep}}$. It then makes sense to talk about $\text{Gal}(f(x) | \mathbb{F}_p(x))$ and we check that this Galois group does not depend, up to isomorphism, on the choice of the representative of $f(x)$ in $\mathbb{F}_p(x)^{\text{sep}}$.

In what follows, if $f(x)$ is a series with coefficients in $\mathbb{Z}_{(p)}$ and $f(x) \bmod p$ is algebraic, we shall often slightly abuse notation and write $\text{Gal}(f(x) | \mathbb{F}_p(x))$ for $\text{Gal}(f(x) \bmod p | \mathbb{F}_p(x))$.

2.1 Getting intuition by examples

In this introductory subsection, we present and discuss various examples, illustrating the most important phenomena we have observed. For each example $f(x)$, we will determine the primes p for which $f(x) \bmod p$ is well-defined and algebraic and compute (or at least estimate) the corresponding Galois groups.

In the next subsections, we will rely on these results to elaborate our conjectures and justify their statements.

2.1.1 $f(x) = (1-x)^{a/d}$

We begin with a simple example, which is already algebraic over $\mathbb{Q}(x)$. Before proceeding, we underline that the expansion

$$f(x) = \sum_{k=0}^{\infty} (-1)^k \cdot \frac{a}{d} \cdot \left(\frac{a}{d} - 1\right) \cdots \left(\frac{a}{d} - k + 1\right) \cdot \frac{x^k}{k!}$$

shows that $f(x)$ is indeed in $\mathbb{Q}[[x]]$. We also note that it is also D -finite¹ since it is solution of the differential equation $d \cdot (1+x)f'(x) - af(x) = 0$.

As $f(x)$ is itself algebraic over $\mathbb{Q}(x)$, we start by computing its Galois group over $\mathbb{Q}(x)$. For this, assuming that a and d are coprime, we observe that the conjugates of $f(x)$ are the functions $\zeta_d^v f(x)$ ($0 \leq v < d$) where ζ_d is a primitive d -th root of unity, namely $\zeta_d = \exp(\frac{2i\pi}{d}) \in \mathbb{C}$. The corresponding splitting field is $\mathbb{Q}(x)(\zeta_d, f(x))$, which can be viewed as a Kummer extension on top of a cyclotomic extension:

¹In fact, it is a standard result that algebraic functions are always D -finite.

$$\begin{array}{c}
\mathbb{Q}(x)(\zeta_d, f(x)) \\
\left| \text{Kummer extension} \right. \\
\mathbb{Q}(x)(\zeta_d) \\
\left| \text{cyclotomic extension} \right. \\
\mathbb{Q}(x)
\end{array}$$

The Galois group of the cyclotomic extension is $(\mathbb{Z}/d\mathbb{Z})^\times$, while that of the Kummer extension is cyclic of order d , and hence isomorphic to $\mathbb{Z}/d\mathbb{Z}$. We deduce from this that

$$\text{Gal}(f(x) | \mathbb{Q}(x)) \simeq \mathbb{Z}/d\mathbb{Z} \rtimes (\mathbb{Z}/d\mathbb{Z})^\times$$

where $(\mathbb{Z}/d\mathbb{Z})^\times$ acts on $\mathbb{Z}/d\mathbb{Z}$ by multiplication. Concretely, the action of the Galois group on $\mathbb{Q}(x)(\zeta_d, f(x))$ is given by $\zeta_d \mapsto \zeta_d^u$, $f(x) \mapsto \zeta_d^v f(x)$ for $u \in (\mathbb{Z}/d\mathbb{Z})^\times$ and $v \in \mathbb{Z}/d\mathbb{Z}$.

The series $f(x)$ can be properly reduced modulo p for any prime number p which does not divide d . Assuming this, we can compute $\text{Gal}(f(x) | \mathbb{F}_p(x))$ by applying the same strategy as in characteristic zero. The only difference is that the Galois group of the cyclotomic part can now be a *strict* subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$. More precisely, it is the same as the Galois group of $\mathbb{F}_p(\xi_d)/\mathbb{F}_p$ where ξ_d is a primitive d -th root of unity in an algebraic closure of \mathbb{F}_p . This Galois group being generated by the Frobenius, we conclude that $\text{Gal}(\mathbb{F}_p(x)(\xi_d)/\mathbb{F}_p(x))$ is the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p . Therefore, we finally find

$$\text{Gal}(f(x) | \mathbb{F}_p(x)) \simeq \mathbb{Z}/d\mathbb{Z} \rtimes \langle p \bmod d \rangle.$$

Altogether this shows that there are only finitely many possibilities for $\text{Gal}(f(x) | \mathbb{F}_p(x))$ when p varies. More precisely, this Galois group is entirely determined by the class of p modulo d .

2.1.2 $f(x) = \exp(\arctan x)$

In this example, the function $f(x)$ is transcendental over $\mathbb{Q}(x)$ but still it is the solution of a linear differential equation of order 1, given that

$$\frac{f'(x)}{f(x)} = \arctan'(x) = \frac{1}{x^2 + 1}. \quad (2.1.1)$$

Using Dwork's criterion [Rob00, p.409], one proves that $f(x) \in \mathbb{Z}_{(p)}[[x]]$ if and only if $p \equiv 1 \pmod{4}$ (see also [BCR24, Example 3.34]). For those primes, it turns out that the differential equation (2.1.1) can be solved over the p -adics.

Let \mathbb{Z}_p be the ring of p -adic integers and let $i \in \mathbb{Z}_p$ be a square root of -1 (which exists because p is congruent to 1 modulo 4). Over $\mathbb{Z}_p(x)$, we have the following partial fraction decomposition:

$$\frac{1}{x^2 + 1} = \frac{1}{2} \cdot \left(\frac{1}{1 + ix} + \frac{1}{1 - ix} \right).$$

Solving Equation (2.1.1) and taking care of the initial condition $f(0) = 1$, we obtain the following closed formula for $f(x)$:

$$f(x) = (1 + ix)^{-i/2} \cdot (1 - ix)^{i/2} \in \mathbb{Z}_p[[x]]. \quad (2.1.2)$$

Here the p -adic exponentiation is defined through its p -adic expansion; namely, for $a \in \mathbb{Z}_p$ and a formal expression u , we set

$$(1+u)^a := \sum_{k=0}^{\infty} \frac{a \cdot (a-1) \cdots (a-k+1)}{k!} \cdot u^k.$$

We now write the p -adic expansions of the exponents $-i/2$ and $i/2$ as follows:

$$-\frac{i}{2} = a_0 + pa_1 + p^2a_2 + \cdots \quad \text{and} \quad \frac{i}{2} = b_0 + pb_1 + p^2b_2 + \cdots$$

with $a_k, b_k \in \{0, 1, \dots, p-1\}$. Reducing Equation (2.1.2) modulo p then gives

$$f(x) \bmod p = \prod_{k=0}^{\infty} (1 + ix^{p^k})^{a_k} \cdot (1 - ix^{p^k})^{b_k} \in \mathbb{F}_p[[x]],$$

where $i \equiv 2b_0 \pmod{p}$.

Proposition 2.1.1. *For all primes p congruent to 1 modulo 4, the function $f(x) \bmod p$ is transcendental over $\mathbb{F}_p(x)$.*

Proof. For an integer $u \in \{0, \dots, p-1\}$, we define $g_u(x) := (1+ix)^u \cdot (1-ix)^{p-1-u}$ and, for a sequence $\underline{u} = (u_k)_{k \geq 0}$, we set

$$g_{\underline{u}}(x) := \prod_{k=0}^{\infty} g_{u_k}(x^{p^k}) = \prod_{k=0}^{\infty} g_{u_k}(x)^{p^k}.$$

Noticing that $a_0 + b_0 = p$ and $a_k + b_k = p-1$ as soon as $k \geq 1$, we find $f(x) = (1-ix) \cdot g_{\underline{a}}(x)$ in $\mathbb{F}_p[[x]]$ where $\underline{a} = (a_k)_{k \geq 0}$. Hence it is enough to prove that $g_{\underline{a}}(x)$ is transcendental.

For $r \in \{0, \dots, p-1\}$, we introduce the section operator

$$\sigma_r : \mathbb{F}_p[[x]] \rightarrow \mathbb{F}_p[[x]], \quad \sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} a_{pn+r} x^n.$$

The action of σ_r on the series $g_{\underline{u}}(x)$ is easily described. Indeed, remarking that $\sigma_r(g(x)^p h(x)) = g(x) \sigma_r(h(x))$ for all series $g(x)$ and $h(x)$, we obtain the relation

$$\sigma_r(g_{\underline{u}}(x)) = \sigma_r(g_{u_0}(x)) \cdot g_{S\underline{u}}(x)$$

where $S\underline{u}$ is the shifted sequence defined by $(S\underline{u})_k = u_{k+1}$ for $k \in \mathbb{N}$. We notice in addition that the prefactor $\sigma_r(g_{u_0}(x))$ is a scalar in \mathbb{F}_p given that $g_{u_0}(x)$ is a polynomial of degree $p-1$. Moreover, when $r = 0$, this scalar is 1 and we just have $\sigma_0(g_{\underline{u}}(x)) = g_{S\underline{u}}(x)$.

We now use the following characterization of algebraicity, known as Christol's theorem [Chr79; Chr+80]: a series $g(x) \in \mathbb{F}_p[[x]]$ is algebraic over $\mathbb{F}_p(x)$ if and only if there exists a finite set which contains $g(x)$ and is stable by the σ_r . In our case of interest, it is then enough to prove that the series $\sigma_0^k(g_{\underline{a}}(x)) = g_{S^k \underline{a}}(x)$ are pairwise distinct.

Let $\ell > k$ be two nonnegative integers. We first notice that the sequences $S^k \underline{a}$ and $S^\ell \underline{a}$ cannot be equal. Indeed, from their coincidence, we would deduce that \underline{a} is ultimately periodic (with period $\ell-k$), which is not the case because $i \notin \mathbb{Q}$. We now fix an integer n such that restricting to the n first terms is enough to distinguish between $S^k \underline{a}$ and $S^\ell \underline{a}$. An easy computation shows that

$$\begin{aligned} g_{S^k \underline{a}}(x) &\equiv \frac{1}{1-ix} \cdot \left(\frac{1+ix}{1-ix} \right)^{a_k + pa_{k+1} + \cdots + p^{n-1} a_{k+n-1}} \pmod{x^{p^n}} \\ g_{S^\ell \underline{a}}(x) &\equiv \frac{1}{1-ix} \cdot \left(\frac{1+ix}{1-ix} \right)^{a_\ell + pa_{\ell+1} + \cdots + p^{n-1} a_{\ell+n-1}} \pmod{x^{p^n}} \end{aligned}$$

Thanks to our choice of n , the exponents appearing in the above expressions are distinct. Observing moreover that the change of variables $y = \frac{1+ix}{1-ix}$ is invertible in $\mathbb{F}_p[[x]]$ (with inverse $x = i \cdot \frac{y-1}{y+1}$), we conclude that $g_{S^k_a}(x)$ and $g_{S^{\ell}_a}(x)$ are not congruent modulo x^{p^n} , and so that they are not equal. \square

Remark 2.1.2. Examples 2.1.1 and 2.1.2 are representative of all what can happen with differential equations of order 1. Indeed, let us consider a series $f(x)$ which is solution of the equation $f'(x) = a(x)f(x)$ for some $a(x) \in \mathbb{Q}(x)$. If $a(x)$ exhibits a multiple pole (possibly at infinity), then $f(x)$ is transcendental and cannot be reduced modulo p for any prime p . Otherwise we have the following dichotomy:

- (Case of Example 2.1.1) If the residues of $a(x)$ all lie in \mathbb{Q} , then $f(x)$ is algebraic over $\mathbb{Q}(x)$. In this case, $f(x)$ can be reduced modulo almost all primes p and all those reductions are algebraic with Galois groups closely related to the Galois group of $f(x)$ over $\mathbb{Q}(x)$.
- (Case of Example 2.1.2) If one residue of $a(x)$ is not in \mathbb{Q} , then $f(x)$ is transcendental over $\mathbb{Q}(x)$. In this case, $f(x)$ can be reduced modulo p if and only if $a(x) \bmod p$ continues to have only simple poles in $\mathbb{P}^1(\mathbb{F}_p)$ and all the corresponding residues are in \mathbb{F}_p . Moreover, when this occurs, $f(x) \bmod p$ is always transcendental.

$$\mathbf{2.1.3} \quad f(x) = \sum_{n=0}^{\infty} \binom{2n}{n}^2 \cdot x^n$$

Before computing Galois groups, we briefly mention that the series $f(x)$ is indeed D -finite as the sequence of its coefficients obviously satisfies a recurrence relation with polynomial coefficients. Concretely, $f(x)$ is a solution of the differential equation

$$x(16x-1)f''(x) + (32x-1)f'(x) + 4f(x) = 0. \quad (2.1.3)$$

Apart from this, the function $f(x)$ is also one of the simplest examples of a series exhibiting the p -Lucas property, which will play a very important role throughout this paper. To explain what it means, we pick a nonnegative integer n and write the Euclidean division of n by p as follows: $n = u + pv$. We then have the congruence

$$(1+x)^{2n} \equiv (1+x)^{2u} \cdot (1+x^p)^{2v} \pmod{p},$$

which, after extracting the coefficient of x^n , leads to

$$\binom{2n}{n} \equiv \binom{2u}{u} \cdot \binom{2v}{v} \pmod{p}.$$

Raising this congruence to the square, we deduce that the coefficients a_n of $f(x)$ satisfy the congruence $a_n \equiv a_u a_v \pmod{p}$ as well; we say that the series $f(x)$ is p -Lucas.

The p -Lucas property has strong consequences on the Galois groups we are interested in. Indeed, defining the truncation

$$A_p(x) = \sum_{n=0}^{p-1} a_n x^n \in \mathbb{F}_p[x],$$

being p -Lucas translates to the algebraic relation

$$f(x) \equiv A_p(x) \cdot f(x)^p \pmod{p}.$$

In particular, $f(x) \bmod p$ is algebraic and, even better, it appears as a $(p-1)$ -th root of the polynomial $A_p(x)$. Since \mathbb{F}_p contains all the $(p-1)$ -th roots of unity, Kummer's theory ensures that $\text{Gal}(f(x) | \mathbb{F}_p(x))$ embeds into $\mu_{p-1}(\mathbb{F}_p) = \mathbb{F}_p^\times$ and that equality holds as soon as $A_p(x)$ is a not a power (with exponent at least 2) of a rational function.

The following lemma will be used many times throughout the rest of the paper. It helps to determine the multiplicity of certain polynomials tied to solutions of differential equations.

Lemma 2.1.3. *Let $g(x) \in \mathbb{F}_p[[x]]$ be a power series, which satisfies a linear differential equation with polynomial coefficients of order $r < p$. Let $\overline{\mathbb{F}}_p$ denote a fixed algebraic closure of \mathbb{F}_p and let $\xi \in \overline{\mathbb{F}}_p$ be an ordinary point of that differential equation. If $g(x) = A(x)h(x^p)$ for some polynomial $A(x)$ of degree less than p and some power series $h(x) \in \mathbb{F}_p[[x]]$, then $\text{val}_\xi(A(x)) < r$.*

In particular, if $g(x)$ is p -Lucas, then $\text{val}_\xi(g(x) \bmod x^p) < r$.

Proof. From $g(x) = A(x)h(x^p)$, it is clear that $A(x)$ is a solution of the same differential equation as $g(x)$. The local exponents of this equation at ξ are $0, 1, \dots, r-1$. Thus, $\text{val}_\xi(A(x)) \in \{0, 1, \dots, r-1\} \bmod p$. Because $\deg(A(x)) < p$, we conclude $\text{val}_\xi(A(x)) \in \{0, 1, \dots, r-1\}$. \square

Back to our example of the generating function of the squares of the central binomial coefficients, we can use Lemma 2.1.3 to obtain the following.

Corollary 2.1.4. *If $p > 2$, the polynomial $A_p(x)$ cannot be written as $B(x)^e$ with $B(x) \in \mathbb{F}_p(x)$ and $e > 1$.*

Proof. To start with, we observe that $A_p(x)$ is a polynomial of degree exactly $\frac{p-1}{2}$, because, when $\frac{p}{2} \leq n < p$, the central binomial coefficient $\binom{2n}{n}$ is divisible by p . Moreover, any element $\xi \in \overline{\mathbb{F}}_p \setminus \{0, \frac{1}{16}\}$ is a regular point of the differential equation (2.1.3). By Lemma 2.1.3, we find that ξ cannot be a double root of $A_p(x)$. Clearly $A_p(0) = 1$, so 0 is also not a (double) root of $A_p(x)$. To conclude, it then remains to exclude the case $A_p(x) = (1-16x)^{\frac{p-1}{2}}$. This can be done easily by looking at the coefficient of x : in $A_p(x)$, it is equal to 4, while in the right hand side, it is equal to $-8(p-1)$, which is 8 modulo p . \square

It follows from all what precedes that $\text{Gal}(f(x) | \mathbb{F}_p(x)) \simeq \mathbb{F}_p^\times$ for $p > 2$. The isomorphism is actually also correct when $p = 2$ because $f(x) \bmod p = 1$ in this case.

$$\mathbf{2.1.4} \quad f(x) = \sum_{n=0}^{\infty} \binom{2n}{n}^3 \cdot x^n$$

This example looks similar to the previous one (the only difference is that the exponent 2 has been replaced by 3) but we will see that the behavior of the Galois groups exhibits a new interesting phenomenon.

The function $f(x)$ is still D -finite and is now a solution of a differential equation of order 3:

$$x^2(64x-1)f'''(x) + x(288x-3)f''(x) + (208x-1)f'(x) + 8f(x) = 0.$$

Of course, $f(x)$ is again p -Lucas, from which we get the algebraic relation

$$f(x) \equiv A_p(x) \cdot f(x)^p \pmod{p},$$

where $A_p(x)$ is the truncation of $f(x)$ defined by

$$A_p(x) = \sum_{n=0}^{p-1} \binom{2n}{n}^3 \cdot x^n \in \mathbb{F}_p[x].$$

Again, this implies that $\text{Gal}(f(x) \mid \mathbb{F}_p(x))$ embeds into \mathbb{F}_p^\times but it might happen now that this inclusion is strict.

Lemma 2.1.5. *Let p be prime number with $p \equiv 1 \pmod{4}$. Then $A_p(x)$ is a square in $\mathbb{F}_p[x]$.*

Proof. We reinterpret the function $f(x)$ as an hypergeometric series as follows:

$$f(x) = {}_3F_2\left(\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), (1, 1); 64x\right).$$

It then follows from Clausen's formula [Cla28] that $f(x) = g(x)^2$ with $g(x) = {}_2F_1\left(\left(\frac{1}{4}, \frac{1}{4}\right), (1); 64x\right)$. We now let $B_p(x)$ denote the truncation at x^p of $g(x) \pmod{p}$, so that

$$A_p(x) \equiv B_p(x)^2 \pmod{x^p}. \quad (2.1.4)$$

As in the proof of Corollary 2.1.4, we find that $A_p(x)$ has degree $\frac{p-1}{2}$. Similarly, using the congruence $p \equiv 1 \pmod{4}$, we prove that $\deg B_p(x) = \frac{p-1}{4}$. Hence the congruence (2.1.4) has to be an equality in $\mathbb{F}_p[x]$, which proves the lemma. \square

By Lemma 2.1.3, we have that $A_p(x)$ is not a e -th power for any $e > 2$. Moreover, when $p \equiv 3 \pmod{4}$, it is not a square either because it has odd degree. We conclude that

$$\text{Gal}(f(x) \mid \mathbb{F}_p(x)) \simeq \begin{cases} (\mathbb{F}_p^\times)^\square & \text{if } p \equiv 3 \pmod{4} \\ \mathbb{F}_p^\times & \text{if } p \equiv 1 \pmod{4} \end{cases}, \quad (2.1.5)$$

where, when G is a commutative group, the notation G^\square refers to its subgroup of squares.

2.1.5 $f(x) = \sum_{n=0}^{\infty} \sum_{k=0}^n \binom{n+k}{k}^2 \binom{n}{k}^2 \cdot x^n$ **and related functions**

The series $f(x)$ is the so-called *Apéry series* because the sequence of its coefficients appears as a key ingredient in Apéry's proof of the irrationality of $\zeta(3)$ [Apé79; Fis04]. It is solution of the differential equation

$$x^2(x^2 - 34x + 1)f'''(x) + 3x(2x^2 - 51x + 1)f''(x) + (7x^2 - 112x + 1)f'(x) + (x - 5)f(x) = 0 \quad (2.1.6)$$

and it turns out that the reductions of $f(x)$ modulo the primes behave quite similarly to what we described in the previous example. First of all, it is known that $f(x)$ is p -Lucas [Ges82]. Therefore, once again, its reductions modulo p satisfy the algebraic relation

$$f(x) \equiv A_p(x) \cdot f(x)^p \pmod{p}$$

where $A_p(x)$ is the truncation of $f(x)$:

$$A_p(x) = \sum_{n=0}^{p-1} \sum_{k=0}^n \binom{n+k}{k}^2 \binom{n}{k}^2 \cdot x^n \in \mathbb{F}_p[x].$$

As a consequence the Galois group $\text{Gal}(f(x) \mid \mathbb{F}_p(x))$ appears as a subgroup of \mathbb{F}_p^\times . Moreover since the order of the differential equation (2.1.6) is 3, Lemma 2.1.3 shows that $A_p(x)$ cannot be a e -th power with $e > 2$ (except if it is a constant polynomial). However it still can be a square and, as we will see in the sequel, this actually happens from time to time.

Computational experiments tend to imply that whether $A_p(x)$ is a square or not is governed by the class of congruence of p modulo 24. More precisely, we observed the following.

Heuristic observation 2.1.6. *There exists a polynomial $B_p(x) \in \mathbb{F}_p[x]$ such that*

- $A_p(x) = B_p(x)^2$ if $p \equiv 1, 5, 7, 11 \pmod{24}$,
- $A_p(x) = (x^2 - 34x + 1) \cdot B_p(x)^2$ if $p \equiv 13, 17, 19, 23 \pmod{24}$.

We leave the above heuristic as an open question for the time being and explore its consequences. First of all, at the level of Galois groups, it implies

$$\text{Gal}(f(x) \mid \mathbb{F}_p(x)) \simeq \begin{cases} (\mathbb{F}_p^\times)^\square & \text{if } p \equiv 1, 5, 7, 11 \pmod{24} \\ \mathbb{F}_p^\times & \text{if } p \equiv 13, 17, 19, 23 \pmod{24} \end{cases}$$

given that the polynomial $x^2 - 34x + 1$ is not a square in $\mathbb{F}_p[x]$ as soon as $p \geq 5$.

Going further, Heuristic 2.1.6 suggests to introduce the following functions:

$$g(x) = \sqrt{f(x)} \quad \text{and} \quad h(x) = \sqrt{\frac{f(x)}{x^2 - 34x + 1}}.$$

Those can be expanded as series in the variable x , and so they are elements of $\mathbb{Q}[[x]]$. Moreover, it turns out that they are both D -finite, being solutions of the differential equations

$$\begin{aligned} 4x(x^2 - 34x + 1)g''(x) + 4(2x^2 - 51x + 1)g'(x) + (x - 10)g(x) &= 0, \\ 4x(x^2 - 34x + 1)h''(x) + 4(4x^2 - 85x + 1)h'(x) + (9x - 78)h(x) &= 0. \end{aligned}$$

Of course, $g(x) \pmod{p}$ and $h(x) \pmod{p}$ are also algebraic and one can be interested in their Galois groups. When $A_p(x) = B_p(x)^2$, we have

$$g(x) = \frac{g(x)^p}{\sqrt{f(x)^{p-1}}} \equiv B_p(x) \cdot g(x)^p \pmod{p}$$

and similarly

$$h(x) \equiv (x^2 - 34x + 1)^{\frac{p-1}{2}} B_p(x) \cdot h(x)^p \pmod{p}.$$

In this case, we see that the series $g(x) \pmod{p}$ and $h(x) \pmod{p}$ satisfy algebraic relations of the same shape and, using that $B_p(x)$ is not an e -th power for any $e > 1$ (because $A_p(x)$ has no ordinary points as roots of multiplicity $2e$), we conclude that

$$\text{Gal}(g(x) \mid \mathbb{F}_p(x)) \simeq \text{Gal}(h(x) \mid \mathbb{F}_p(x)) \simeq \mathbb{F}_p^\times.$$

On the contrary, when $A_p(x) = (x^2 - 34x + 1) \cdot B_p(x)^2$, we get the relations

$$g(x) \equiv (x^2 - 34x + 1)^{\frac{p+1}{2}} B_p(x) \cdot h(x)^p \pmod{p} \tag{2.1.7}$$

$$h(x) \equiv B_p(x) \cdot g(x)^p \pmod{p} \tag{2.1.8}$$

which now intertwine the functions $g(x)$ and $h(x)$. Combining these equations, we deduce the untangled algebraic relations

$$g(x) \equiv (x^2 - 34x + 1)^{\frac{p+1}{2}} B_p(x)^{p+1} \cdot g(x)^{p^2} \pmod{p} \tag{2.1.9}$$

$$h(x) \equiv (x^2 - 34x + 1)^{\frac{p(p+1)}{2}} B_p(x)^{p+1} \cdot h(x)^{p^2} \pmod{p}. \tag{2.1.10}$$

We observe that the coefficients of $g(x)^{p^2}$ and of $h(x)^{p^2}$ on the right hand sides of these equations both are $\frac{p+1}{2}$ -th powers, but not higher ones. So, at the level of Galois groups, we obtain

$$\mathrm{Gal}(g(x) \mid \mathbb{F}_p(x)) \simeq \mathrm{Gal}(h(x) \mid \mathbb{F}_p(x)) \simeq \sqrt{\mathbb{F}_p^\times} \rtimes \mathbb{Z}/2\mathbb{Z},$$

where by definition

$$\sqrt{\mathbb{F}_p^\times} := \left\{ x \in \mathbb{F}_{p^2}^\times \text{ such that } x^2 \in \mathbb{F}_p^\times \right\}$$

and where $\mathbb{Z}/2\mathbb{Z}$ acts on it through the Frobenius.

Remark 2.1.7. In these examples, we observe that both of the Galois groups $\mathrm{Gal}(g(x) \mid \mathbb{F}_p(x))$ and $\mathrm{Gal}(h(x) \mid \mathbb{F}_p(x))$ might be commutative for an infinitely many primes p and noncommutative for another infinity of primes p at the same time (at least if we believe in Heuristic 2.1.6).

Remark 2.1.8. We thank Alin Bostan for pointing out to us that similar phenomena occur with several other series of interest. Here are two examples:

- The generating series of Domb numbers [Dom60]

$$f(x) = \sum_{n=0}^{\infty} \sum_{k=0}^n \binom{2k}{k} \binom{2n-2k}{n-k} \binom{n}{k}^2 \cdot x^n.$$

In this case, computations suggest that the Galois group $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$ is \mathbb{F}_p^\times when $p \equiv -1 \pmod{6}$ and its subgroup of squares when $p \equiv 1 \pmod{6}$.

- The generating series of Almkvist–Zudilin numbers [Zag09; AZ06]

$$f(x) = \sum_{n=0}^{\infty} \sum_{k=0}^n (-1)^{n-k} 3^{n-3k} \frac{(3k)!}{k!^3} \binom{n}{3k} \binom{n+k}{k} \cdot x^n.$$

In this case, our computations tend to imply that the Galois group $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$ is \mathbb{F}_p^\times when $p \equiv 5, 7 \pmod{8}$ and its subgroup of squares when $p \equiv 1, 3 \pmod{8}$.

These examples, together with the Apéry numbers, are appearing as sporadic examples of differential equations having solutions with integral coefficients, studied for example in [Beu02; Zag09; AVZ11]. Especially [AVZ11, Theorem 4.1] is reminiscent of our argument involving Clausen’s formula in the proof of Lemma 2.1.5. It expresses the Apéry series (where the variable is substituted by a rational function) as the square of another, explicitly determined, power series times a polynomial, and could provide direction in the quest to prove our Observations 2.1.6.

2.1.6 $f(x) = {}_3F_2\left(\left(\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right), \left(\frac{1}{3}, 1\right); x\right)$

We conclude our tour by an example of a hypergeometric function, anticipating on the forthcoming results of Section 3. Here, the series $f(x)$ is a solution of the differential equation

$$729x^2(x-1)f'''(x) + 81x(37x-21)f''(x) + 9(200x-27)f'(x) + 20f(x) = 0.$$

In Section 3 (see Example 3.2.14), we will show that $f(x)$ can be reduced modulo any prime $p \neq 3$ and that the Galois group of $f(x) \pmod{p}$ satisfy

$$\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x)) \subset \begin{cases} \mathrm{GL}_2(\mathbb{F}_p) & \text{if } p \equiv 1 \pmod{9} \\ \mathbb{F}_{p^6}^\times \rtimes \mathbb{Z}/6\mathbb{Z} & \text{if } p \equiv 2 \text{ or } 5 \pmod{9} \\ \mathrm{GL}_2(\mathbb{F}_{p^3}) \rtimes \mathbb{Z}/3\mathbb{Z} & \text{if } p \equiv 4 \text{ or } 7 \pmod{9} \\ \mathbb{F}_{p^2}^\times \rtimes \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 8 \pmod{9} \end{cases} \quad (2.1.11)$$

where the element $1 \in \mathbb{Z}/d\mathbb{Z}$ ($d \in \{2, 3, 6\}$) always acts through the Frobenius on the left-hand factor of the semi-direct product. We actually expect that all these inclusions are equalities but were not able to prove it in full generality.

This example is novel in the sense that, for the first time, it goes beyond cyclic groups (or simple semi-direct products of them) and involves groups of matrices of higher rank. We see moreover that the latter does not show up in each case: for some classes of congruences, the expected Galois group remains resoluble while it suddenly becomes more complicated for other congruences classes.

2.2 The conjectures: weak and strong forms

The aim of this subsection is to formulate plausible conjectures describing the behavior of $\text{Gal}(f(x) \mid \mathbb{F}_p(x))$ when p varies.

2.2.1 Discarding too naive expectations

Since $\text{Gal}(f(x) \mid \mathbb{F}_p(x))$ always appears as a subgroup of $\text{GL}_n(\mathbb{F}_p)$ for some integer n (depending possibly on p), the first naive question we may wonder about is the following: does there exist a subgroup of $\text{GL}_n(\mathbb{Z})$ whose reduction modulo p agrees with $\text{Gal}(f(x) \mid \mathbb{F}_p(x))$ for (almost) all primes p ? Unfortunately, the answer is negative, even if we replace \mathbb{Z} by $\mathbb{Z}[\frac{1}{N}]$ for a positive integer N . Indeed, Subsection 2.1.5 exhibits a situation where $\text{Gal}(g(x) \mid \mathbb{F}_p(x))$ is commutative for half of the primes and noncommutative for the other half; the next lemma shows that this cannot occur for the reductions modulo p of a single subgroup of $\text{GL}_n(\mathbb{Z}[\frac{1}{N}])$.

Lemma 2.2.1. *Let G be a subgroup of $\text{GL}_n(\mathbb{Z}[\frac{1}{N}])$ for some positive integers n and N . We assume that, for infinitely many primes p , the image of G in $\text{GL}_n(\mathbb{F}_p)$ is commutative. Then G is commutative.*

Proof. We pick $A, B \in G$ and form the commutator $C = ABA^{-1}B^{-1}$. For any prime p not dividing N , the matrix $C \bmod p$ is the commutator of $A \bmod p$ and $B \bmod p$. Thanks to our assumption, these commutators are trivial for infinitely many such primes p . Hence, denoting by I_n the identity matrix, we get $C \equiv I_n \pmod{p}$ for infinitely many primes p . Therefore $C = I_n$ and we conclude that A and B commute in G . \square

Remark 2.2.2. One may argue that the issue we just raised with the function $g(x)$, defined as the square root of the Apéry series in Example 2.1.5, can be easily fixed by considering Galois groups over $\mathbb{F}_{p^2}(x)$ instead of $\mathbb{F}_p(x)$: doing this, the factors $\mathbb{Z}/2\mathbb{Z}$ disappear and all the Galois groups $\text{Gal}(g(x) \mid \mathbb{F}_{p^2}(x))$ are commutative. This is indeed correct. However, Example 2.1.6 shows an even worse situation where half of the groups are resoluble, while the other half of them are not; in this case, the issue cannot be solved by changing the base field.

If one unique subgroup of $\text{GL}_n(\mathbb{Z}[\frac{1}{N}])$ is not enough to uniformize, one may now wonder if a finite family of them could do the job. Unfortunately, this is again not the case: a counterexample is given by Example 2.1.3, as shown by the next proposition.

Proposition 2.2.3. *Let t, n , and N be positive integers and let G_1, \dots, G_t be subgroups of $\text{GL}_n(\mathbb{Z}[\frac{1}{N}])$. Then, there exist infinitely many prime numbers p , not dividing N , for which none of the groups $G_1 \bmod p, \dots, G_t \bmod p$ are cyclic of order $p-1$.*

Proof. For $i \in \{1, \dots, t\}$, we let \mathcal{P}_i denote the set of primes p , not dividing N , for which $G_i \bmod p$ is cyclic of order $p-1$. We also set $\mathcal{P} := \mathcal{P}_1 \cup \dots \cup \mathcal{P}_t$ and denote by \mathcal{P}' the complement of \mathcal{P} in the set of all primes. We have to show that \mathcal{P}' is infinite.

Without loss of generality, we may assume that each \mathcal{P}_i is infinite. Indeed, when \mathcal{P}_i is finite, the lemma for the family $(G_1, \dots, G_{i-1}, G_{i+1}, \dots, G_t)$ implies the lemma for (G_1, \dots, G_t) .

We fix an index i . We claim that all matrices in G_i are semi-simple, *i.e.*, diagonalizable over an algebraic closure \mathbb{Q} . Indeed, pick $M \in G_i$ and a change-of-basis matrix $A \in \mathrm{GL}_n(\mathbb{Q})$ such that $T := A^{-1}MA$ is in Jordan form. We notice that A has all its entries in a certain number field K . Besides, A and M can be reduced modulo p for almost prime number p . We assume by contradiction that T has a nontrivial Jordan block of the form

$$T_0 := \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \lambda & 1 \\ & & & \lambda \end{pmatrix}.$$

For almost all primes $p \in \mathcal{P}_i$, we have

$$T_0^{p-1} \equiv \begin{pmatrix} \lambda^{p-1} & -\lambda^{p-2} & \star & \star \\ & \ddots & \ddots & \star \\ & & \lambda^{p-1} & -\lambda^{p-2} \\ & & & \lambda^{p-1} \end{pmatrix} \pmod{p}.$$

From the fact that $G_i \pmod{p}$ is cyclic of order $p-1$, we deduce that λ must vanish modulo p . Since this holds for infinitely many primes p , we finally obtain $\lambda = 0$, which is a contradiction.

On the other hand, we deduce from Lemma 2.2.1 that G_i is commutative. Consequently, all matrices in G_i are simultaneously diagonalizable, *i.e.*, there exists a matrix $A \in \mathrm{GL}_n(K_i)$ (for a certain number field K_i) such that $A^{-1}MA$ is diagonal for all $M \in G_i$. Up to enlarging N , we may further assume that $A \in \mathrm{GL}_n(\mathcal{O}_{K_i}[\frac{1}{N}])$ where \mathcal{O}_{K_i} denotes the ring of integers of K_i . Let H_i be the subgroup of $\mathcal{O}_{K_i}[\frac{1}{N}]^\times$ generated by all the eigenvalues of all the matrices $M \in G_i$. By Dirichlet's theorem, we know that $\mathcal{O}_{K_i}[\frac{1}{N}]^\times$ is of finite type. Hence H_i is also and we can choose a finite set of generators S_i of H_i .

We now uniformize this construction over i : we let K be the number field generated by all the K_i and set $S := S_1 \cup \dots \cup S_t$. By Chebotarev's density theorem applied to the number field $L = K(\sqrt{s}, s \in S)$, there exist infinitely many primes p such that p splits in K and $s \pmod{\mathfrak{p}}$ is a square in \mathbb{F}_p for all $s \in S$ and all primes \mathfrak{p} of K above p . For those primes, all groups G_i reduce modulo p to a subgroup of $(\mathbb{F}_p^\times)^\square$ and hence cannot have order $p-1$. \square

2.2.2 First formulation of the conjecture

The previous discussion leaves open the possibility that the Galois groups $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$ are uniformized by a finite family (G_1, \dots, G_t) of subgroups of $\mathrm{GL}_n(\mathbb{Q})$ in the following sense: for each prime p , there exists an index i such that

$$\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x)) \simeq \mathrm{image}(G_i \cap \mathrm{GL}_n(\mathbb{Z}_{(p)}) \rightarrow \mathrm{GL}_n(\mathbb{F}_p)),$$

where we recall that $\mathbb{Z}_{(p)}$ denotes the localization of \mathbb{Z} at p . At least, this formulation clearly allows for catching $\mathbb{F}_p^\times = \mathrm{GL}_1(\mathbb{F}_p)$ for all p , as we can simply take $G = \mathrm{GL}_1(\mathbb{Q})$.

Although this expectation looks rather reasonable, many examples encountered in Subsection 2.1 involve the multiplicative group of some finite extension of \mathbb{F}_p . It then sounds natural to look for the groups G_i , not inside $\mathrm{GL}_n(\mathbb{Q})$, but rather inside $\mathrm{GL}_n(K)$ where K is a number field.

In a similar fashion, we observe that most of the Galois groups computed in Subsection 2.1 are not exactly subgroups of some GL_n but rather semi-direct products of groups of this type with

cyclic groups, the latter corresponding to an unramified initial extension of the form $\mathbb{F}_q(x)/\mathbb{F}_p(x)$. This phenomenon is actually a general fact about splitting fields of series in $\mathbb{F}_p[[x]]$ and can be isolated.

Definition 2.2.4. The *residual splitting field* of an algebraic series $f(x) \in \mathbb{F}_p[[x]]$ is $L \cap \bar{\mathbb{F}}_p$, where $L \subseteq \mathbb{F}_p(x)^{\text{sep}}$ is the splitting field of $f(x)$.

Lemma 2.2.5. Let $f(x) \in \mathbb{F}_p[[x]]$ be an algebraic series and let ℓ be its residual splitting field. For any subfield k of $\bar{\mathbb{F}}_p$, we have an exact sequence

$$1 \longrightarrow \text{Gal}(f(x) \mid k(x)) \longrightarrow \text{Gal}(f(x) \mid \mathbb{F}_p(x)) \longrightarrow \text{Gal}(k \cap \ell / \mathbb{F}_p) \longrightarrow 1. \quad (2.2.1)$$

Proof. For a subfield k of $\bar{\mathbb{F}}_p$, we let $S_k \subseteq \mathbb{F}_p(x)^{\text{sep}}$ be the splitting field of $f(x)$ over $k(x)$. By definition, $\text{Gal}(f(x) \mid k(x))$ is then the Galois group of S_k over $k(x)$. For convenience, we also set $S := S_{\bar{\mathbb{F}}_p}$.

We consider the field $\mathbb{F}_p(x)[f]$. It is a subfield of $\mathbb{F}_p((x))$ and so it is linearly disjoint from k . As a consequence, the minimal polynomial of $f(x)$ over $\mathbb{F}_p(x)$ remains irreducible over $k(x)$. Therefore, all the Galois conjugates of $f(x)$ over $\mathbb{F}_p(x)$ are also Galois conjugates over $k(x)$. It follows that S_k is the compositum of S and $k(x)$, *i.e.*, $S_k = S \cdot k(x)$ as subfields of $\mathbb{F}_p(x)^{\text{sep}}$. Noticing moreover that $S \cap k(x) = (k \cap \ell)(x)$, the exact sequence (2.2.1) follows from classical Galois theory. \square

It follows from Lemma 2.2.5 that $\text{Gal}(f(x) \mid k(x))$ is independent of k as soon as k contains the residual splitting field of $f(x)$. This is the part of the Galois group we will be mostly interested in and which is depicted by our conjecture.

Conjecture 2.2.6. Let $f(x) \in \mathbb{Q}[[x]]$ be a D -finite series and let n be the minimal order of a differential operator that annihilates $f(x)$.

Then, there exist a number field K and a family (G_1, \dots, G_t) of subgroups of $\text{GL}_n(K)$ such that the following holds: for almost all rational prime p for which $f(x) \bmod p$ is well defined and algebraic over $\mathbb{F}_p(x)$, and for any prime \mathfrak{p} of K above p , there exists an index $i \in \{1, \dots, t\}$ such that

- (a) the residual splitting field of $f(x) \bmod p$ is contained in $k_{\mathfrak{p}}$, and
- (b) there exists an (abstract) isomorphism of groups

$$\text{Gal}(f(x) \mid k_{\mathfrak{p}}(x)) \simeq \text{image}(G_i \cap \text{GL}_n(\mathcal{O}_{(\mathfrak{p})}) \rightarrow \text{GL}_n(k_{\mathfrak{p}})),$$

where, in what precedes, $\mathcal{O}_{(\mathfrak{p})}$ denotes the localization of the ring of integers of K at \mathfrak{p} and $k_{\mathfrak{p}}$ is the residue field of K at \mathfrak{p} .

We briefly comment Conjecture 2.2.6 on several important points.

First, we remark that the assertion (a) above indicates that the Galois group $\text{Gal}(f(x) \mid k_{\mathfrak{p}}(x))$ has attained the limit, in the sense that it is equal to $\text{Gal}(f(x) \mid k(x))$ for any extension k of $k_{\mathfrak{p}}$ sitting inside $\bar{\mathbb{F}}_p$. We deduce from this observation that, if Conjecture 2.2.6 holds with the number field K , then it holds as well for any finite extension K' of K with the same family of groups (G_1, \dots, G_t) .

Second, we underline that the n in $\text{GL}_n(K)$, *i.e.*, the size of matrices, is expected to be controlled by the order of a differential operator \mathcal{L} with $\mathcal{L}(f(x)) = 0$. In fact, more is expected: for a given prime p , we actually believe that $\text{Gal}(f(x) \mid k_{\mathfrak{p}}(x))$ embeds into $\text{GL}_{n_p}(k_{\mathfrak{p}})$ where n_p is the $\mathbb{F}_p(x^p)$ -dimension of the space of solutions of $\mathcal{L} \bmod p$ (observe that $n_p \leq n$). We will come

back to these dimension bounds and give more evidences and arguments supporting them in Subsection 2.3.

Finally, we mention that it is still unclear to us what could be the (minimal) number field K in general, although we expect it to be somehow related to the differential Galois group (or maybe the monodromy group) of the minimal differential equation satisfied by $f(x)$. Again, we will give more evidences supporting this hope in Subsection 2.3.

Back to the examples. We now come back to the examples of Subsection 2.1 and show that Conjecture 2.2.6 perfectly fits with all of them.

In Example 2.1.1, the part of the Galois group that the conjecture is concerned with is the factor $\mathbb{Z}/d\mathbb{Z}$, which is always present regardless of the choice of the prime p . Since this factor corresponds to the Galois group over $\mathbb{F}_p(x)(\zeta_d)$, the natural choice for the number field K is the cyclotomic extension $K = \mathbb{Q}(\zeta_d)$. For any prime \mathfrak{p} of K , we have $\text{Gal}(f(x) \mid k_{\mathfrak{p}}(x)) \simeq \mathbb{Z}/d\mathbb{Z}$ and we can simply take $t = 1$ and $G_1 = \mu_d(K) \subseteq \text{GL}_1(K)$.

In Example 2.1.2, there is nothing to comment on, since $f(x) \bmod p$ is never algebraic.

In Example 2.1.3, we can simply take $t = 1$ and $G = \mathbb{Q}^\times = \text{GL}_1(\mathbb{Q})$.

In Example 2.1.4, one option is to take $t = 2$, as well as $G_1 = \text{GL}_1(\mathbb{Q})^\square$, and $G_2 = \text{GL}_1(\mathbb{Q})$: when $p \equiv 1 \pmod{4}$, we choose the index $i = 1$ whereas, when $p \equiv 3 \pmod{4}$, we choose $i = 2$ (and we choose either $i = 1$ or $i = 2$ when $p = 2$). It is however a nice observation that the Galois groups can actually be uniformized by a unique subgroup $G \subseteq \text{GL}_1(\mathbb{Q})$, namely

$$G := \text{GL}_1(\mathbb{Q})^\square \cdot \{\pm 1\} \subseteq \text{GL}_1(\mathbb{Q}).$$

Indeed, one checks that G reduces modulo p to $\text{GL}_1(\mathbb{F}_p)^\square \cdot \{\pm 1\}$ and, now, we remember that -1 is a square modulo p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.

The Apéry series $f(x)$ of Example 2.1.5 is quite similar to what precedes: either, we can take $G_1 = \text{GL}_1(\mathbb{Q})^\square$ and $G_2 = \text{GL}_1(\mathbb{Q})$ or we can pick just one group which is

$$G := \text{GL}_1(\mathbb{Q})^\square \cdot \langle -6 \rangle \subseteq \text{GL}_1(\mathbb{Q}).$$

Indeed, it follows from the law of quadratic reciprocity that -6 is a square modulo a prime number $p > 3$ if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$.

For the series $g(x)$ and $h(x)$, we observe that the relevant part of $\text{Gal}(g(x) \mid \mathbb{F}_p(x)) \simeq \text{Gal}(h(x) \mid \mathbb{F}_p(x))$ is, in some sense, the “square root” of $\text{Gal}(f(x) \mid \mathbb{F}_p(x))$. This observation leads us to consider the number field $K = \mathbb{Q}(\mathbf{i}\sqrt{6})$ together with the group

$$G := \text{GL}_1(\mathbb{Q}) \cdot \langle \mathbf{i}\sqrt{6} \rangle \subseteq \text{GL}_1(K).$$

When p is 1, 5, 7 or 11 modulo 24, there are two places \mathfrak{p}_1 and \mathfrak{p}_2 above p with residue field \mathbb{F}_p . Moreover, in this case, the reduction of $\mathbf{i}\sqrt{6}$ in the residue field lies obviously in \mathbb{F}_p , and so

$$\text{image}(G \cap \text{GL}_1(\mathcal{O}_{(\mathfrak{p}_i)}) \rightarrow \text{GL}_1(\mathbb{F}_p)) = \text{GL}_1(\mathbb{F}_p) = \mathbb{F}_p^\times.$$

On the contrary, when $p \equiv 13, 17, 19, 23 \pmod{24}$, there is only one place \mathfrak{p} above p with residue field \mathbb{F}_{p^2} and we find

$$\text{image}(G \cap \text{GL}_1(\mathcal{O}_{(\mathfrak{p})}) \rightarrow \text{GL}_1(\mathbb{F}_{p^2})) = \sqrt{\mathbb{F}_{p^2}^\times},$$

which is also the Galois group of $g(x)$ (resp. $h(x)$) over $\mathbb{F}_{p^2}(x)$.

In Example 2.1.6 finally, getting inspired by what precedes, we are looking for a number field for which the splitting properties of a rational prime p depends on its congruence class modulo 9.

A natural candidate is the cyclotomic extension $K = \mathbb{Q}(\zeta_9)$. Regarding the groups, one checks that we can take

$$\begin{aligned} G_1 &:= \mathrm{GL}_1(K) \quad (\text{works for } p \equiv 2 \pmod{3}), \\ G_2 &:= \mathrm{GL}_2(K) \quad (\text{works for } p \equiv 1 \pmod{3}). \end{aligned}$$

Remark 2.2.7. In the Conjecture 2.2.6 we consider prime numbers for which $f(x) \bmod p$ is well-defined and algebraic, without considering which prime numbers satisfy this condition. In a refined version, Conjecture 2.2.11 we ask for some structure of this set of prime numbers. Here, we mention one important case related to an old conjecture of Christol. A power series $f(x) \in \mathbb{Q}[[x]]$ is said to be *globally bounded*, if there is $a \in \mathbb{Z}$ such that $f(ax) - f(0) \in \mathbb{Z}[[x]]$. In particular, in that case $f(x)$ can be reduced modulo almost all primes p , possibly with the exceptions of the primes dividing a and the denominator of $f(0)$. Christol's conjecture [Chr86b] states that every D-finite power series that is globally bounded, is the diagonal of a multivariate rational function. By Fursteberg's Theorem [Fur67], $f(x) \bmod p$ then is algebraic for almost all p . Christol's conjecture is still wide open, for example, for the globally bounded function ${}_3F_2\left(\left[\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right], \left[\frac{1}{3}, 1\right]; x\right)$, discussed in Subsection 2.1.6, it is not known, whether it is a diagonal [BY22, p.1085, footnote].

2.2.3 Two refinements

Although Conjecture 2.2.6 might look already rather strong and difficult, there are several points on which it remains quite vague and unprecise. The first one is that it does not say too much about the groups G_i , expect that they exist and are contained in some GL_n . However, while this fragility is certainly the most significant one, discussing it will require some categorical language and machinery. For this reason, we prefer postponing this to Subsection 2.3 and start by presenting, in this subsection, two other simpler improvements.

A Galois equivariant version. A first evident weakness of Conjecture 2.2.6 is that it does not concern the complete Galois group $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$ but only a part of it, even if it is quite large and arguably the most interesting one. This issue can be solved by adding descent data in the formulation of the conjecture as follows. We require that K/\mathbb{Q} is Galois and that each group $G_i \subseteq \mathrm{GL}_n(K)$ is stable by the Galois action. For a prime \mathfrak{p} of K , the group

$$G_{i,\mathfrak{p}} := \text{image} \left(G_i \cap \mathrm{GL}_n(\mathcal{O}_{(\mathfrak{p})}) \rightarrow \mathrm{GL}_n(k_{\mathfrak{p}}) \right) \quad (2.2.2)$$

which appears in Conjecture 2.2.6 is then stable by the natural action of $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$; indeed this action corresponds to that of the decomposition group at \mathfrak{p} which, by assumption, stabilizes G_i . We can then form the semi-direct product $G_{i,\mathfrak{p}} \rtimes \mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$ (where $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$ acts on $G_{i,\mathfrak{p}}$ through its natural action on $\mathrm{GL}_n(k_{\mathfrak{p}})$), which looks like a very good candidate to be the complete Galois group $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$. This expectation is actually a bit too naive because the factor $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$ may vary a lot with the choice of K . Instead, we propose the following formulation.

Conjecture 2.2.8. *Let $f(x) \in \mathbb{Q}[[x]]$ be a D-finite series and let n be the minimal order of a differential operator that annihilates $f(x)$.*

Then, there exist a Galois extension K/\mathbb{Q} and a family (G_1, \dots, G_t) of subgroups of $\mathrm{GL}_n(K)$ stable by the action of $\mathrm{Gal}(K/\mathbb{Q})$ such that the following holds: for almost all rational primes p for which $f(x) \bmod p$ is well defined and algebraic over $\mathbb{F}_p(x)$, and for any prime \mathfrak{p} of K above p , there exists an index $i \in \{1, \dots, t\}$ such that

- (a) *the residual splitting field of $f(x) \bmod p$ is the field $\ell_{\mathfrak{p}}$ defined as the smallest subfield of $k_{\mathfrak{p}}$ for which $G_{i,\mathfrak{p}} \subseteq \mathrm{GL}_n(\ell_{\mathfrak{p}})$.*

(b) there is an isomorphism of exact sequences:

$$\begin{array}{ccccccc}
1 & \longrightarrow & \text{Gal}(f(x) \mid k_{\mathfrak{p}}(x)) & \longrightarrow & \text{Gal}(f(x) \mid \mathbb{F}_p(x)) & \longrightarrow & \text{Gal}(\ell_{\mathfrak{p}}/\mathbb{F}_p) \longrightarrow 1 \\
& & \downarrow \sim & & \downarrow \sim & & \parallel \\
1 & \longrightarrow & G_{i,\mathfrak{p}} & \longrightarrow & G_{i,\mathfrak{p}} \times \text{Gal}(\ell_{\mathfrak{p}}/\mathbb{F}_p) & \longrightarrow & \text{Gal}(\ell_{\mathfrak{p}}/\mathbb{F}_p) \longrightarrow 1
\end{array}$$

where $G_{i,\mathfrak{p}}$ is defined by Equation (2.2.2) and the exact sequence on the top is that of Lemma 2.2.5.

Remark 2.2.9. The point (b) above is equivalent to requiring, in addition of the assertion (b) of Conjecture 2.2.6, that the exact sequence of Lemma 2.2.5 splits and that the induced action of $\text{Gal}(\ell_{\mathfrak{p}}/\mathbb{F}_p)$ on $G_{i,\mathfrak{p}}$ agrees with its natural action on $\text{GL}_n(\ell_{\mathfrak{p}})$.

Remark 2.2.10. Another interesting feature of Conjecture 2.2.8 is that it clearly highlights that all the places \mathfrak{p} above a fixed rational prime p play the same role (since they are permuted by $\text{Gal}(K/\mathbb{Q})$).

Finally, we leave it as an exercise to the reader to check that all the examples of Subsection 2.1 satisfy Conjecture 2.2.8.

Controlling the partition of primes. The second point on which we would like to add precisions to Conjecture 2.2.6 concerns the dependence of the index i , *i.e.*, the subgroup G_i we choose, with respect to p . On all the examples of Subsection 2.1, we observe that this dependence is very easy to settle: the choice of i always only depends on the congruence class of p modulo a certain fixed number. We would not expect however such a simple pattern to be repeated in full generality. Our doubts come already from the case of linear differential equation of order 1, namely

$$f'(x) + a(x) \cdot f(x) = 0.$$

More precisely, we have explained in Remark 2.1.2 that for a solution $f(x)$ of the above equation, the property to be reducible modulo p is governed by the factorization properties of $a(x) \bmod p$ which, in turn, can be read off from the decomposition of p in the splitting field L of $a(x)$ over \mathbb{Q} . This behavior is indeed controlled by congruence conditions on p when L is an abelian extension of \mathbb{Q} ; however it might be much more complicated in general.

For this reason, we prefer formulating our refined conjecture as follows.

Conjecture 2.2.11. *Let $f(x) \in \mathbb{Q}[[x]]$ be a D -finite series. Let n be the minimal degree of a differential operator that annihilates $f(x)$. Then, there exist*

- a number field K ,
- a finite Galois extension L/\mathbb{Q} ,
- two subsets $\mathcal{C}_{\text{alg}} \subseteq \mathcal{C}_{\text{red}}$ of the set of conjugacy classes of $\text{Gal}(L/\mathbb{Q})$ and
- for each $C \in \mathcal{C}_{\text{alg}}$, a subgroup $G_C \subseteq \text{GL}_n(K)$

such that, for almost all primes p , if C denotes the conjugacy class containing the Frobenius morphism at p in $\text{Gal}(L/\mathbb{Q})$, we have:

- (1) $C \in \mathcal{C}_{\text{red}}$ if and only if $f(x) \in \mathbb{Z}_{(p)}[[x]]$,
- (2) $C \in \mathcal{C}_{\text{alg}}$ if and only if $f(x) \in \mathbb{Z}_{(p)}[[x]]$ and $f(x) \bmod p$ is algebraic over $\mathbb{F}_p(x)$,

(3) if $C \in \mathcal{C}_{\text{alg}}$, for any prime \mathfrak{p} in K above p , the residue field $k_{\mathfrak{p}}$ contains the residual splitting field of $f(x) \bmod p$ and there is an isomorphism

$$\text{Gal}(f(x) \mid k_{\mathfrak{p}}(x)) \simeq \text{image}(G_C \cap \text{GL}_n(\mathcal{O}_{(\mathfrak{p})}) \rightarrow \text{GL}_n(k_{\mathfrak{p}})).$$

We underline that Conjecture 2.2.11 also includes a criterion for recognizing whether $f(x)$ can be reduced modulo p and, when this is the case, whether the reduction is algebraic or not. This part was not covered in the previous formulations.

On a different note, it is obvious that if Conjecture 2.2.11 holds with a number field L and it holds for any extension L' of L (with L'/Q Galois) as well. Since a similar property also holds for the number field K , one can safely assume that $K = L$ in Conjecture 2.2.11. However, it looks important to us to make the distinction between K and L as they seem to play different roles. For instance, in many examples considered in Subsection 2.1, taking simply $L = \mathbb{Q}$ (which corresponding to having just one group G_i) is possible while it is often necessary to work with a nontrivial number field K .

Finally, we notice that the two refinements provided by Conjectures 2.2.8 and 2.2.11 are somehow independent and can be combined.

2.3 The language of differential modules and Frobenius modules

In this subsection, following standard ideas which go back to Dwork and Christol (see in particular [Chr86a]), we reinterpret the main protagonists we have encountered so far using the more powerful language of differential modules and Frobenius modules and use it to gain height on Conjecture 2.2.6. This will help us to better understand what could be the mysterious groups G_i by connecting them to the differential Galois group of the underlying differential equation.

2.3.1 Different types of modules

Differential modules. We begin with linear differential equations. It is a standard fact that the categorical shadow of these equations is the notion of differential modules, whose definition is recalled below.

Definition 2.3.1. Let K be a field equipped with a derivation $\partial : K \rightarrow K$. A *differential module* (or a *module with connection*) over (K, ∂) is a finite dimensional K -vector space M , together with an additive map ∇ satisfying

$$\forall \lambda \in K, \forall m \in M, \quad \nabla(\lambda m) = \partial(\lambda)m + \lambda \nabla(m).$$

We write Mod_K^{∇} for the category of differential modules over (K, ∂) .

To any differential equation of the form

$$\partial^r(f) + a_{r-1}\partial^{(r-1)}(f) + \cdots + a_1\partial(f) + a_0f = 0 \quad (a_i \in K) \quad (2.3.1)$$

we attach the differential module $M = Ke_0 \oplus \cdots \oplus Ke_{r-1}$ with connection ∇ defined by

$$\begin{aligned} \nabla(e_i) &= e_{i+1} & \text{if } 0 \leq i \leq r-2, \\ \nabla(e_{r-1}) &= -(a_0e_0 + \cdots + a_{r-1}e_{r-1}). \end{aligned}$$

The map $f \mapsto \sum_{i=0}^{r-1} \partial^i(f)e_i$ induces a bijection between the space of solutions in K of the differential equation (2.3.1) with the space $M^{\nabla=0}$ of *horizontal vectors*, that are, by definition, vectors m such that $\nabla(m) = 0$.

This framework also allows for looking at solutions in extensions. More precisely, let L be an extension of K over which the derivation ∂ extends. Given a differential module M over K , one can form the tensor product $L \otimes_K M$ and endow it with a connection defined by

$$\nabla(\lambda \otimes m) = \partial(\lambda) \otimes m + \lambda \otimes \nabla(m) \quad (\lambda \in L, m \in M).$$

The solutions of M over L are then defined as the space of horizontal vectors of $L \otimes_K M$, that is $(L \otimes_K M)^{\nabla=0}$.

Frobenius modules. For the general purpose of this article, we recall from the introduction (see Equation (1.1)) that we are mostly interested in algebraic relations of the form

$$Y^{p^n} + c_{n+1}Y^{p^{n+1}} + \cdots + c_1Y^p + c_0Y = 0 \quad (2.3.2)$$

where Y is the unknown and the coefficients c_i lie in some field of characteristic p which, in our case of interest, is $\mathbb{F}_p(x)$ or an extension of the form $\ell(x)$ where ℓ/\mathbb{F}_p is a field extension. Fortunately, this type of equations can be handled very similarly to what we have presented above for linear differential equations.

In the algebraic situation, the relevant objects are the so-called Frobenius modules that we define now.

Definition 2.3.2. Let R be a ring equipped with an endomorphism $\varphi : R \rightarrow R$. A *Frobenius module* over (R, φ) is a finitely generated projective R -module M equipped with an additive map $\varphi_M : M \rightarrow M$ such that

$$\forall \lambda \in R, \forall m \in M, \quad \varphi_M(\lambda m) = \varphi(\lambda) \cdot \varphi_M(m).$$

We let Mod_R^φ denote the category of Frobenius modules over (R, φ) .

Notation 2.3.3. When the ground ring R has characteristic p and $\varphi : R \rightarrow R$ is the map $x \mapsto x^q$ (where q is a power of p), we write Mod_R^q for Mod_R^φ .

The relationship between Frobenius equations and Frobenius modules is realized as follows. Starting from Equation (2.3.2) with $c_i \in R$, we define the Frobenius module $M = Re_0 \oplus \cdots \oplus Re_{r-1}$ (where R is equipped with its natural Frobenius) with

$$\begin{aligned} \varphi_M(e_i) &= e_{i+1} & \text{if } 0 \leq i \leq r-2, \\ \varphi_M(e_{r-1}) &= -(c_0e_0 + \cdots + c_{r-1}e_{r-1}). \end{aligned}$$

The solutions of Equation (2.3.2) then correspond to vectors $m \in M$ such $\varphi_M(m) = m$ via the map $y \mapsto \sum_{i=0}^{r-1} y^{p^i} e_i$.

Galois representations. The last notion we would like to encapsulate in our new language is, of course, that of Galois groups. For this, given a field K , we write G_K for its absolute Galois group, *i.e.*, $G_K := \text{Gal}(K^{\text{sep}}/K)$. Given an auxiliary field E , we introduce the category $\text{Rep}_E(G_K)$ of all E -linear finite dimensional representations of G_K .

The connection with the Galois groups we used to consider earlier is as follows. Assume that K contains E and let then x be an element in the separable closure K^{sep} of K . We consider its Galois conjugate $x_1 = x, x_2, \dots, x_N \in K^{\text{sep}}$ and the E -vector space V they generate. Clearly V is stable by the action of G_K . Hence, it is a E -linear representation of G_K , *i.e.*, an object in the category $\text{Rep}_E(G_K)$. Besides, if $\rho : G_K \rightarrow \text{GL}(V)$ is the morphism defining the representation, one checks that $\text{Gal}(x | K) \simeq \text{im } \rho$.

2.3.2 Katz' functor

Katz' functor connects Frobenius modules with Galois representations; in some sense, it is the categorical realization of the operation that takes an algebraic equation of the form (2.3.2) and produces the Galois group of one of its solutions.

Concretely, it is defined as follows. We pick a field K of characteristic p , together with a finite extension \mathbb{F}_q of \mathbb{F}_p . We then define

$$\begin{aligned} \mathbf{V} : \text{Mod}_K^q &\longrightarrow \text{Rep}_{\mathbb{F}_q}(G_K) \\ M &\longmapsto (K^{\text{sep}} \otimes_K M)^{\varphi=1} \end{aligned} \quad (2.3.3)$$

where we let φ act on $K^{\text{sep}} \otimes_K M$ by $\lambda \otimes m \mapsto \lambda^q \otimes \varphi_M(m)$ and where the notation “ $\varphi = 1$ ” means that we consider the subset of elements that are fixed by φ . When M comes from an equation of the form (2.3.2) (and thus $q = p$), it follows directly from the definition that the representation $\mathbf{V}(M)$ is the \mathbb{F}_p -vector space of the solutions in K^{sep} equipped with the standard Galois action.

To study Katz' functor, it is convenient to introduce the following definition.

Definition 2.3.4. Let R be a ring equipped with an endomorphism $\varphi : R \rightarrow R$. We say that a Frobenius module $M \in \text{Mod}_R^\varphi$ is *étale* when the image of φ_M spans M .

We write $\text{Mod}_K^{\varphi, \text{ét}}$ for the subcategory of Mod_K^φ consisting of étale Frobenius modules. Moreover, when φ is the map $x \mapsto x^q$, we write $\text{Mod}_K^{q, \text{ét}}$ for $\text{Mod}_K^{\varphi, \text{ét}}$ (see also Notation 2.3.3).

Theorem 2.3.5 (Katz). *Let K be a field of characteristic p and let q be a power of p . The functor \mathbf{V} induces an equivalence of categories $\text{Mod}_K^{q, \text{ét}} \xrightarrow{\sim} \text{Rep}_{\mathbb{F}_q}(G_K)$. Moreover, it preserves the dimension in the sense that, for all $M \in \text{Mod}_K^{q, \text{ét}}$, we have*

$$\dim_K M = \dim_{\mathbb{F}_q} \mathbf{V}(M).$$

Proof. See [Kat73, Proposition 4.1.1]. □

Remark 2.3.6. There exists an explicit formula for the inverse functor \mathbf{M} of \mathbf{V} : if V is a \mathbb{F}_q -linear representation of G_K , its corresponding étale Frobenius module is $\mathbf{M}(V) := (K^{\text{sep}} \otimes_K V)^{G_K}$ where G_K acts diagonally on the tensor product $K^{\text{sep}} \otimes_K V$.

Beyond Katz' theorem, it will be also important for our purpose to study the action of Katz' functor on nonétale Frobenius modules. In this perspective, we set the following definition.

Definition 2.3.7. Let K be a field equipped with a ring endomorphism $\varphi : K \rightarrow K$ and let M be a Frobenius module over (K, φ) . The *étale part* of M is defined as

$$M^{\text{ét}} := \bigcap_{k \geq 0} \langle \varphi_M^k(M) \rangle_K$$

where the notation $\langle \cdot \rangle_K$ stands for the K -span.

It is straightforward to check that $M^{\text{ét}}$ is stable by φ_M , *i.e.*, it is again a Frobenius module, and that it is étale. In other words, the construction $M \mapsto M^{\text{ét}}$ defines a functor $\text{Mod}_K^\varphi \rightarrow \text{Mod}_K^{\varphi, \text{ét}}$.

Lemma 2.3.8. *We assume that K has characteristic p and that q is a power of p . Then, for all $M \in \text{Mod}_K^q$, we have $\mathbf{V}(M) = \mathbf{V}(M^{\text{ét}})$.*

Proof. We form the quotient $M/M^{\text{ét}}$ which inherits an action of φ_M and thus is an object in the category Mod_K^φ . Besides, it follows readily from the definition that φ_M acts nilpotently on $M/M^{\text{ét}}$. Therefore, it also acts nilpotently on $K^{\text{sep}} \otimes_K M/M^{\text{ét}}$, from which follows that $\mathbf{V}(M/M^{\text{ét}}) = 0$. We now consider the exact sequence

$$0 \longrightarrow M^{\text{ét}} \longrightarrow M \longrightarrow M/M^{\text{ét}} \longrightarrow 0$$

which remains exact after tensoring by K^{sep} . Taking then the fixed points under φ (which is a left exact functor), we end up with

$$0 \longrightarrow \mathbf{V}(M^{\text{ét}}) \longrightarrow \mathbf{V}(M) \longrightarrow \mathbf{V}(M/M^{\text{ét}}) = 0.$$

The lemma follows. □

Remark 2.3.9. Lemma 2.3.8 tells us that $M^{\text{ét}}$ is the étale Frobenius module which corresponds to the Galois representation $\mathbf{V}(M)$. With the notation of Remark 2.3.6, we then have $M^{\text{ét}} = \mathbf{M}(\mathbf{V}(M))$.

2.3.3 Frobenius structures on differential modules

The relationship between differential modules and Frobenius modules is far less concrete, but it can nevertheless be approached through the notion of Frobenius structures. Basically, the idea is to equip a differential module M with an extra structure which will eventually define a Frobenius module after reduction modulo p .

In order to define it properly, we cannot continue working over $\mathbb{Q}(x)$ but need to move over the p -adics. Precisely, we define the field E_p as the completion of $\mathbb{Q}(x)$ for the p -adic Gauss norm (defined as the sup norm on the p -adic unit disc); it is the so-called field of *p -adic analytic elements*. It is equipped with the derivation $\frac{d}{dx}$ and a Frobenius map $\varphi : E_p \rightarrow E_p$ which comes from the change of variables $x \mapsto x^p$.

Definition 2.3.10. Let (M_1, ∇_1) and (M_2, ∇_2) be two differential modules over E_p . A *Frobenius morphism* is a φ -semilinear map $\Phi : M_1 \rightarrow M_2$ such that $\nabla_2 \circ \Phi = px^{p-1} \cdot \Phi \circ \nabla_1$.

It is instructive to understand what the effect of a Frobenius morphism at the level of solutions is. The commutation relation of Definition 2.3.10 ensures that a Frobenius morphism $\Phi : M_1 \rightarrow M_2$ induces a \mathbb{Q}_p -linear mapping on horizontal vectors $\Phi : M_1^{\nabla=0} \rightarrow M_2^{\nabla=0}$. If we equip M_1 and M_2 with distinguished bases and if $\text{Mat}(\Phi)$ denotes the matrix of Φ in those bases, we deduce that any solution $(f_1(x), \dots, f_n(x))$ of M_1 produces a solution of M_2 *via* the formula

$$(\varphi(f_1(x)), \dots, \varphi(f_n(x))) \cdot \text{Mat}(\Phi) = (f_1(x^p), \dots, f_n(x^p)) \cdot \text{Mat}(\Phi).$$

If we assume in addition that $\Phi : M_1 \rightarrow M_2$ is an isomorphism, then any solution of M_2 can be (uniquely) written in this way. Frobenius morphisms then appear as a general machinery that permits to interpret the images under φ of a solution of a given differential equation as linear combinations of the solutions of another differential equation and *vice versa* when Φ is an isomorphism. Phrased in this way, we understand that they could provide a powerful tool to find the algebraic relations we are looking for (remember that $f(x^p) = f(x)^p$ after reduction modulo p).

In order to fully take advantage of this observation, it is convenient to use the concept of *preimages under the Frobenius*. To avoid unnecessary complications, we assume from now on that we are given a D -finite series $f(x) \in \mathbb{Z}_{(p)}[[x]]$ and that M is the differential module associated to the linear differential equation over E_p of minimal order satisfied by $f(x)$. A theorem of Christol

(see [Ked10, Theorem 10.4.2]) then implies that M admits a preimage under the Frobenius, which means that there exists a Frobenius *isomorphism* $M^{(-1)} \rightarrow M$ where $M^{(-1)}$ is another differential module. Even better, one can apply Christol's theorem repeatedly and get an infinite sequence of Frobenius isomorphisms

$$\dots \longrightarrow M^{(-3)} \xrightarrow{\sim} M^{(-2)} \xrightarrow{\sim} M^{(-1)} \xrightarrow{\sim} M.$$

We now come to an alternative: either the sequence of $M^{(-i)}$ is periodic or it is not. In the first case, *i.e.*, when there exists a positive integer h such that $M^{(-h)}$ is isomorphic to M as a differential module, we say that M admits a *strong Frobenius structure* (of period h). When this occurs, the composite

$$M \simeq M^{(-h)} \xrightarrow{\sim} \dots \xrightarrow{\sim} M^{(-1)} \xrightarrow{\sim} M.$$

defines a structure of Frobenius modules on M for the twisting morphism φ^h . This makes the connection we were looking for.

On the contrary, when M does not admit a strong Frobenius structure, the above construction fails; however, in this case, we suspect that $f(x) \bmod p$ is not algebraic.

Some examples. It is quite interesting to revisit some examples of Subsection 2.1 in light of what precedes. Let us start with Example 2.1.2. Here $f(x) = \exp(\arctan(x))$ and we recall that, whenever $p \equiv 1 \pmod{4}$, we had obtained the following alternative formula for $f(x)$ as a p -adic series:

$$f(x) = (1 + ix)^{-i/2} \cdot (1 - ix)^{i/2} \in \mathbb{Z}_p[[x]]$$

where $i \in \mathbb{Z}_p$ is a square root of -1 . We recall that we also decomposed the exponents $\pm i/2$ in base p as follows:

$$-\frac{i}{2} = a_0 + pa_1 + p^2a_2 + \dots \quad \text{and} \quad \frac{i}{2} = b_0 + pb_1 + p^2b_2 + \dots$$

It turns out that this decomposition actually reflects the successive preimages by Frobenius of the underlying differential module. Indeed, setting $u_1 := \frac{-i/2 - a_0}{p} = a_1 + pa_2 + \dots$, we can rewrite

$$(1 + ix)^{-i/2} = (1 + ix)^{a_0} \left(\frac{(1 + ix)^p}{1 + ix^p} \right)^{u_1} (1 + ix^p)^{u_1}.$$

Now we observe that the two first factors of the right hand side lie in E_p : it is obvious for the first one, which is a polynomial, and it holds true for the second one as well because $\frac{(1+ix)^p}{1+ix^p}$ is a rational function, which is congruent to 1 modulo p . Proceeding similarly for the factor $(1 - ix)^{i/2}$, we end up with a factorization of the form $f(x) = g_0(x)f_1(x^p)$ where $g_0(x) \in E_p$ and

$$f_1(x) = (1 + ix)^{u_1} \cdot (1 - ix)^{v_1}$$

with $v_1 := \frac{i/2 - b_0}{p} = b_1 + pb_2 + \dots$. Moreover, a simple computation shows that the function $f_1(x)$ is a solution of the linear differential equation

$$y'(x) = \frac{i(u_1 - v_1) + (u_1 + v_1)x}{1 + x^2} \cdot y(x).$$

It is the preimage under the Frobenius of our initial differential equation for $f(x)$. Repeating this argument, we find that the successive preimages under the Frobenius are the differential equations

$$y'(x) = \frac{i(u_k - v_k) + (u_k + v_k)x}{1 + x^2} \cdot y(x)$$

$$\begin{array}{c}
\text{Mod}_{\mathbb{Q}(x)}^{\nabla} \ni M \\
\downarrow \textcircled{1}: \text{Factorization over } E_p \\
\text{Mod}_{E_p}^{\nabla} \ni M_p \\
\vdots \textcircled{2}: \text{Frobenius structure} \\
\text{Mod}_{E_p}^{\varphi^h} \ni M_p \\
\vdots \textcircled{3}: \text{Finding a lattice} \\
\text{Mod}_{E_p^{\circ}}^{\varphi^h, \acute{e}t} \ni M_p^{\circ} \\
\downarrow \textcircled{4}: \text{Reduction modulo } p \\
\text{Mod}_{\mathbb{F}_p(x)}^{q, \acute{e}t} \ni \overline{M}_p \\
\downarrow \textcircled{5}: \text{Katz' functor} \\
\text{Rep}_{\mathbb{F}_q(x)}(G_{\mathbb{F}_q(x)}) \ni V_p
\end{array}$$

FIGURE 1: From differential equations in characteristic 0 to Galois groups in characteristic p

with $u_k = a_k + pa_{k+1} + p^2a_{k+2} + \dots$ and $v_k = b_k + pb_{k+1} + p^2b_{k+2} + \dots$. The nonperiodicity of the sequences $(a_k)_{k \geq 0}$ and $(b_k)_{k \geq 0}$, or equivalently that of the sequences $(u_k)_{k \geq 0}$ and $(v_k)_{k \geq 0}$, now implies that the sequence of preimages under the Frobenius is not periodic as well. This conclusion is perfectly in line with the fact that $f(x) \bmod p$ is not algebraic.

Another interesting example to consider is Example 2.1.5 with the Apéry series. Here, we recall that we had defined two functions $g(x)$ and $h(x)$ whose reductions modulo p satisfy interlaced algebraic relations (see Equations (2.1.7)–(2.1.10)). Those equations suggest that the differential equations that $g(x)$ and $h(x)$ satisfy are fixed by the Frobenius when $p \equiv 1, 5, 7, 11 \pmod{24}$ and exchanged by the Frobenius when $p \equiv 13, 17, 19, 23 \pmod{24}$.

Similar patterns will often occur in Section 3, when we will study hypergeometric series.

2.3.4 The long road from $\text{Mod}_{\mathbb{Q}(x)}^{\nabla}$ to $\text{Rep}_{\mathbb{F}_q(x)}(G_{\mathbb{F}_q(x)})$

All the previous constructions provide a path for going from modules with connections over $\mathbb{Q}(x)$ (which encode the differential equation satisfied by $f(x)$) to Galois representations of the absolute Galois group $G_{\mathbb{F}_q(x)}$ of $\mathbb{F}_q(x)$ (which encodes the Galois group of $f(x) \bmod p$). It consists in the following steps.

- ① (Factorization over E_p) We “ p -minimize” the differential equation we have for $f(x)$, meaning that we replace it by the differential equation *over* E_p of minimal order which is satisfied by $f(x)$; we emphasize that this operation may result in a drop of order even if our initial differential equation was already minimal over $\mathbb{Q}(x)$. At the level of modules, this consists in replacing M by a submodule $M_p \subseteq E_p \otimes_{\mathbb{Q}(x)} M$.
- ② (Frobenius structure) Following the discussion of Subsection 2.3.3, we equip M_p with a Frobenius structure $\Phi_h : M_p \rightarrow M_p$, obtaining this way a Frobenius module over E_p for the twisting morphism φ^h (where h is the period); we underline that this operation may fail if the sequence of the Frobenius preimages of M_p is not periodic.

- ③ (Finding a lattice) In order to reduce modulo p afterwards, we need to find an integral structure inside M_p . Let E_p° denote the valuation ring of E_p , that is the subring of E_p consisting of elements of nonnegative valuation. We select a finitely generated E_p° -submodule M_p° of M_p having the following properties: it generates M_p over E_p , it is stable by Φ_h and it defines an étale Frobenius module over E_p° . Such a module may actually not exist; if it does not, we allow ourselves to change the Frobenius structure, *i.e.*, to replace Φ_h by $\Phi_h \circ \iota$ where ι is a E_p -linear automorphism of M_p commuting with the connection. If even after this relaxation, we are still not able to find a suitable module M_p° , we agree that this step has failed.
- ④ (Reduction modulo p) We reduce M_p° modulo p , *i.e.*, we set $\overline{M}_p := M_p^\circ / pM_p^\circ$. It is an étale Frobenius module over $\mathbb{F}_p(x)$ for the twisting morphism $f \mapsto f^q$ with $q = p^h$.
- ⑤ (Katz' functor) We finally apply Katz' functor to get a representation of $G_{\mathbb{F}_q(x)} := \text{Gal}(\mathbb{F}_q(x)^{\text{sep}}/\mathbb{F}_q(x))$. Some precaution should be taken here because Katz' theorem requires that the base field of the Frobenius module contains \mathbb{F}_q , which is not the case in our setting. We then first extend scalar to $\mathbb{F}_q(x)$, *i.e.*, we define

$$V_p := \mathbf{V}(\mathbb{F}_q(x) \otimes_{\mathbb{F}_p(x)} \overline{M}_p) = (\mathbb{F}_q(x)^{\text{sep}} \otimes_{\mathbb{F}_p(x)} \overline{M}_p)^{\varphi=1}.$$

All this process is summarized in Figure 1. Dashed arrows correspond to steps that may fail. However, if a failure is encountered at some point, our feeling is that $f(x) \bmod p$ cannot be algebraic. On the contrary, when all operations succeed, it is known that $f(x) \bmod p$ is algebraic [Var21, Theorem 2.6]. What we expect actually is that $f(x) \bmod p$ is somehow “contained”, together with its conjugates, in the Galois representation V_p which is produced at the end of the process. More precisely, if we let $\rho_p : G_{\mathbb{F}_q(x)} \rightarrow \text{GL}(V_p)$ be the corresponding group morphism, we expect the Galois group $\text{Gal}(f(x) \mid \mathbb{F}_q(x))$ to be isomorphic to a quotient of the image of ρ_p .

Remark 2.3.11. It worths noticing that Theorem 2.6 of [Var21] only requires the existence of a strong Frobenius structure, and not that of a lattice. This suggests that Step ③ in our construction could never fail.

2.3.5 Connecting Galois groups: insights towards our conjectures

The Tannakian language provides efficient tools to define Galois groups at each step of our constructions and, to some extent, to follow them throughout the whole process. We refer to [DM82] for an exposition of the Tannakian theory. Here, we just recall that the Tannakian formalism attaches a “Galois group” to any object in a Tannakian category. Its definition goes through the notion of constructions. Given T in a Tannakian category \mathcal{T} , a *construction* from T is by definition a subquotient of an object of the form

$$C := T^{\otimes n_1} \oplus T^{\otimes n_2} \oplus \dots \oplus T^{\otimes n_t} \quad (n_i \in \mathbb{Z})$$

where, when n is negative, $T^{\otimes n}$ is understood as the dual of $T^{\otimes(-n)}$. The Galois group $\text{Gal}_{\mathcal{T}}(T)$ is then the group of linear automorphisms $\sigma : T \rightarrow T$ satisfying the following condition: for any C as above and any subobject $S \subseteq C$, the natural extension of σ to C stabilizes S . One proves that $\text{Gal}_{\mathcal{T}}(T)$ is an *algebraic* subgroup of $\text{GL}(T)$.

We now analyze the effect on Galois groups of each step of Figure 1 in light of what precedes. Step ① has already quite a nontrivial impact. To describe it properly, it is convenient to split it

into two parts: firstly, we extend scalars to E_p and secondly, we minimize the differential equation. Regarding scalar extension, it follows from the definition that we have an inclusion

$$\mathrm{Gal}_{\mathrm{Mod}_{E_p}^{\nabla}}(E_p \otimes_{\mathbb{Q}(x)} M) \subseteq \mathrm{Gal}_{\mathrm{Mod}_{\mathbb{Q}(x)}^{\nabla}}(M).$$

Besides, if $E_p \otimes_{\mathbb{Q}(x)} M$ admits a submodule M' , any element of the Galois group of $E_p \otimes_{\mathbb{Q}(x)} M$ necessarily stabilizes M' . Applying this remark with $M' = M_p$, we obtain a group morphism

$$\varpi : \mathrm{Gal}_{\mathrm{Mod}_{E_p}^{\nabla}}(E_p \otimes_{\mathbb{Q}(x)} M) \longrightarrow \mathrm{GL}(M_p)$$

and it follows from the Tannakian theory that the Galois group of M_p is the image of ϖ . As a summary, one can retain that $\mathrm{Gal}_{\mathrm{Mod}_{E_p}^{\nabla}}(M_p)$ appears as a subquotient of $\mathrm{Gal}_{\mathrm{Mod}_{\mathbb{Q}(x)}^{\nabla}}(M)$.

Although the steps ② and ③ seem to be the most delicate ones, their effect on the Galois groups is quite harmless. Indeed, a theorem of Matzat [Mat09a; Mat09b] shows that

$$\mathrm{Gal}_{\mathrm{Mod}_{E_p}^{\nabla}}(M_p) = \mathrm{Gal}_{\mathrm{Mod}_{E_p^{\circ}}^{q,\acute{e}t}}(M_p^{\circ})$$

as soon as M_p° is defined. More precisely, the datum of the lattice M_p° defines a prolongation to $\mathrm{Spec} \mathbb{Z}_p$ of the algebraic group $\mathrm{Gal}_{\mathrm{Mod}_{E_p}^{\nabla}}(M_p)$, which was *a priori* only defined over $\mathrm{Spec} \mathbb{Q}_p$.

Step ④ is a scalar extension and so, it has a similar effect on Galois groups as in Step ①: the Galois group of \overline{M}_p is a subgroup of the reduction modulo p of the Galois group of M_p° . Concerning Step ⑤, the same phenomenon occurs when extending scalars to $\mathbb{F}_q(x)$, and finally, applying Katz' functor is transparent at the level of Galois groups because it is an equivalence of categories.

All in all, the conclusion is that the Galois group of $f(x) \bmod p$ appears as a subquotient of a certain scalar extension of the reduction modulo p of the differential Galois group of M . This remark suggests that the groups G_i of Conjecture 2.2.6 could show up as subquotients of the K -valued points of $\mathrm{Gal}_{\mathrm{Mod}_{\mathbb{Q}(x)}^{\nabla}}(M)$. The fact that we are losing dimensions when passing from M to M_p also explains that G_i sometimes (naturally) embeds in $\mathrm{GL}_m(K)$ with $m < \dim M$.

Uniformity in p . So far, we have fixed a prime number p from the beginning and carried out all our constructions and reasonings with this particular p . In fact, the content of Conjecture 2.2.6 (and its refinements) is somehow that all of this can be achieved uniformly with respect to p , with precise control encoded by certain number fields!

Recycling the same set of ideas, one could also expect that some numerical invariants that we have encountered along the way, *e.g.*, the dimension of M_p , behave quite nicely when p varies. This leads to the two following independent questions, which sound quite interesting to us, and that we ask to the community.

Question 2.3.12. Let $f(x) \in \mathbb{Q}[[x]]$ be a D -finite series and, for all prime number p , let r_p be the minimal order of a differential equation over E_p satisfied by $f(x)$. How does r_p vary with respect to p ?

Question 2.3.13. Let M be a differential module over $\mathbb{Q}(x)$ and, for almost all prime number p , let d_p be the dimension over $\mathbb{F}_p(x^p)$ of the space of the solutions of M over $\mathbb{F}_p(x)$. By Cartier's Lemma (see [BCR24, Theorem 3.19]), d_p is also the dimension of the kernel of the p -curvature of M . How does d_p vary with respect to p ?

If the exponents at 0 of the minimal differential equation of a D -finite series $f(x) \in \mathbb{Q}[[x]]$ are all 0, the function $f(x)$ is said to have *maximal unipotent monodromy (MUM)* and one proves that

$r_p = d_p = 1$ for almost all p . This answers Questions 2.3.12 and 2.3.13 in this case. In Section 3 (see Theorem 3.1.17), we will study the case where M is the differential module corresponding to an hypergeometric operator \mathcal{H} and show, in this situation, that d_p depends only on the congruence class of p modulo a common denominator of the parameters of \mathcal{H} .

3 Hypergeometric series and their reductions modulo p

The hypergeometric differential operator is defined as

$$\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}) = -x \prod_{i=1}^n (\vartheta + \alpha_i) + \vartheta \prod_{j=1}^m (\vartheta + \beta_j - 1) \quad \left(\vartheta := x \cdot \frac{d}{dx} \right) \quad (3.0.1)$$

where n and m are positive integers, $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in (\mathbb{Q} \setminus (-\mathbb{N}))^n$ and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_m) \in (\mathbb{Q} \setminus (-\mathbb{N}))^m$. The solutions of the equation $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})y = 0$ over the rational numbers can be expressed in terms of hypergeometric series

$${}_nF_m(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) := \sum_{k=0}^{\infty} h(\boldsymbol{\alpha}, \boldsymbol{\beta}; k) x^k \in \mathbb{Q}[[x]], \quad (3.0.2)$$

with

$$h(\boldsymbol{\alpha}, \boldsymbol{\beta}; k) := \frac{(\alpha_1)_k \cdots (\alpha_n)_k}{(\beta_1)_k \cdots (\beta_m)_k} \cdot \frac{1}{k!} \in \mathbb{Q},$$

where $(\gamma)_k := \gamma \cdot (\gamma + 1) \cdots (\gamma + k - 1)$ denotes the rising factorial.

In the following we will restrict to the case $m = n - 1$. Moreover, if we consider a set of parameters $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{Q}^{n+(n-1)}$, we set $\beta_n = 1$ and write $\boldsymbol{\beta}$ both for the $(n-1)$ -tuple of rational parameters and for the n -tuple also including $\beta_n = 1$. For given parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}$ we denote by $d(\boldsymbol{\alpha}, \boldsymbol{\beta})$ the least common multiple of their denominators in reduced form. If the parameters are clear, we will omit them from the notation and will simply write d .

Let us recall some facts about the hypergeometric differential equation $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})y = 0$. It is *Fuchsian*, meaning that all of its *singularities* are *regular*. The singular points are $0, 1, \infty$ and the sets of *local exponents* at those singular points are

$$\begin{aligned} \text{at } 0: & \quad \{1 - \beta_1, \dots, 1 - \beta_{n-1}, 0\}, \\ \text{at } 1: & \quad \{0, 1, 2, \dots, n - 2, -1 + (\sum_{j=1}^n \beta_j - \sum_{i=1}^n \alpha_i)\}, \\ \text{at } \infty: & \quad \{\alpha_1, \dots, \alpha_n\}. \end{aligned}$$

Finally, assuming that $\alpha_i - \beta_j \notin \mathbb{Z}$ for all $i, j \in \{1, \dots, n\}$, a \mathbb{Q} -basis of solutions of $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})y = 0$ at the singularity 0 is given by

$$z^{1-\beta_j} {}_nF_{n-1}(1 + \boldsymbol{\alpha} - \beta_j, 1 + \boldsymbol{\beta} - \beta_j; x), \quad (3.0.3)$$

where $1 + \beta_j - \beta_j$ is omitted in the bottom parameter.

Hypergeometric functions and equations serve as test cases for many conjectures and investigations concerning D -finite power series. For example, Christol conjectured that any globally bounded D -finite power series is a diagonal of an algebraic multivariate series, and investigated this for hypergeometric series [Chr86b]. Adamczewski and Delaygue, as attributed by Vargas-Montoya [Var21, Conjecture 1.1], conjectured that the reduction modulo p of any G -function, which can be reduced modulo an infinite number of primes, is algebraic over $\mathbb{F}_p(x)$ for almost all such primes p . For hypergeometric series ${}_nF_{n-1}$, this statement follows from Christol's work [Chr86a] showing

that solutions of equations with strong Frobenius structure are p -automatic, and thus they are algebraic, following earlier work by Christol [Chr79; Chr+80]. This result was made explicit by Vargas-Montoya [Var21; Var24], bounding the algebraicity degree and giving an explicit shape of an annihilating polynomial in the form of Equation (2.3.2). As test cases to Conjecture 2.2.6 and its refinements we will study hypergeometric series for the remaining part of this article.

3.1 Reductions of hypergeometric series modulo p

In this section, we investigate how hypergeometric functions and equations behave when passing to positive characteristic. Our first result classifies those prime numbers p , modulo which a given hypergeometric function can be reduced, in terms of the repartition of the values $\exp(2i\pi\lambda\alpha_i)$ and $\exp(2i\pi\lambda\beta_j)$ (for λ varying in \mathbb{Z}) on the complex unit circle. This refines a theorem of Christol [Chr86b, Proposition 1], classifying all globally bounded hypergeometric functions, that is, those where the reduction is possible modulo almost all primes. We refer to [DRR17, Section 5] for a more recent treatment in English.

We then study the solution space of a hypergeometric differential equation modulo p and describe an explicit basis of it. We connect in particular its dimension to numerical invariants attached to the parameters α and β defining the underlying hypergeometric operator and show that it only depends on the congruence of p modulo d , a common denominator for α, β . Our results provide in particular a satisfying answer to Question 2.3.13, raised at the end of Section 2 in the case of hypergeometric functions.

3.1.1 Interlacing criteria

We denote the p -adic valuation of a rational number by $v_p(\cdot)$. Further, we write $\{\cdot\}_0$ (resp. $\{\cdot\}_1$) for the decimal part function (resp. the decimal part where we assign to integers the value 1 instead of 0). Christol defines a total ordering \preceq on \mathbb{Q} as follows:

$$a \preceq b \iff \{a\}_1 < \{b\}_1 \text{ or } (\{a\}_1 = \{b\}_1 \text{ and } a \geq b).$$

Let $f(x) = {}_nF_{n-1}(\alpha, \beta; x)$ be a hypergeometric function with rational parameters $\alpha, \beta \in (\mathbb{Q} \setminus (-\mathbb{N}))^{2n-1}$ and set $\beta_n = 1$. We denote by d the common denominator of all parameters. Then Christol defines a function $\mathcal{M} : \mathbb{Q} \times (\mathbb{Z}/d\mathbb{Z})^\times \rightarrow \mathbb{Z}$ by

$$\mathcal{M}(x, \lambda) := |\{1 \leq i \leq n : \lambda\alpha_i \preceq x\}| - |\{1 \leq j \leq n : \lambda\beta_j \preceq x\}|. \quad (3.1.1)$$

We note that the function $\mathcal{M}(\cdot, \lambda)$ is piecewise constant and continuous from the left, and that its jump points are among the values $\{\alpha_i\lambda\}_0 + \mathbb{Z}$ and $\{\beta_j\lambda\}_0 + \mathbb{Z}$.

We say that $f(x)$ satisfies *Christol's interlacing condition* for $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$ if $\mathcal{M}(x, \lambda) \geq 0$ for all $x \in \mathbb{Q}$. To determine whether $\mathcal{M}(\cdot, \lambda)$ is always positive, it suffices to check that $\mathcal{M}(\lambda\beta_j, \lambda) \geq 0$ for all j , or, to order the values of $\lambda\alpha_i$ and $\lambda\beta_j$ according to \preceq simultaneously and check if among the first ℓ entries for $1 \leq \ell \leq 2n$ of the joint ordered list there are always at least as many entries of the form $\lambda\alpha_i$ as of the form $\lambda\beta_j$. If the parameters of a hypergeometric function $f(x)$ are pairwise incongruent modulo \mathbb{Z} , Christol's interlacing condition for λ can be interpreted graphically on the unit circle as follows. We draw the two sets $\{\exp(2i\pi\lambda\alpha_i) : 1 \leq i \leq n\}$ in red and $\{\exp(2i\pi\lambda\beta_j) : 1 \leq j \leq n\}$ in blue on the unit circle. Then $f(x)$ satisfies Christol's interlacing condition if and only if, going around the unit circle starting after 1, one always encounters at least as many red points as blue ones.

Christol's classification of globally bounded hypergeometric functions reads as follows [Chr86b, Proposition 1].

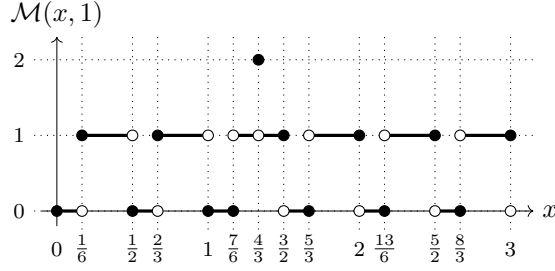


FIGURE 2: The function $\mathcal{M}(\cdot, 1)$ for the function ${}_3F_2\left(\left(\frac{1}{6}, \frac{2}{3}, \frac{4}{3}\right), \left(\frac{1}{3}, \frac{1}{2}\right); x\right)$ in the interval $[0, 3]$

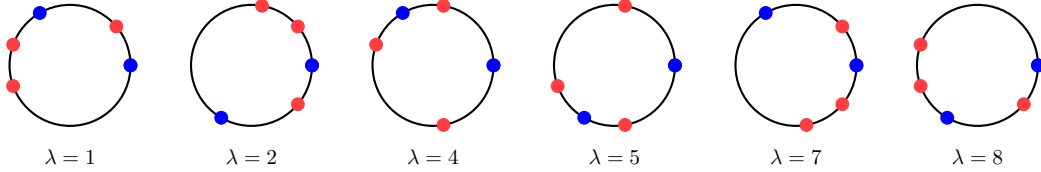


FIGURE 3: Christol's interlacing condition depicted on the unit circle for the function ${}_3F_2\left(\left(\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right), \left(\frac{1}{3}, 1\right); x\right)$

Theorem 3.1.1 (Christol, 1986). *The hypergeometric function $f(x) = {}_nF_{n-1}(\alpha, \beta; x)$ with $\alpha, \beta \in (\mathbb{Q} \setminus (-\mathbb{N}))^{2n-1}$ is globally bounded if and only if $f(x)$ satisfies Christol's interlacing criterion for all $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$, where d denotes the common denominator of the parameters α, β .*

Example 3.1.2. We consider $f(x) = {}_3F_2\left(\left(\frac{1}{6}, \frac{2}{3}, \frac{4}{3}\right), \left(\frac{1}{3}, \frac{1}{2}\right); x\right)$. Then the functions $\mathcal{M}(\cdot, 1)$ is depicted in Figure 2. This function is always nonnegative, and easily one also checks that also $\mathcal{M}(\cdot, 5)$ takes no negative values. Similarly the function $g(x) = {}_3F_2\left(\left(\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right), \left(\frac{1}{3}, 1\right); x\right)$ satisfies Christol's interlacing condition for all values of $\lambda \in (\mathbb{Z}/9\mathbb{Z})^\times$ as shown in Figure 3. Christol's criterion implies that f and g are globally bounded.

In Subsection 3.1.2 below, we will prove the following extension of Christol's theorem.

Theorem 3.1.3. *Let $f(x) = {}_nF_{n-1}(\alpha, \beta; x) = \sum_{k=0}^{\infty} h(\alpha, \beta; k)x^k$ be a hypergeometric function with rational parameters $\alpha, \beta \in (\mathbb{Q} \setminus (-\mathbb{N}))^{2n-1}$. Let $d \in \mathbb{N}$ be the smallest denominator of all parameters α_i, β_j and let p be a prime number, coprime to d . Assume that $p > 2d \cdot \max\{|\alpha_i|, |\beta_j|, 1\} + 1$, and consider the subgroup $\langle p \bmod d \rangle \subseteq (\mathbb{Z}/d\mathbb{Z})^\times$. Then $f(x)$ can be reduced modulo p if and only if Christol's interlacing condition is fulfilled for all $\lambda \in \langle p \bmod d \rangle$. For all other p , $v_p(h(\alpha, \beta; k))$ is not bounded from below.*

Remark 3.1.4. We note in particular, that if Christol's interlacing condition is not fulfilled for $\lambda = 1$, then $f(x)$ cannot be reduced modulo any prime number p , as $1 \in \langle p \bmod d \rangle$ for all p .

Example 3.1.5. Let

$$f(x) = {}_2F_1\left(\left(\frac{1}{2}, \frac{2}{3}\right), \left(\frac{1}{3}\right); x\right)$$

At the first glance one might be tempted to think that $f(x)$ can be reduced modulo prime numbers congruent to 5 modulo 6, as Christol's interlacing condition is fulfilled for $\lambda = 5$ (see the left hand part of Figure 4). However, by Remark 3.1.4, this is not the case.

Example 3.1.6. Consider the hypergeometric function

$$g(x) = {}_2F_1\left(\left(\frac{1}{4}, \frac{1}{2}\right), \left(\frac{15}{4}\right); x\right) = 1 + \frac{1}{30}x + \frac{1}{152}x^2 + \frac{15}{6992}x^3 + \dots$$

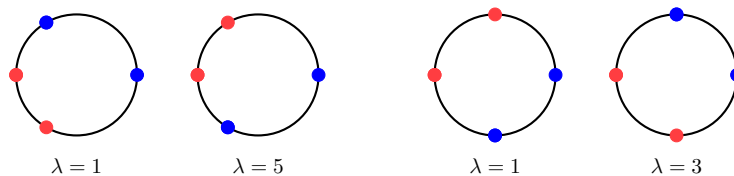


FIGURE 4: Christol's interlacing condition illustrated on the unit circle for the function $f(x) = {}_2F_1\left(\left(\frac{1}{2}, \frac{2}{3}\right), \left(\frac{1}{3}\right); x\right)$ (on the left) and the function $g(x) = {}_2F_1\left(\left(\frac{1}{4}, \frac{1}{2}\right), \left(\frac{15}{4}\right); x\right)$ (on the right)

For large enough primes p that are congruent to 3 modulo 4 the function $g(x)$ cannot be reduced modulo p , while reduction is possible for almost all prime numbers congruent to 1 modulo 4, as the right hand part of Figure 4 shows. However, taking $p = 5$, we see that already the coefficient of x in $g(x)$ is $1/30$, which cannot be reduced modulo 5. This does not contradict Theorem 3.1.3, as $5 < 2 \cdot 4 \cdot 15/4 + 1 = 31$.

We also mention here a similar criterion for the algebraicity of hypergeometric functions. It was formulated by Christol [Chr86b, Proposition 3, p.15 Corollary] in the same paper as the criterion for global boundedness, although his proof relies on the validity of the p -curvature conjecture for hypergeometric differential equations, which follows from Katz' work [Kat72], as elaborated in [Kat90]. Shortly after, it was independently stated by Beukers and Heckman [BH89, Theorem 4.8] with a more or less elementary proof, at the same time giving an elementary proof of the Grothendieck p -curvature conjecture for hypergeometric equations.

Theorem 3.1.7 (Christol, 1986; Beukers–Heckman, 1989; Katz, 1990). *Let $f(x) = {}_nF_{n-1}(\alpha, \beta; x)$ with $\alpha, \beta \in (\mathbb{Q} \setminus (-\mathbb{N}))^{2n-1}$ be a hypergeometric function and assume that $\alpha_i - \beta_j, \alpha_i \notin \mathbb{Z}$ for all i, j . Denote by d the common denominator of the parameters α, β and set $\beta_n = 1$. Then $f(x)$ is algebraic over $\mathbb{Q}(x)$ if and only if for all $j = 1, \dots, n$ and all $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$, we have*

$$\mathcal{M}(\lambda\beta_j, \lambda) = 0.$$

In the interpretation on the unit circle, this means that the sets $\{\exp(2i\pi\lambda\alpha_i) : 1 \leq i \leq s\}$ and $\{\exp(2i\pi\lambda\beta_j) : 1 \leq j \leq s\}$ alternate on the unit circle. We also underline that the criterion of Theorem 3.1.7 only works for hypergeometric functions with rational parameters without integer differences. A complete classification of algebraic hypergeometric functions with arbitrary complex parameters is given in [FY24].

Example 3.1.8. The hypergeometric function ${}_3F_2\left(\left(\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right), \left(\frac{1}{3}, 1\right); x\right)$ is not algebraic (although it is globally bounded), as it can be seen from the graphics in Figure 3.

By standard results from differential Galois theory, it is equivalent that a hypergeometric function ${}_nF_{n-1}(\alpha, \beta; x)$ is algebraic and that the monodromy group of its minimal differential operator, which is given by $\mathcal{H}(\alpha, \beta)$ under the assumption $\alpha_i - \beta_j \notin \mathbb{Z}$, is finite. The following result, appearing in Levelt's dissertation [Lev61] (and there attributed to N. G. de Bruijn), see also [BH89, Theorem 3.5], gives an explicit realization of the monodromy group of a hypergeometric differential equation as a group of matrices.

Theorem 3.1.9. *We assume that there are no integer differences between the sets $\alpha, \beta \in (\mathbb{Q} \setminus (-\mathbb{N}))^n$ with $\beta_n = 1$ of parameters of a hypergeometric operator $\mathcal{H}(\alpha, \beta)$. Let A_0, \dots, A_{n-1}*

and B_0, \dots, B_{n-1} be defined by the identities

$$A(x) := \prod_{i=1}^n (x - \exp(2i\pi\alpha_i)) = x^n + A_{n-1}x^{n-1} + \dots + A_0$$

$$B(x) := \prod_{j=1}^n (x - \exp(2i\pi\beta_j)) = x^n + B_{n-1}x^{n-1} + \dots + B_0.$$

We define the matrices

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & -A_0 \\ 1 & 0 & \cdots & 0 & -A_1 \\ 0 & 1 & & 0 & -A_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & -A_{n-1} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & \cdots & 0 & -B_0 \\ 1 & 0 & \cdots & 0 & -B_1 \\ 0 & 1 & & 0 & -B_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & -B_{n-1} \end{pmatrix}.$$

Then A is the local monodromy matrix of $\mathcal{H}(\alpha, \beta)$ at infinity, B^{-1} is the local monodromy matrix at 0 and together they generate the global monodromy group of $\mathcal{H}(\alpha, \beta)$.

3.1.2 Proof of Theorem 3.1.3

We start by recalling some technical results of Christol from his proof of Theorem 3.1.1. We write $f(x) = {}_nF_{n-1}(\alpha, \beta; x) = \sum_k h(\alpha, \beta; k)x^k$ and shorthand $h(\alpha, \beta; k) =: h_k$. We set $\beta_n = 1$. Let q be coprime to d and let $\Delta \in \mathbb{Z}$ be such that $\Delta q \equiv 1 \pmod{d}$. Then we define

$$V(x, q) := \left| \left\{ 1 \leq i \leq n : \{\Delta\alpha_i\}_1 - \frac{\alpha_i}{q} < x \right\} \right| - \left| \left\{ 1 \leq j \leq n : \{\Delta\beta_j\}_1 - \frac{\beta_j}{q} < x \right\} \right|. \quad (3.1.2)$$

Christol [Chr86b, p.6., Equation (6)] proves the following on the p -adic valuation of the coefficients of a hypergeometric function.

Lemma 3.1.10 (Christol). *We have $v_p(h_k) = \sum_{r=1}^{\infty} V\left(\left\{\frac{k}{p^r}\right\}_0, p^r\right)$.*

For each $\alpha \in \mathbb{Z}_p$ and $q = p^r$ for some positive integer r , we uniquely write $\alpha = qQ(\alpha, q) - R(\alpha, q)$ with $Q(\alpha, q) \in \mathbb{Z}_p$ and $0 \leq R(\alpha, q) < q$. Christol also proves the following about the quantities defining V [Chr86b, Lemma 4]:

Lemma 3.1.11 (Christol). *Let $\gamma \in \frac{1}{d}\mathbb{Z} \setminus (-\mathbb{N})$, let p be a prime number not dividing d . Let r be a positive integer such that $p^r > d \cdot |\gamma|$ and let Δ be such that $\Delta p \equiv 1 \pmod{d}$. Then we have*

$$\frac{R(\gamma, p^r)}{p^r} = \{\gamma\Delta^r\}_1 - \frac{\gamma}{p^r}.$$

The following two Lemmata are implicitly part of Christol's proof of the criterion for global boundedness of hypergeometric functions.

Lemma 3.1.12 (Christol). *Let $0 < x < \frac{1}{2d}$ and let p be a prime number not dividing d . We choose Δ such that $\Delta p \equiv 1 \pmod{d}$ and let r be a positive integer such that $p^r > 2d \cdot \max\{|\alpha_i|, |\beta_j|\}$. Then*

(i) *we have $V(x, p^r) = 0$, and*

(ii) for all $j \in \{1, \dots, n\}$, we have

$$V\left(\frac{R(\beta_j, p^r)}{p^r} + x, p^r\right) = \mathcal{M}(\beta_j \Delta^r, \Delta^r).$$

Proof. For (i), we note that

$$\{\gamma \Delta^r\}_1 - \frac{\gamma}{p^r} > \frac{1}{d} - \frac{1}{2d} > \frac{1}{2d}$$

for all $\gamma \in \{\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n\}$, as $\{\gamma \Delta^r\}_1 \in \frac{1}{d}\mathbb{N}_{>0}$. Therefore $V(x, p^r) = 0$.

For (ii), we write $\xi_j = \{\beta_j \Delta^r\}_1 - \frac{\beta_j}{p^r}$ and notice, as Christol, that

$$\lim_{x \rightarrow \xi_j^+} V(x, p^r) = \mathcal{M}(\Delta^r \beta_j, \Delta^r).$$

Indeed, for all $\gamma, \delta \in \{\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n\}$, the condition $\{\gamma \Delta^r\}_1 - \frac{\gamma}{p^r} \leq \{\delta \Delta^r\}_1 - \frac{\delta}{p^r}$ is equivalent to $\gamma \Delta^r \preceq \delta \Delta^r$ because of the bound on p^r . Moreover, by Lemma 3.1.11, we know that

$$\frac{R(\beta_j, p^r)}{p^r} = \{\beta_j \Delta^r\}_1 - \frac{\beta_j}{p^r}.$$

Finally, it follows as in the proof of (i) that the function $V(\cdot, p^r)$ is constant on the interval $\left(\frac{R(\beta_j, p^r)}{p^r}, \frac{R(\beta_j, p^r)}{p^r} + \frac{1}{2d}\right)$. \square

Lemma 3.1.13 (Christol). *We assume $p^r > 2d \cdot \max(|\alpha_i|, |\beta_j|)$ is coprime with d , we choose Δ such that $p\Delta \equiv 1 \pmod{d}$ and assume that $f(x)$ satisfies Christol's interlacing condition for Δ^r . Then $V(x, p^r) \geq 0$ for all $x \in \mathbb{Q}$.*

Proof. The function $V(\cdot, p^r)$ is piecewise constant and its jumps of negative height happen at the values $\{\beta_j \Delta^r\}_1 - \beta_j/p^r$. By the assumption and Lemma 3.1.12.(ii), the function $V(\cdot, p^r)$ is still positive after these jump points. \square

We are now ready to complete the proof of Theorem 3.1.3. We assume that Christol's interlacing criterion is fulfilled for all $\lambda \in \langle p \pmod{d} \rangle$. Then, by Lemma 3.1.10, we have

$$v_p(h_k) = \sum_{r=1}^{\infty} V\left(\left\{\frac{k}{p^r}\right\}_0, p^r\right)$$

for all k . From Lemma 3.1.13, we see that each of the summands is nonnegative, and thus $v_p(h_k) \geq 0$ for all k . Conversely, let us assume that there is $\lambda \in \langle p \pmod{d} \rangle$ such that Christol's interlacing condition is not fulfilled. We denote by m the minimal positive integer such that $\lambda \equiv \Delta^m \pmod{d}$ and set $\ell := \text{ord}_d(p) = |\langle p \pmod{d} \rangle|$. We choose j in such a way that

$$\mathcal{M}(\Delta^m \beta_j, \Delta^m) = |\{1 \leq i \leq n : \Delta^m \alpha_i \preceq \Delta^m \beta_j\}| - |\{1 \leq i \leq n : \Delta^m \beta_i \preceq \Delta^m \beta_j\}| < 0.$$

For any $a \in \mathbb{N}$, we will construct k such that $v_p(h_k) \leq -a$. To do this, we first set $k_{m+(a-1)\ell} := R(\beta_j, p^{m+(a-1)\ell})$. Successively for $r = m + (a-1)\ell - 1, m + (a-1)\ell - 2, \dots, 1$, we then consider the unique integer $d_r \in \{0, 1, \dots, p^{r-1}\}$ such that

$$k_r + d_{r-1} \equiv \begin{cases} 0 \pmod{p^{r-1}} & \text{if } r \not\equiv m \pmod{\ell} \\ R(\beta_j, p^{r-1}) \pmod{p^{r-1}} & \text{otherwise,} \end{cases}$$

and set $k_{r-1} := k_r + d_{r-1}$. We finally take $k := k_1$. For each r , we then have $d_{r-1} + \dots + d_0 \leq p^{r-1} + \dots + p + 1 = \frac{p^r - 1}{p - 1} < \frac{p^r}{2d}$, which ensures that k satisfies

$$k \in \begin{cases} \left[R(\beta_j, p^r) + 1, R(\beta_j, p^r) + \frac{p^r}{2d} \right) \pmod{p^r} & \text{if } r < \ell \cdot a \text{ and } r \equiv m \pmod{\ell} \\ \left[1, \frac{p^r}{2d} \right) \pmod{p^r} & \text{otherwise.} \end{cases}$$

Thus, we get $\left\{ \frac{k}{p^r} \right\}_0 < \frac{1}{2d}$ for all $r \not\equiv m \pmod{\ell}$ and all $r > a\ell$. For $r = m, m + \ell, \dots, m + (a - 1)\ell$ we have $\left\{ \frac{k - R(\beta_j, p^r)}{p^r} \right\}_0 \leq \frac{1}{2d}$, and therefore, by Lemma 3.1.12,

$$V\left(\left\{ \frac{k}{p^r} \right\}_0, p^r\right) = \begin{cases} \mathcal{M}(\Delta^r \beta_j, \Delta^r) & r = m, m + \ell, \dots, m + (a - 1)\ell \\ 0 & \text{otherwise.} \end{cases}$$

Finally, using Lemma 3.1.10, we compute

$$v_p(h_k) = \sum_{r=1}^{\infty} V\left(\left\{ \frac{k}{p^r} \right\}_0, p^r\right) = a\mathcal{M}(\Delta^m \beta_j, \Delta^m) \leq -a.$$

Remark 3.1.14. For small prime numbers p it is enough to check the p -adic evaluation of finitely many coefficients to conclude that the hypergeometric function might be reduced properly modulo p . Indeed, let r_0 be such that $p^{r_0} > 2d \cdot \max\{|\alpha_i|, |\beta_j|, 1\} + 1$. Then, for all n , we have

$$v_p(h_k) = \sum_{r=1}^{\infty} V\left(\left\{ \frac{k}{p^r} \right\}_0, p^r\right) = \sum_{r=1}^{r_0-1} V\left(\left\{ \frac{k}{p^r} \right\}_0, p^r\right) + \sum_{r=r_0}^{\infty} V\left(\left\{ \frac{k}{p^r} \right\}_0, p^r\right)$$

where the right summand is always positive, if Christol's interlacing condition is fulfilled for all $\lambda \in \langle p \pmod{d} \rangle$, and the left summand is periodic in k with period p^{r_0-1} .

Example 3.1.15. Continuing Example 3.1.5, that is

$$f(x) = {}_2F_1\left(\left(\frac{1}{2}, \frac{2}{3}\right), \left(\frac{1}{3}\right); x\right) = \sum_{n \geq 0} h_n x^n,$$

we can construct explicitly an integer n such that the denominator of h_n is divisible by 17^2 using the strategy of the proof of Theorem 3.1.3. We have $a = 2, \ell = 2$ and $m = 2$ and use $\beta_j = 1/3$. With this, we compute $k_4 = 27840, k_3 = 29478, k_2 = 29574$ and $k_1 = 29580$. And, indeed, checking with a computer algebra system, we convince ourselves that the 17-adic evaluation of h_{29580} is -2 .

3.1.3 Solutions of the hypergeometric differential equation modulo p

We now discuss the question of determining the dimension of the space of solutions of a hypergeometric differential equation modulo p in $\mathbb{F}_p[[x]]$ when p does not divide d . It turns out that this dimension is also encoded by the relative position of the exponentials of α_i and β_j on the unit complex circle; the slight difference between what precedes is that we will not work with the reductions of α_i and β_j modulo \mathbb{Z} , but modulo p . More precisely, for each index $i \in \{1, \dots, n\}$, we consider the complex number

$$\alpha_{i,p} := \zeta_{2p} \cdot \zeta_p^{-\alpha_i \pmod{p}} = \exp\left(2i\pi \cdot \left(\frac{1}{2p} - \frac{\alpha_i \pmod{p}}{p}\right)\right)$$

and color it in green. We underline that the previous definition is not ambiguous because the fraction $(\alpha_i \bmod p)/p$ is well-defined modulo \mathbb{Z} . In concrete terms, $\zeta_p^{-\alpha_i \bmod p} = \zeta_p^{-\alpha_{i,p}}$ where $\alpha_{i,p}$ is an *integer* which is congruent to α_i modulo p . Similarly, we color in yellow the points

$$\beta_{j,p} := \zeta_p \cdot \zeta_p^{-\beta_j \bmod p} = \exp\left(2i\pi \cdot \left(\frac{1}{p} - \frac{\beta_j \bmod p}{p}\right)\right)$$

for j varying in $\{1, \dots, n\}$ as well. Since $\beta_n = 1$, the point $1 \in \mathbb{C}$ is always colored in yellow.

Definition 3.1.16. The p -interlacing number of (α, β) is the number of times we observe a green point followed by a yellow one (or, equivalently, a yellow one followed by a green) when running clockwise through the unit circle.

The p -interlacing number will allow us to answer Question 2.3.13 for hypergeometric equations. The proof of the following result can be easily deduced from Katz' results on the p -curvature of a hypergeometric operator $\mathcal{H} = \mathcal{H}(\alpha, \beta)$ [Kat90, Proof of Sublemma 5.5.2.1, p. 174 f.]. Below, we reformulate it in a more down-to-earth fashion, avoiding the use of the p -curvature.

Theorem 3.1.17. Let $\mathcal{T}_p(\alpha, \beta)$ denote the set of exponents t corresponding to a yellow point for which there is a green point before we reach the next yellow point when running clockwise on the unit complex circle. For $t \in \mathcal{T}_p(\alpha, \beta)$, we denote by k_t the exponent corresponding to the next green point. We set

$$f_t(x) := \sum_{k=t}^{k_t-1} h(\alpha, \beta; k) \cdot p^{-v_p(h(\alpha, \beta; t))} x^k. \quad (3.1.3)$$

The family $(f_t(x))_{t \in \mathcal{T}_p(\alpha, \beta)}$ is a $\mathbb{F}_p(x^p)$ -basis of the space of solutions of $\mathcal{H}(\alpha, \beta)$.

In particular, the dimension of this vector space is given by the p -interlacing number of (α, β) .

Proof (after Katz). We view $\mathbb{F}_p(x)$ as a p -dimensional vector space over $\mathbb{F}_p(x^p)$. The operator $\mathcal{H}(\alpha, \beta)$ is a linear endomorphism of this vector space. It is determined by $\mathcal{H}(\alpha, \beta)(x^k) = -A(k)x^{k+1} + B(k)x^k$, where $A(k) = \prod_{i=1}^n (k + \alpha_i)$ and $B(k) = \prod_{j=1}^n (k + \beta_j - 1)$. We chose $m \in \mathbb{F}_p$, such that $m \equiv 1 - \alpha_i \pmod{p}$ for some $i \in \{1, \dots, n\}$. The matrix of this linear map in the basis $(x^m, x^{m+1}, \dots, x^{m+p-1})$ is of the form

$$\begin{pmatrix} B(m) & 0 & 0 & \cdots & 0 & -A(m+p-1) \\ -A(m) & B(m+1) & 0 & \cdots & 0 & 0 \\ 0 & -A(m+1) & B(m+2) & & 0 & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & 0 & 0 & \ddots & B(m+p-2) & 0 \\ 0 & 0 & 0 & & -A(m+p-2) & B(m+p-1) \end{pmatrix},$$

where the top right entry is zero, as $A(m+p-1) = 0$ by definition. The matrix decomposes into a block diagonal form, each zero of A separating two blocks. Each of the blocks is a lower diagonal matrix with consecutive values of B on the main diagonal, and consecutive values of A , all nonzero, on the diagonal below. The co-rank of this matrix is at most one, as the bottom left minor of order one less is non-zero. Moreover as the blocks are lower triangular, the co-rank is zero and only if all entries on the main diagonal are different from zero.

Consider such a block of co-rank one and let $b := 1 - \beta_j \pmod{p}$ be the last zero of B in this block, and let $a := -\alpha_i \pmod{p}$ the following zero of A . Then it is easy to convince oneself, that

$$v_b := \left(0 \quad \cdots \quad 0 \quad 1 \quad \frac{A(b)}{B(b+1)} \quad \frac{A(b)A(b+1)}{B(b+1)B(b+2)} \quad \cdots \quad \frac{A(b)\cdots A(a-1)}{B(b+1)\cdots B(a)} \right)^\top$$

is a well-defined vector in the kernel of this block. It corresponds to the function $h(\boldsymbol{\alpha}, \boldsymbol{\beta}; b)^{-1} f_b(x)$. The proposition follows from these observations. \square

Remark 3.1.18. If we assume that $f(x) = {}_nF_{n-1}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ can be reduced modulo p , then the truncation at x^p of $f(x) \bmod p$ is a linear combination of the polynomials $f_t(x)$. Those t , for which the polynomials $f_t(x)$ have nonzero coefficients in this combination, are precisely the elements of the set

$$\mathcal{S}_p(\boldsymbol{\alpha}, \boldsymbol{\beta}) := \left\{ r \in \{0, \dots, p-1\} : r \equiv 1 - \beta_j \pmod{p} \text{ for some } j \text{ and } v_p(h(\boldsymbol{\alpha}, \boldsymbol{\beta}; r)) = 0 \right\}. \quad (3.1.4)$$

Remark 3.1.19. In [Dwo90], Dwork constructed a differential field extension of $\mathbb{F}_p[x]$ defined by considering countably many variables z_i with $z'_i = \frac{z_{i-1}}{z_i - 1}$, resembling the derivation rule of iterated logarithms in characteristic 0. Dwork's construction provides a full basis of n solutions of differential equations with nilpotent p -curvature, such as the hypergeometric differential equation. Indeed, the Chudnovsky's showed in [CC85] that minimal differential operators of G -functions, such as hypergeometric functions ${}_nF_{n-1}$ with rational parameters and no integer differences between them [Gal81], are globally nilpotent, *i.e.*, they have p -curvature 0 for almost all prime numbers. In [FH23], Dwork's ideas are extended to arbitrary regular singular differential equations with coefficients in $\mathbb{F}_p[[x]]$, and an algorithm for explicitly computing solutions in the extension is depicted. Applying this to the hypergeometric differential equation $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})y = 0$, we find a basis of n linearly independent polynomial solutions of the form $f_t(x) = \sum_{k=t}^{k_t-1} g_{k,t}(z_1, z_2, \dots) x^k \in \mathbb{F}_p[x, z_1, z_2, \dots]$ with $k_t \leq 2p$ and $g_{k,t}(z_1, z_2, \dots) \in \mathbb{F}_p[z_1, z_2, \dots]$ for all $t = 1 - \beta_j \bmod p$.

We next discuss how the number of solutions of the reduction of a fixed hypergeometric differential equation $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})y = 0$ with rational coefficients modulo p varies with the prime number p . Let d denote again the common denominator of the parameters $\boldsymbol{\alpha}, \boldsymbol{\beta} \in (\mathbb{Q} \setminus (-\mathbb{N}))^{2n-1}$ of $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})$.

Proposition 3.1.20. *Let $p > 2d \cdot \max\{|\alpha_i|, |\beta_j|, 1\}$ and choose Δ such that $p\Delta \equiv 1 \pmod{d}$. Then the p -interlacing number of $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is equal to the number of local minima in the cyclic sequence $(\mathcal{M}(\gamma_k \Delta, \Delta))_{k=1}^{2n}$, where $\{\gamma_k\} = \{\Delta\alpha_i\} \cup \{\Delta\beta_j\}$ and $\gamma_1 < \gamma_2 < \dots < \gamma_{2n}$. In particular, the number of solutions of the hypergeometric differential equation in $\mathbb{F}_p[x]$ for large characteristics p depends only on the congruence class of p modulo d .*

Proof. We know from Lemma 3.1.11 that for $p > 2d \cdot \max\{|\alpha_i|, |\beta_j|, 1\}$ we have

$$\frac{R(\alpha_i, p)}{p} = \{\alpha_i \Delta\}_1 - \frac{\alpha_i}{p}.$$

Moreover we have seen in the proof of Lemma 3.1.12 that

$$\{\gamma \Delta\}_1 - \frac{\gamma}{p} < \{\delta \Delta\}_1 - \frac{\delta}{p} \iff \gamma \Delta \preceq \delta \Delta \quad (\gamma, \delta \in \frac{1}{d}\mathbb{Z}). \quad (3.1.5)$$

This shows that the (negative) residues $R(\gamma_k, p)$ of the parameters γ_k modulo p are ordered in the same way as the decimal parts $\{\gamma_k \Delta\}_1$. Finally, a block of consecutive elements colored in yellow (resp. green), corresponds to consecutive zeroes of $A(t)$ (resp. $B(t)$) in \mathbb{F}_p , which then correspond to a block of increasing respectively decreasing sequence elements of the sequence $(\mathcal{M}(\gamma_k \Delta, \Delta))_{k=1}^{2n}$, which in turn is equal to the number of local minima attained in this sequence. \square

Remark 3.1.21. Assuming that $\alpha_i - \beta_j \notin \mathbb{Z}$, Proposition 3.1.20 can be visualized geometrically on the unit circle. Indeed, under the assumptions of the proposition, the equivalence (3.1.5) shows that the points $\alpha_{i,p}, \beta_{j,p}$ ($1 \leq i, j \leq n$) are ordered in the same way on the unit complex circle than the points $\exp(2i\pi\Delta\alpha_i), \exp(2i\pi\Delta\beta_j)$ ($1 \leq i, j \leq n$).

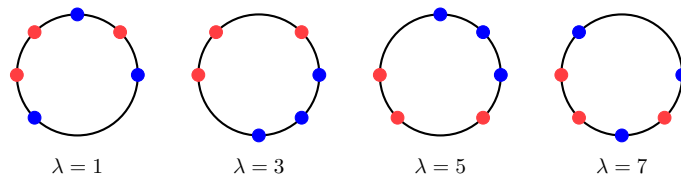


FIGURE 5: The sets $\{\exp(2i\pi\lambda\alpha_i)\}$ and $\{\exp(2i\pi\lambda\beta_j)\}$ for ${}_3F_2\left(\left(\frac{1}{8}, \frac{3}{8}, \frac{1}{2}\right), \left(\frac{1}{4}, \frac{5}{8}\right); x\right)$

Example 3.1.22. The hypergeometric function $f(x) = {}_3F_2\left(\left(\frac{1}{8}, \frac{3}{8}, \frac{1}{2}\right), \left(\frac{1}{4}, \frac{5}{8}\right); x\right)$ is not globally bounded. Christol's interlacing condition is fulfilled for $\lambda = 1, 3$, but not for $\lambda = 5, 7$. Therefore, according to Theorem 3.1.3, $f(x)$ can be reduced modulo almost all prime numbers congruent to 1 and 3 modulo 8, but almost all prime numbers congruent to 5 or 7 modulo 8 appear up to arbitrarily high powers in the denominators of the coefficients of $f(x)$. Moreover, the $\mathbb{F}_p[[x^p]]$ -dimension of the solutions of the hypergeometric differential equation

$$\mathcal{H}\left(\left(\frac{1}{8}, \frac{3}{8}, \frac{1}{2}\right), \left(\frac{1}{4}, \frac{5}{8}\right)\right)y = 0$$

in $\mathbb{F}_p[[x]]$ is for sufficiently large primes p , according to Theorem 3.1.17 and Proposition 3.1.20, two if $p \equiv 1, 7 \pmod{8}$ and one otherwise. All this information can be read off from Figure 5.

3.2 Algebraicity modulo p and Galois groups

In [Var24], it was shown that the reductions of hypergeometric functions modulo p are algebraic over $\mathbb{F}_p(x)$. In this subsection, we recall the methods of *loc. cit.* and develop them further in order to get annihilating polynomials of smaller sizes. This will be important for the computations of the Galois groups later on.

3.2.1 The Dwork map

A main tool in the construction is the Dwork map $\mathfrak{D}_p : \mathbb{Z}_{(p)} \rightarrow \mathbb{Z}_{(p)}$, defined by Euclidean division: as before, we write $\gamma \in \mathbb{Z}_{(p)}$ uniquely as $\gamma = pQ(\gamma, p) - R(\gamma, p)$ with $Q(\gamma, p) \in \mathbb{Z}_{(p)}$ and $0 \leq R(\gamma, p) < p$. We set $\mathfrak{D}_p(\gamma) := Q(\gamma, p)$. In other words, \mathfrak{D}_p is uniquely defined by the relation

$$p \cdot \mathfrak{D}_p(x) - x \in \{0, 1, \dots, p-1\}.$$

We collect a few facts about \mathfrak{D}_p .

Lemma 3.2.1. (1) For $\gamma \in \mathbb{Z}_{(p)}$, let

$$-\gamma = \gamma^{(0)} + p\gamma^{(1)} + p^2\gamma^{(2)} + \dots$$

be the p -adic expansion of $-\gamma$. Then, for any integer $k \geq 1$,

$$-\mathfrak{D}_p^k(\gamma) = \gamma^{(k)} + p\gamma^{(k+1)} + p^2\gamma^{(k+2)} + \dots.$$

(2) The Dwork operator \mathfrak{D}_p acts on $\mathbb{Z}_{(p)}/\mathbb{Z}$; more precisely, for any fixed $d \in \mathbb{N}$ not divisible by p , it acts on $(\frac{1}{d}\mathbb{Z})/\mathbb{Z}$ by multiplication with p^{-1} .

(3) The Dwork operator \mathfrak{D}_p maps $(0, 1] \cap \frac{1}{d}\mathbb{Z}$ to itself.

(4) For $\gamma \in (0, 1] \cap \mathbb{Z}_{(p)}^\times$, the smallest positive integer ℓ such that $\mathfrak{D}_p^\ell(\gamma) = \gamma$ is equal to the smallest positive integer ℓ such that $p^\ell \gamma \equiv \gamma \pmod{\mathbb{Z}}$, that is, if $\gamma = \frac{c}{d}$ with $\gcd(c, d) = 1$, ℓ is given as the order of p modulo d .

Proof. The first assertion follows directly from the definition when $k = 1$. For general k , it follows by induction. For (2), we write $\gamma = \frac{c}{d}$ with $\gcd(c, d) = 1$. We then have $\frac{c}{d} = p\mathfrak{D}_p(\gamma) - R(\gamma, p)$ with $R(\gamma, p) \in \{0, 1, \dots, p-1\}$, so clearly $\mathfrak{D}_p(\gamma) \in \frac{1}{d}\mathbb{Z}$, say $\mathfrak{D}_p(\gamma) = \frac{c'}{d}$. Then $c \equiv pc' \pmod{d}$, so c' only depends on $c \pmod{d}$ and \mathfrak{D}_p indeed acts by multiplication with p^{-1} . For (3), keeping the previous notation, we note that $e > p$ implies $c = pe - R(\gamma, p)d$ and then $c > d$, contradicting $0 < c \leq d$. Likewise, if $e \leq 0$, then $c \leq 0$, also a contradiction. The last point is obvious from what precedes. \square

For $\gamma \in \mathbb{Z}_{(p)}$, let $\ell_p(\gamma)$ denote the smallest positive integer ℓ such that $p^\ell \gamma \equiv \gamma \pmod{\mathbb{Z}}$ as in Lemma 3.2.1.(4). More generally, given an arbitrary sets of parameters $\alpha, \beta \in \mathbb{Z}_{(p)}^{n+(n-1)}$, we define $\ell_p(\alpha, \beta)$ as the smallest positive integer such that $\mathfrak{D}_p^{\ell_p(\alpha, \beta)}(\alpha) \equiv \alpha \pmod{\mathbb{Z}}$ and $\mathfrak{D}_p^{\ell_p(\alpha, \beta)}(\beta) \equiv \beta \pmod{\mathbb{Z}}$, where these equations are to be read as equalities of sets. In particular, $\ell_p(\alpha, \beta)$ always divides the order of p in $(\mathbb{Z}/d\mathbb{Z})^\times$, where d denotes the common denominator of the parameters. However, in general there is no equality, as demonstrated by the following example.

Example 3.2.2. We have $\ell_{13}((\frac{1}{7}, \frac{6}{7}), (\frac{1}{2})) = 1$, as $\mathfrak{D}_{13}(\frac{1}{7}) = \frac{6}{7}$, $\mathfrak{D}_{13}(\frac{6}{7}) = \frac{1}{7}$ and $\mathfrak{D}_{13}(\frac{1}{2}) = \frac{1}{2}$. At the same time we have $\text{ord}_{14}(13) = 2$.

When the parameters α, β are clear from the context, we will suppress them in the notation and write simply ℓ_p for $\ell_p(\alpha, \beta)$.

3.2.2 The hypergeometric relation graph

We are going to construct a graph, whose vertices correspond to parameters of hypergeometric functions, and whose edges will encode algebraic relations between those functions. We denote by

$$\mathcal{V}_p := (\mathbb{Z}_{(p)} \setminus (-\mathbb{N}))^{n+(n-1)}$$

the set of vertices corresponding to all possible parameters. Moreover, we let

$$\mathcal{V}_p(\alpha, \beta) := \{(\alpha', \beta') \in \mathcal{V}_p : \alpha_i \equiv \alpha'_i \pmod{\mathbb{Z}}, \beta_j \equiv \beta'_j \pmod{\mathbb{Z}}\}.$$

These sets form a partition of \mathcal{V}_p .

We define the *hypergeometric relation graph* \mathcal{G}_p as the following directed graph with labeled edges. The vertices are given by \mathcal{V}_p . For the edges we carry out the following construction. For $\gamma \in \mathbb{Z}_{(p)}^m$ and let $r \in \mathbb{N}$, we put

$$\mathfrak{D}_{p,r}(\gamma) := \begin{cases} \mathfrak{D}_p(\gamma) + 1 & \text{if } (\gamma)_r \in p\mathbb{Z}_{(p)} \\ \mathfrak{D}_p(\gamma) & \text{otherwise.} \end{cases}$$

For every $s \in \mathcal{S}_p(\alpha, \beta)$, as defined in Equation (3.1.4), we connect $(\alpha, \beta) \in \mathcal{V}_p$ with $\mathfrak{D}_{p,s}(\alpha, \beta) \in \mathcal{V}_p$ with a directed edge $e : (\alpha, \beta) \rightarrow \mathfrak{D}_{p,s}(\alpha, \beta)$ labeled by the polynomial $Q(e) := f_s(x)$ as defined by Equation (3.1.3).

We define $\mathcal{G}_p(\alpha, \beta)$ as the sub-graph, of \mathcal{G}_p containing (α, β) , and all vertices reachable by an oriented path, starting at (α, β) .

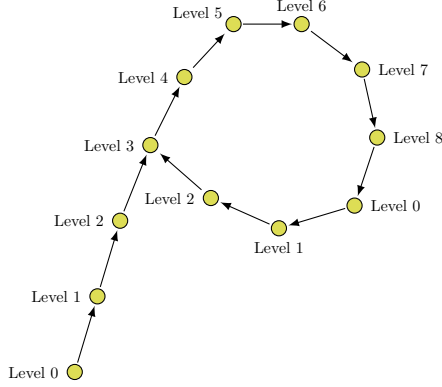


FIGURE 6: The shape of the graph $\mathcal{G}_p(\alpha, \beta)$ when $\beta = (1, \dots, 1)$

Lemma 3.2.3. (1) Let $\gamma = \frac{c}{d} \in \mathbb{Z}_{(p)} \setminus (-\mathbb{N})$, where p is a prime number with $p > 2d \cdot |\gamma|$. Then $\mathfrak{D}_p(\gamma) \in (0, 1]$

(2) Let $r \in \mathbb{N}$ and $M \geq \frac{2p-1}{p-1}$. If $|\gamma| \leq M$, then $|\mathfrak{D}_{p,r}(\gamma)| \leq M$.

Proof. For (1), we first assume by contradiction that $\mathfrak{D}_p(\gamma) > 1$. We have $\mathfrak{D}_p(\gamma) \in \frac{1}{d}\mathbb{Z}$, and so

$$p\mathfrak{D}_p(\gamma) - \gamma \geq (p + p/d) - \gamma \geq p,$$

contradicting the definition of \mathfrak{D}_p . Similarly, if $\mathfrak{D}_p(\gamma) < 0$, we obtain

$$p\mathfrak{D}_p(\gamma) - \gamma \leq (-p/d) - \gamma < 0,$$

again contradicting the definition of \mathfrak{D}_p . Finally, if $\mathfrak{D}_p(\gamma) = 0$, we must have $-\gamma \in \{0, 1, \dots, p-1\}$, a contradiction to our assumption.

For the second part, we have $p\mathfrak{D}_p(\gamma) \in \gamma + \{0, 1, \dots, p-1\}$. So $-M \leq p\mathfrak{D}_p(\gamma) \leq \gamma + p - 1 \leq M + p - 1$, and therefore $-M \leq -M/p \leq \mathfrak{D}_{p,r}(\gamma) \leq \mathfrak{D}_p(\gamma) \leq \frac{M+p-1}{p} + 1 \leq M$. \square

We conclude that, for each choice of (α, β) , the graph $\mathcal{G}_p(\alpha, \beta)$ is a finite graph. This follows from the fact that for large enough M the finite set $\frac{1}{d}[-M, M]$ is mapped into itself by $\mathfrak{D}_{p,r}$, as shown by the Lemmata 3.2.1 and 3.2.3.

Let us assume that $(\alpha, \beta) \in (0, 1]^{n+(n-1)}$. In $\mathcal{G}_p(\alpha, \beta)$, we say that a vertex (α', β') is at level $k \in \{0, 1, \dots, \ell_p - 1\}$ if it is in $\mathcal{V}(\mathfrak{D}_p^k(\alpha), \mathfrak{D}_p^k(\beta))$. We define the *width* of level k of $\mathcal{G}_p(\alpha, \beta)$ as the number of vertices on level k , and the *width* of the graph as the minimum of the widths of each level. For arbitrary (α, β) , we say that the width of $\mathcal{G}_p(\alpha, \beta)$ is given by the width of $\mathcal{G}_p(\bar{\alpha}, \bar{\beta})$ with $\bar{\alpha} = \{\alpha\}_1$ and $\bar{\beta} = \{\beta\}_1$. This will make sense after the Proposition 3.2.5, in which we show that (at least for large enough p), the graph $\mathcal{G}_p(\bar{\alpha}, \bar{\beta})$ is an induced subgraph of $\mathcal{G}_p(\alpha, \beta)$.

Example 3.2.4. We consider the case where $\beta = (1, \dots, 1)$. Then, for all integer k , we have $\mathfrak{D}_p^k(\beta) = (1, \dots, 1)$ as well and that the set $\mathcal{S}_p(\mathfrak{D}_p^k(\alpha), (1))$ is the singleton $\{0\}$. It follows by induction that each vertex in $\mathcal{G}_p(\alpha, \beta)$ is of the form $(\mathfrak{D}_p^k(\alpha), (1))$ and has only one outgoing edge to $(\mathfrak{D}_p^{k+1}(\alpha), (1))$. Hence the graph $\mathcal{G}_p(\alpha, \beta)$ has a shape of a “ ρ ,” as drawn in Figure 6. The value $\ell_p(\alpha, \beta)$ is the length of the “circle part” (it is 9 on the drawing of Figure 6) and the level increases by 1 modulo $\ell_p(\alpha, \beta)$ each time we move from a vertex to the next one.

In addition, the vertices in the circle part are characterized by the fact that the corresponding $\mathfrak{D}_p^k(\alpha)$ has all its coordinates in $(0, 1]$. In particular, when (α, β) itself is in $(0, 1]^{n+(n-1)}$, the

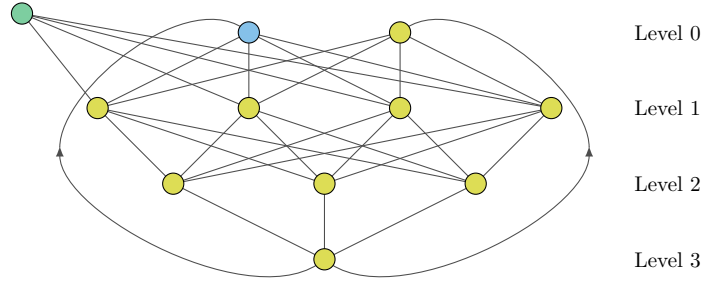


FIGURE 7: The graph $\mathcal{G}_p(\alpha, \beta)$ for $\alpha = (-6/25, 9/25, 39/25, 54/25, 74/25)$, $\beta = (-9/5, 3/5, 9/5, 3)$ with the vertex (α, β) drawn in green, and the vertex $(\bar{\alpha}, \bar{\beta})$ drawn in blue for $p \equiv 13 \pmod{25}$ and $p > 200$. All edges are oriented downwards except marked otherwise.

initial part before the circle is not present and the graph thus reduces to a circle. For arbitrary (α, β) , Proposition 3.2.5 below ensures that, when p is large enough, the initial part is constituted of at most one point.

Proposition 3.2.5. *Let $\alpha, \beta \in (\mathbb{Q} \setminus (-\mathbb{N}))^{n+(n-1)}$ be two sets of parameters of a hypergeometric function with common denominator d and let p be a prime with $p > 2d \cdot \max\{|\alpha_i| + 1, |\beta_j| + 1\}$, we choose Δ such that $p\Delta \equiv 1 \pmod{d}$ and set $\bar{\alpha} = \{\alpha\}_1$ and $\bar{\beta} = \{\beta\}_1$.*

- (1) *Assuming $\alpha = \bar{\alpha}$ and $\beta = \bar{\beta}$, there is an edge in $\mathcal{G}_p(\alpha, \beta)$ from any vertex at level k to any vertex at level $k + 1$ for all k taken modulo ℓ_p .*
- (2) *If $(\alpha, \beta) \in \mathcal{G}_p(\bar{\alpha}, \bar{\beta})$ then $\mathcal{G}_p(\bar{\alpha}, \bar{\beta}) = \mathcal{G}_p(\alpha, \beta)$. Otherwise, $\mathcal{G}_p(\bar{\alpha}, \bar{\beta})$ is the induced subgraph of $\mathcal{G}_p(\alpha, \beta)$ obtained by removing the vertex (α, β) .*
- (3) *The shape of $\mathcal{G}_p(\alpha, \beta)$ only depends on the congruence class of p modulo d .*
- (4) *Assuming $\alpha = \bar{\alpha}$ and $\beta = \bar{\beta}$, the width at level k is equal to the number of β_j such that $\mathcal{M}(\Delta^{k-1}\beta_j, \Delta^{k-1}) = 0$, and the width of $\mathcal{G}_p(\alpha, \beta)$ is at most equal to the number of solutions of $\mathcal{H}(\alpha, \beta)y = 0$ that can be reduced modulo p .*

Figure 7 shows the typical shape of the induced subgraph $\mathcal{G}(\alpha, \beta)$ of the hypergeometric relation graph, corresponding to a pair of parameters (α, β) for a prime number p , large enough with respect to the common denominator d of the parameters.

Proof. We will show that the vertices on level k are given by

$$(\mathfrak{D}_{p,r}(\mathfrak{D}_p^{k-1}(\alpha)), \mathfrak{D}_{p,r}(\mathfrak{D}_p^{k-1}(\beta))) \quad (3.2.1)$$

for $r \in \mathcal{S}_p(\mathfrak{D}_p^{k-1}(\alpha), \mathfrak{D}_p^{k-1}(\beta))$ for $k = 0, \dots, \ell_p - 1$. First, those vertices are all distinct and the order of the tuple (α, β) under \mathfrak{D}_p is ℓ_p . Also, it is clear that these vertices are all to be found at level k . Moreover, we will show that any edge starting at one vertex of the form (3.2.1) at level k ends at a vertex at level $k + 1$ of the same form. Thus the induced subgraph of $\mathcal{G}_p(\alpha, \beta)$ consisting of these vertices (and, possibly, (α, β)) contains all edges, and thus agrees with $\mathcal{G}_p(\alpha, \beta)$.

Without loss of generality, let us consider the vertex (α, β) and another vertex (α', β') of the form (3.2.1) at the same level 0. Then each entry of α', β' differs from α, β by either 0 or 1. We consider one local exponent $r \in \mathcal{S}_p(\alpha, \beta)$ and take $r' \in \mathcal{S}_p(\alpha', \beta')$ with $r - r' \in \{0, 1\}$. If

$r = 0$, we pick $r' = 0$ as well. Otherwise, we note that the exponent r' exists, as r is of the form $1 - \beta_j \bmod p$, and we can pick $\beta'_j \in \beta'$ differing from β_j by at most 1 to obtain $r' = 1 - \beta'_j$. It is left to show that the condition on the valuation of $h(\alpha, \beta; r)$ is fulfilled if and only if it is fulfilled for $h(\alpha', \beta'; r')$. According to Lemma 3.1.10, we have

$$v_p(h(\alpha', \beta'; r')) = \sum_{i=0}^{\infty} V' \left(\left\{ \frac{r'}{p^i} \right\}_0, p^i \right),$$

where V' is the function defined in Equation (3.1.2) for the parameters α', β' . By Lemma 3.1.12.(i) we now have for $i > 1$ that

$$V' \left(\left\{ \frac{r'}{p^i} \right\}_0, p^i \right) = 0,$$

since $r'/p^i < 1/p < 1/2d$. For $i = 1$, we observe that $\frac{r'}{p} = \frac{R(\beta'_j, p)}{p} + \frac{1}{p}$ with $\frac{1}{p} < \frac{1}{2d}$. Thus, by Lemma 3.1.12.(ii), we obtain

$$V' \left(\left\{ \frac{r'}{p^i} \right\}_0, p \right) = \mathcal{M}'(\beta'_j \Delta, \Delta),$$

where \mathcal{M}' is defined as in Equation (3.1.1) for the parameters α', β' . Similarly, we obtain

$$V \left(\left\{ \frac{r}{p^i} \right\}_0, p \right) = \mathcal{M}(\beta_j \Delta, \Delta).$$

As the parameters α, β and α', β' differ by integers and there are no integer differences between the parameters α and β , or between α' and β' , the values $\mathcal{M}(\beta_j \Delta, \Delta)$ and $\mathcal{M}'(\beta'_j \Delta, \Delta)$ agree, and thus the p -adic valuations of $h(\alpha', \beta'; r')$ and $h(\alpha, \beta; r)$ are the same as well.

We finally show that $\mathfrak{D}_{p,r'}(\alpha', \beta') = \mathfrak{D}_{p,r}(\alpha, \beta)$. First we note that $\mathfrak{D}_p(\gamma) = \mathfrak{D}_p(\gamma + 1)$ for all $\gamma \in \mathbb{Z}_{(p)}$ if p does not divide γ . By assumption $p > 2d$, and $\alpha_i, \beta_j \in [0, 2]$, so $\mathfrak{D}_p(\alpha_i) = \mathfrak{D}_p(\alpha'_i)$ and $\mathfrak{D}_p(\beta_j) = \mathfrak{D}_p(\beta'_j)$ for all i, j . Last one checks that $(\alpha_i)_r \in p\mathbb{Z}_{(p)}$ if and only if $(\alpha'_i)_{r'} \in p\mathbb{Z}_{(p)}$ and $(\beta_j)_r \in p\mathbb{Z}_{(p)}$ if and only if $(\beta'_j)_{r'} \in p\mathbb{Z}_{(p)}$ for all j .

Indeed, $(\alpha_i)_r \in p\mathbb{Z}_{(p)}$ if and only if $\alpha_i \bmod p \in \{0, p-r+1, \dots, p-1\}$. We distinguish between the four possible combinations of the cases $r = r'$ or $r = r' + 1$ and $\alpha_i = \alpha'_i$ or $\alpha_i = \alpha'_i - 1$. The only problems arise if $\alpha_i + 1 \equiv p - r + 1 \pmod{p}$ or $\alpha_i \equiv 0 \pmod{p}$. In the first case, writing $\alpha_i = a/d$, $\beta_j = b/d$ with $a, b \in [0, d-1]$, this equation is equivalent to $a - b \equiv -d \pmod{p}$, a contradiction. Similarly, the second case can be discarded.

All what precedes concludes the proof of part (1). Further, we notice that $\mathfrak{D}_p(\alpha) = \mathfrak{D}_p(\bar{\alpha})$ and $\mathfrak{D}_p(\beta) = \mathfrak{D}_p(\bar{\beta})$ (see Lemma 3.2.3.(1)) and so the cardinalities of $\mathcal{S}_p(\alpha, \beta)$ and $\mathcal{S}_p(\bar{\alpha}, \bar{\beta})$ agree, as the function \mathcal{M} only depends on $\alpha \bmod \mathbb{Z}$ and $\beta \bmod \mathbb{Z}$. Also, it is clear that $(\bar{\alpha}, \bar{\beta}) \in \mathcal{G}(\alpha, \beta)$, by following the edges corresponding to $r = 0$ in $\mathcal{S}_p(\mathfrak{D}_p^k(\alpha), \mathfrak{D}_p^k(\beta))$ for all k . In combination with what was said before, this shows (2).

By part (2) it suffices to prove claim (3) for α, β between 0 and 1, which we will assume without loss of generality. We claim that whether $r = 1 - \beta_j \bmod p$ is in $\mathcal{S}_p(\alpha, \beta)$ only depends on the congruence class of $p \bmod d$. Indeed, choose Δ with $\Delta p \equiv 1 \pmod{d}$. We have $v_p(h(\alpha, \beta; r)) = \mathcal{M}(\beta_{j(r)} \Delta, \Delta)$ by a combination of Lemmata 3.1.10 and 3.1.12. Here the right-hand side only depends on $p \bmod d$. Also $\mathfrak{D}_p(\alpha)$, $\mathfrak{D}_p(\beta)$ and the value of ℓ_p only depend on the congruence class of $p \bmod d$. Thus, the number of vertices on each level and the number of levels is fixed for each congruence class, according to part (1). Also, by (1), all edges between vertices of two consecutive levels, exist in $\mathcal{G}_p(\alpha, \beta)$. Thus the claim follows.

We finally prove (4). We have seen in the proof of part (1) that the width at level k is equal to the cardinality of $\mathcal{S}_p(\mathfrak{D}_p^{k-1}(\alpha), \mathfrak{D}_p^{k-1}(\beta))$. From the definition of \mathcal{M} (see Equation (3.1.1)), we

find that this quantity equals the number of β_j such that $\mathcal{M}(\Delta^k \beta_j, \Delta^k) = 0$. This proves the first statement.

By Theorem 3.1.3 a hypergeometric function can be reduced modulo p , if and only if it satisfies Christol's interlacing condition for all $\lambda \in \langle p < \text{mod } d \rangle = \langle \Delta \text{ mod } d \rangle$. According to Equation (3.0.3), a basis of solutions at 0 of $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta})y = 0$ is given monomial multiples of $F_{(j)} := {}_nF_{n-1}(\boldsymbol{\alpha}_{(j)}, \boldsymbol{\beta}_{(j)}; x)$, where $\boldsymbol{\alpha}_{(j)} = \boldsymbol{\alpha} + 1 - \beta_j$ and $\boldsymbol{\beta}_{(j)} = \boldsymbol{\beta} + 1 - \beta_j$. Let $\mathcal{M}_{(j)}$ denote the function \mathcal{M} for the sets of parameters $\boldsymbol{\alpha}_{(j)}, \boldsymbol{\beta}_{(j)}$. We have $\mathcal{M}_{(j)}(\cdot, \lambda) = \mathcal{M}(\cdot, \lambda) - \mathcal{M}(\lambda \beta_j, \lambda)$. The solution $F_{(j)}$ can be reduced modulo p if $\mathcal{M}_{(j)}(\cdot, \lambda)$ is always non-negative for all $\lambda \in \langle p \text{ mod } d \rangle$. As $\mathcal{M}(\cdot, \lambda)$ is always non-negative for all λ , but assumes the value 0, this can only be the case if $\mathcal{M}(\lambda \beta_j, \lambda) = 0$. So the number of solutions that can be reduced modulo p is less than the number of b_j such that $\mathcal{M}(\lambda \beta_j, \lambda^k) = 0$ for all $\lambda \in \langle p \text{ mod } p \rangle$, and the claim follows. \square

3.2.3 Finding algebraic relations

We now want to find relations between several reductions of hypergeometric functions modulo a fixed prime number p and combine them to obtain annihilating polynomials for the reduction of a single hypergeometric function. We recall that we have determined in Theorem 3.1.3 the set of prime numbers for which a hypergeometric function can be reduced.

In the language of the hypergeometric relation graph $\mathcal{G}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ introduced above, a modified version of Lemma 8.1 of [Var24], which we will need, reads as follows.

Proposition 3.2.6. *Let $v = (\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathcal{V}_p$. If p does not divide any of the numerators of the elements of $\mathfrak{D}_p(\boldsymbol{\alpha}) \cup \mathfrak{D}_p(\boldsymbol{\beta})$ and if ${}_nF_{n-1}(v; x)$ can be reduced modulo p , then*

$${}_nF_{n-1}(v; x) \equiv \sum_{v \xrightarrow{e} v'} Q(e) \cdot {}_nF_{n-1}(v'; x)^p \pmod{p}.$$

Proof. According to Theorem 3.1.17, the polynomials

$$f_t(x) = \sum_{k=t}^{k_t-1} h(v; k) p^{-v_p(h(v;t))} x^k$$

with $t \in \mathcal{T}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ form a basis of solutions of $\mathcal{H}(v)$ over $\mathbb{F}_p((x^p))$. Since ${}_nF_{n-1}(v; x)$ is a solution that can be reduced modulo p , there exist $g_t \in \mathbb{F}_p((x))$ such that

$${}_nF_{n-1}(v; x) \equiv \sum_{t \in \mathcal{T}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})} f_t(x) \cdot g_t(x^p) \pmod{p}.$$

We recall that, for $r \in \{0, \dots, p-1\}$, we have introduced the section operator

$$\sigma_r : \mathbb{F}_p[[x]] \rightarrow \mathbb{F}_p[[x]], \quad \sum_{n=0}^{\infty} a_n x^n \mapsto \sum_{n=0}^{\infty} a_{pn+r} x^n.$$

Applying σ_t to the previous equality, we obtain

$$\sigma_t({}_nF_{n-1}(v; x)) \equiv \tilde{h}(v; t) \cdot g_t(x) \pmod{p},$$

where, by definition, $\tilde{h}(v; t) = h(v; t) p^{-v_p(h(v;t))} \in \mathbb{Z}_{(p)}^\times$. Besides, it follows from [Var24, Lemma 8.7.(5)] that, for all $t \in \mathcal{T}_p(v)$,

$$\sigma_t({}_nF_{n-1}(v; x)) \equiv h(v; t) \cdot {}_nF_{n-1}(\mathfrak{D}_{p,t}(v); x) \pmod{p}.$$

Comparing these congruences, we find that $g_t(x) = 0$ whenever $h(v; t) \equiv 0 \pmod{p}$, i.e., $t \in \mathcal{T}_p(v) \setminus \mathcal{S}_p(v)$ and $g_t(x) = {}_nF_{n-1}(\mathfrak{D}_{p,t}(v); x)$ otherwise. For $t \in \mathcal{S}_p(v)$, we have $Q(v \rightarrow \mathfrak{D}_{p,t}(v)) = f_t$ and the proposition follows. \square

Remark 3.2.7. Proposition 3.2.6 is connected to the notion of Frobenius preimages we discussed in Subsection 2.3.3. Precisely, a theorem of Kedlaya [Ked22, Theorem 4.1.2] (which is in fact attributed to Dwork in *loc. cit.*) indicates that the hypergeometric equation $\mathcal{H}(\mathfrak{D}_p(\alpha), \mathfrak{D}_p(\beta))$ is the preimage by Frobenius of $\mathcal{H}(\alpha, \beta)$. The relation of Proposition 3.2.6 can be seen as an incarnation modulo p of this property.

Proposition 3.2.6 provides a large set of algebraic relations between hypergeometric series in positive characteristic. We will now combine them in order to find an annihilating polynomial for ${}_nF_{n-1}(\alpha, \beta; x)$.

Theorem 3.2.8. *Let $(\alpha, \beta) \in \mathcal{V}_p$. If $p > 2d \cdot \max\{|\alpha_i| + 1, |\beta_j| + 1\}$ and ${}_nF_{n-1}(\alpha, \beta; x)$ can be reduced modulo p then there exists a relation of the form*

$$A_0(x) {}_nF_{n-1}(\alpha, \beta; x) + \cdots + A_w(x) {}_nF_{n-1}(\alpha, \beta; x)^{q^w} \equiv 0 \pmod{p},$$

where $q = p^{\ell_p(\alpha, \beta)}$, w is the width of the graph $\mathcal{G}_p(\alpha, \beta)$ and the $A_i(x)$ are in $\mathbb{F}_q[x]$ and do not all vanish.

Proof. We use the theory of Frobenius modules (see Definition 2.3.2). We define

$$M := \bigoplus_{v \in \mathcal{G}_p(\alpha, \beta)} \mathbb{F}_p(x) \cdot m_v,$$

where the notation means that the sum runs over the set of vertices v of $\mathcal{G}_p(\alpha, \beta)$. We then turn M into an object of the category $\text{Mod}_{\mathbb{F}_p(x)}^p$ by setting

$$\varphi_M(m_v) = \sum_{v' \xrightarrow{e} v} Q(e) \cdot m_{v'}.$$

To it, is attached the \mathbb{F}_p -linear representation $\mathbf{V}(M)$ of $\text{Gal}(\mathbb{F}_p(x)^{\text{sep}}/\mathbb{F}_p(x))$ defined by Formula (2.3.3). A straightforward computation shows that $\mathbf{V}(M)$ consists of families $(f_v)_{v \in \mathcal{G}_p(\alpha, \beta)}$ of elements of $\mathbb{F}_p(x)^{\text{sep}}$ satisfying the equations

$$f_v = \sum_{v' \xrightarrow{e} v} Q(e) \cdot f_{v'}^p.$$

In particular, Proposition 3.2.6 shows that it contains the family $({}_nF_{n-1}(v; x) \pmod{p})_{v \in \mathcal{G}_p(\alpha, \beta)}$.

On the other hand, M admits a canonical decomposition corresponding to the level partition of the graph $\mathcal{G}_p(\alpha, \beta)$, namely we have

$$M = M_0 \oplus M_1 \oplus \cdots \oplus M_{\ell_p(\alpha, \beta)-1},$$

where the summand M_k corresponds to the vertices of level k . The fact that an edge in $\mathcal{G}_p(\alpha, \beta)$ connects a vertex of level k to a vertex of level $k+1$ implies that φ_M maps M_{k+1} to M_k . It follows that each M_k is stable by the composite $\varphi_M^{\ell_p(\alpha, \beta)}$, which thus defines a structure of q -Frobenius module on this space for $q = p^{\ell_p(\alpha, \beta)}$.

If $\mathcal{G}_p(\alpha, \beta)_0$ denote the set of vertices of $\mathcal{G}_p(\alpha, \beta)$ of level 0, $\mathbf{V}(M_0)$ is a finite dimensional \mathbb{F}_q -representation of $\text{Gal}(\mathbb{F}_q(x)^{\text{sep}}/\mathbb{F}_q(x))$ and we have an inclusion

$$\mathbf{V}(M_0) \subseteq (\mathbb{Q}(x)^{\text{sep}})^{\mathcal{G}_p(\alpha, \beta)_0}$$

commuting with the Galois action. Moreover $\mathbf{V}(M_0)$ contains a vector whose $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ -coordinate is ${}_n F_{n-1}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) \bmod p$. Let then

$$\varpi : (\mathbb{Q}(x)^{\text{sep}})^{\mathcal{G}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})_0} \rightarrow \mathbb{Q}(x)^{\text{sep}}$$

denote the projection on the $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ -coordinate and V be the image of $\mathbf{V}(M_0)$ under ϖ . Clearly V is finite dimensional over \mathbb{F}_q , it is stable by the action of $\text{Gal}(\mathbb{F}_q(x)^{\text{sep}}/\mathbb{F}_q(x))$ and it contains ${}_n F_{n-1}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) \bmod p$. These properties permits to build an annihilating polynomial for ${}_n F_{n-1}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) \bmod p$, namely

$$Z(Y) := \prod_{y \in V} (Y - y).$$

The stability by the Galois action ensures that $Z(Y)$ has coefficients in $\mathbb{F}_q(x)$. Moreover, the fact that V is a \mathbb{F}_q -linear vector space implies that $Z(Y)$ is a q -linearized polynomial, *i.e.*, it has the shape

$$Z(Y) = c_0 Y + c_1 Y^q + \cdots + c_s Y^{q^s} \quad (c_i \in \mathbb{F}_q(x)).$$

By comparing degrees, we find that s is the dimension of V over \mathbb{F}_q .

It then only remains to show that $s \leq w$. For this, we recall that we have introduced in Definition 2.3.7 the *étale part* of a Frobenius module. Applying Theorem 2.3.5 and Lemma 2.3.8, we get

$$s = \dim_{\mathbb{F}_q} V \leq \dim_{\mathbb{F}_q} \mathbf{V}(M_0) = \dim_{\mathbb{F}_q} \mathbf{V}(M_0^{\text{ét}}) = \dim_{\mathbb{Q}(x)} M_0^{\text{ét}}.$$

On the other hand, we observe that φ_M induces a map $M_{k+1}^{\text{ét}} \rightarrow M_k^{\text{ét}}$. We need to be careful that it is not linear but we can actually make it linear by twisting the domain, *i.e.*, we consider

$$\begin{aligned} \psi_k : \mathbb{F}_q(x) \otimes_{\varphi, \mathbb{F}_q(x)} M_{k+1}^{\text{ét}} &\longrightarrow M_k^{\text{ét}} \\ \lambda \otimes m &\longmapsto \lambda \varphi_M(m) \end{aligned}$$

which is now $\mathbb{F}_q(x)$ -linear. Furthermore, the composite of the ψ_k (correctly twisted) is the linearization of $\varphi_M^{\ell_p(\boldsymbol{\alpha}, \boldsymbol{\beta})}$ acting on $M_0^{\text{ét}}$ and hence is an isomorphism by étaleness. We conclude that each ψ_k is itself an isomorphism, which finally leaves up with the inequality

$$\dim_{\mathbb{F}_q(x)} M_0^{\text{ét}} = \min_k \dim_{\mathbb{F}_q(x)} M_k^{\text{ét}}.$$

Let w_k be the width of level k of $\mathcal{G}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$. Under our assumptions on p , it follows from Proposition 3.2.5 that

$$\dim_{\mathbb{F}_q(x)} M_k^{\text{ét}} \leq \dim_{\mathbb{F}_q(x)} M_k = w_k$$

whenever $k > 0$. This estimation also holds for $k = 0$ if the vertex $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ survives in $\mathcal{G}_p(\bar{\boldsymbol{\alpha}}, \bar{\boldsymbol{\beta}})$. On the contrary, if it does not, Proposition 3.2.5 again ensures that there is no edge in $\mathcal{G}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ ending at $(\boldsymbol{\alpha}, \boldsymbol{\beta})$. Consequently, the corresponding vector $m_{(\boldsymbol{\alpha}, \boldsymbol{\beta})}$ cannot be in $M_0^{\text{ét}}$ and we deduce

$$\dim_{\mathbb{F}_q(x)} M_0^{\text{ét}} \leq \dim_{\mathbb{F}_q(x)} M_0 - 1 = w_0.$$

In all cases, we thus have $\dim_{\mathbb{F}_q(x)} M_k^{\text{ét}} \leq w_k$, which finally implies that $s \leq \min_k w_k = w$ as desired. \square

3.2.4 Approaching Galois groups

Our objective is now to reinterpret the previous results along the lines of Conjecture 2.2.6. For this, we need to exhibit a number field whose residue fields are somehow related to the values $\ell_p(\alpha, \beta)$.

In all what follows, our number fields will all be defined as subfields of the field of complex numbers \mathbb{C} . For a positive integer d , we set $\zeta_d = \exp(2i\pi/d) \in \mathbb{C}$; it is a primitive d -th root of unity and it generates the cyclotomic field $\mathbb{Q}(\zeta_d)$. We recall that $\mathbb{Q}(\zeta_d)$ is a Galois extension of \mathbb{Q} and that its Galois group is canonically isomorphic to $(\mathbb{Z}/d\mathbb{Z})^\times$: an element $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$ acts on $\mathbb{Q}(\zeta_d)$ by $\zeta_d \mapsto \zeta_d^\lambda$. In particular, we notice that the element $-1 \in (\mathbb{Z}/d\mathbb{Z})^\times$ acts as complex conjugation.

As before, we let d be the smallest common denominator of all the parameters α and β . Further we define the group

$$D(\alpha, \beta) := \{ \lambda \in (\mathbb{Z}/d\mathbb{Z})^\times : \lambda \cdot \alpha \equiv \alpha \pmod{\mathbb{Z}} \text{ and } \lambda \cdot \beta \equiv \beta \pmod{\mathbb{Z}} \text{ as sets} \}.$$

We can map $D(\alpha, \beta)$ to a product of symmetric groups. Precisely, let $\mathfrak{S}(\alpha)$ (resp. $\mathfrak{S}(\beta)$) be the group of bijections of α (resp. β) viewed as a multiset. We then have a group morphism $\sigma : D(\alpha, \beta) \rightarrow \mathfrak{S}(\alpha) \times \mathfrak{S}(\beta)$ that takes λ to the multiplication by λ .

Lemma 3.2.9. *The morphism σ is injective.*

Proof. We write $\alpha_i = \frac{a_i}{d}$, $\beta_i = \frac{b_i}{d}$. By definition of d , we have $\gcd(a_1, \dots, a_n, b_1, \dots, b_{n-1}, d) = 1$ as otherwise the fractions $\frac{a_i}{d}$ and $\frac{b_i}{d}$ could all be simplified by a common factor, which is excluded. By Bézout's theorem, there exist integers $u_1, \dots, u_n, v_1, \dots, v_{n-1}, w$ such that

$$u_1 a_1 + \dots + u_n a_n + v_1 b_1 + \dots + v_{n-1} b_{n-1} + wd = 1.$$

We now assume that we are given $\lambda, \mu \in D(\alpha, \beta)$ such that $\sigma(\lambda) = \sigma(\mu)$. Then, following the definition, we find that $\lambda a_i \equiv \mu a_i \pmod{d}$ and $\lambda b_i \equiv \mu b_i \pmod{d}$ for all i . Weighting these congruences with the coefficients u_i and v_i and summing them, we get

$$\begin{aligned} \lambda \cdot (u_1 a_1 + \dots + u_n a_n + v_1 b_1 + \dots + v_{n-1} b_{n-1}) \\ \equiv \mu \cdot (u_1 a_1 + \dots + u_n a_n + v_1 b_1 + \dots + v_{n-1} b_{n-1}) \pmod{d} \end{aligned}$$

which finally reduces to $\lambda \equiv \mu \pmod{d}$. □

Definition 3.2.10. We define $K(\alpha, \beta)$ as the subextension of $\mathbb{Q}(\zeta_d)$ corresponding to $D(\alpha, \beta)$ via Galois correspondence.

In concrete terms, $K(\alpha, \beta) := \mathbb{Q}(\zeta_d)^{D(\alpha, \beta)}$. The field $K(\alpha, \beta)$ is undoubtedly the number field we are looking for, as we shall demonstrate in the sequel. First of all, we observe that it is closely related to the Galois group of the hypergeometric differential equation in characteristic zero. Indeed, it is the subfield generated by the entries of the monodromy matrices exhibited in Theorem 3.1.9 and we know that those matrices generate the differential Galois group as an algebraic group.

Now, we make the connection between the field $K(\alpha, \beta)$ and the numbers $\ell_p(\alpha, \beta)$, which will eventually relate $K(\alpha, \beta)$ to the Galois groups of the reduction of the hypergeometric series ${}_nF_{n-1}(\alpha, \beta; x)$ modulo the primes.

Proposition 3.2.11. *Let p be a prime number which does not divide d , and let \mathfrak{p} be a prime in $K(\alpha, \beta)$ above p . Then the residue field of $K(\alpha, \beta)$ at \mathfrak{p} has degree $\ell_p(\alpha, \beta)$ over \mathbb{F}_p .*

Proof. Throughout the proof, we omit the parameter (α, β) in the notation and simply write K and ℓ_p for $K(\alpha, \beta)$ and $\ell_p(\alpha, \beta)$ respectively. The assumption on p implies that p is not ramified in the extension $\mathbb{Q}(\zeta_d)/\mathbb{Q}$. Let \mathfrak{q} be a prime of $\mathbb{Q}(\zeta_d)$ above \mathfrak{p} and write $k_{\mathfrak{p}}$ (resp. $k_{\mathfrak{q}}$) for the residue field of K at \mathfrak{p} (resp. of $\mathbb{Q}(\zeta_d)$ at \mathfrak{q}). The Galois group of the extension $k_{\mathfrak{q}}/\mathbb{F}_p$ is the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p ; we call it P . Since K is defined as the fixed subfield by D , we deduce that $k_{\mathfrak{p}}$ is the subfield of $k_{\mathfrak{q}}$ fixed by $P \cap D$. Thus

$$\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) = P/(D \cap P).$$

Besides the cardinality of $P/(D \cap P)$ is the smallest positive integer e such that $p^{-e} \in D$. The latter condition is equivalent to the statement “ $\mathfrak{D}^e(\alpha) = \alpha$ and $\mathfrak{D}^e(\beta) = \beta$ ” given that, according to Lemma 3.2.1.(2), the Dwork map acts by division by p on $\mathbb{Z}_{(p)}/\mathbb{Z}$. Comparing with the definition of ℓ_p , we find that $P/(D \cap P)$ has cardinality ℓ_p , which concludes the proof. \square

Theorem 3.2.12. *Let p be a prime number with $p > 2d \cdot \max\{|\alpha_i| + 1, |\beta_j| + 1\}$ and let \mathfrak{p} be a prime in $K(\alpha, \beta)$ above p . Then*

$$\mathrm{Gal}({}_n F_{n-1}(\alpha, \beta; x) \mid k_{\mathfrak{p}}(x)) \subseteq \mathrm{GL}_w(k_{\mathfrak{p}})$$

where w denotes the width of the graph $\mathcal{G}_p(\alpha, \beta)$.

Proof. By Proposition 3.2.11, we have $k_{\mathfrak{p}} \simeq \mathbb{F}_{p^{\ell_p(\alpha, \beta)}}$. With this, the theorem follows from Theorem 3.2.8. \square

We conclude this section by looking at some examples we already considered in Section 2.

Example 3.2.13. We recall the example from Subsection 2.1.4:

$$f(x) = \sum_{n=0}^{\infty} \binom{2n}{n}^3 \cdot x^n = {}_3F_2\left(\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right), (1, 1); 64x\right).$$

Clearly $\ell_p(\alpha, \beta) = 1$ for all prime numbers p , as $(\mathbb{Z}/2\mathbb{Z})^\times$ is trivial. Moreover, as all bottom parameters are equal to 1, it follows from Example 3.2.4 that the width w of the graph is 1, and consequently, the Galois group $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$ embeds into \mathbb{F}_p^\times . This agrees with the *ad-hoc* arguments deployed in Subsection 2.1.4. However, we cannot provide a systematic argument explaining the dichotomy of the Galois groups exhibited in Equation (2.1.5) here.

Example 3.2.14. We now consider the example $f(x) = {}_3F_2\left(\left(\frac{1}{9}, \frac{4}{9}, \frac{5}{9}\right), \left(\frac{1}{3}, 1\right); x\right)$ from Subsection 2.1.6. We have seen in Example 3.1.8 that $f(x)$ is globally bounded. An easy computation shows that $\ell_p(\alpha, \beta) = \ell_p = \mathrm{ord}_9(p)$ and these values are given by

$$\ell_p = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{9} \\ 2 & \text{if } p \equiv 8 \pmod{9} \\ 3 & \text{if } p \equiv 4, 7 \pmod{9} \\ 6 & \text{if } p \equiv 2, 5 \pmod{9} \end{cases}$$

We next discuss the width of the graphs $\mathcal{G}_p(\alpha, \beta)$. In Figure 3, we see that, for $\lambda = 2, 5, 8$, we have $\mathcal{M}(\lambda^k \beta_j, \lambda^k) = 0$ only for $\beta_j = 1$ and, for $\lambda = 1, 4, 7$, the equation also holds for $\beta_j = \frac{1}{3}$. We have $\langle p \bmod 9 \rangle \subseteq \{1, 4, 7\}$ if and only if $p \equiv 1, 4, 7$. This shows that the width w of the graph is 2 in the first case and 1 in the second case. By Theorem 3.2.12, we conclude that $\mathrm{Gal}(f(x) \mid \mathbb{F}_q(x))$ embeds into $\mathrm{GL}_w(\mathbb{F}_q)$, where $q = p^{\ell_p(\alpha, \beta)}$. If we pass to $\mathrm{Gal}(f(x) \mid \mathbb{F}_p(x))$ we have additionally the Frobenius morphism acting. Altogether, this shows that the Galois groups of $f(x)$ over $\mathbb{F}_p(x)$ embed into the semidirect products given in Equation (2.1.11). We cannot make any statement about the index or precise nature of the subgroup with the techniques developed here, although we conjecture equality for all prime numbers based on computer experiments.

3.3 The case of Gaussian hypergeometric functions

We now consider the case of Gaussian hypergeometric functions with bottom parameter 1, that are functions of the form ${}_2F_1(\boldsymbol{\alpha}, (1); x)$ with $\boldsymbol{\alpha} = (\alpha_1, \alpha_2) \in \mathbb{Q}^2$ and $\boldsymbol{\beta} = (1)$. While this is an extremely particular case of globally bounded D -finite functions, already for such function an astonishing amount of nontrivial phenomena occur. We present strong evidence towards an affirmative answer to Conjecture 2.2.6 (and its refinements) in this case.

Throughout this subsection, the letter p refers to a prime number which is coprime with d . For simplicity, we will often omit the parameter $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ in the notation when no confusion can occur; for example, we shall simply write ℓ_p for $\ell_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and similarly, we set $D := D(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and $K := K(\boldsymbol{\alpha}, \boldsymbol{\beta})$. By Lemma 3.2.9, the group D has cardinality at most 2, *i.e.*, $D = \{1, \lambda\}$ with $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$, $\lambda^2 = 1$. We also define $e_p := \ell_p/2$.

3.3.1 Estimating the Galois group

We know from Example 3.2.4 that, in our case of interest, the graph $\mathcal{G}_p(\boldsymbol{\alpha}, \boldsymbol{\beta})$ has the ρ -shape drawn in Figure 6. Let $(\boldsymbol{\alpha}_k, (1))$ denote the parameter corresponding to the vertex of level k in the circle part, *i.e.*, $\boldsymbol{\alpha}_k = \mathfrak{D}_p^{k'}(\boldsymbol{\alpha})$ where k' is large enough and congruent to k modulo ℓ_p . Let also $H_k(x)$ denote the reduction modulo p of the hypergeometric series attached to the parameters $(\boldsymbol{\alpha}_k, (1))$. Similarly we define $B_k(x)$ as the truncation at x^p of $H_k(x) \bmod p$; thus $B_k(x)$ is a polynomial of degree less than p with coefficients in \mathbb{F}_p . Proposition 3.2.6 ensures that

$$H_k(x) \equiv B_k(x) \cdot H_{k+1}^p(x). \quad (3.3.1)$$

Combining these equations, we get the relation $H_0(x) = A(x) \cdot H_0(x)^q$ where $q = p^{\ell_p}$ and

$$A(x) = B_0(x) \cdot B_1(x)^p \cdots B_{\ell_p-1}(x)^{p^{\ell_p-1}}. \quad (3.3.2)$$

Similarly, we find that there exist a polynomial $\tilde{A}(x) \in \mathbb{F}_q[x]$ and a nonnegative integer m such that ${}_2F_1(\boldsymbol{\alpha}, (1); x) = \tilde{A}(x)H_0(x)^{q^m}$. We observe moreover that the relation

$${}_2F_1(\boldsymbol{\alpha}, (1); x) \equiv \tilde{A}(x)H_0(x)^{q^m} = \tilde{A}(x) \cdot A(x)^{1+q+\cdots+q^{m-1}} H_0(x) \pmod{p}$$

indicates that the functions ${}_2F_1(\boldsymbol{\alpha}, (1); x)$ and $H_0(x)$ generate the same extension over $k_p(x)$. In other words, we can assume without loss of generality that the parameters α_1 and α_2 are both in the interval $(0, 1]$, *i.e.*, $H_0(x) = {}_2F_1(\boldsymbol{\alpha}, (1); x) \bmod p$.

Besides, if α_1 or α_2 is equal to 1, the hypergeometric series ${}_2F_1(\boldsymbol{\alpha}, (1); x)$ is equal to $(1-x)^{-\alpha}$ (where α is the value of the other parameter), a case we already covered in Subsection 2.1.1. Therefore, from now on, we suppose $\alpha_1, \alpha_2 \in (0, 1)$.

The Galois groups we are interested in can be computed using Kummer theory.

Proposition 3.3.1. *Let \mathfrak{p} be a prime of K above p . The Galois group $\text{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \mid k_{\mathfrak{p}}(x))$ naturally embeds in $k_{\mathfrak{p}}^\times$ and hence is a cyclic group. Moreover, its order is*

$$\frac{q-1}{\gcd(r, q-1)}$$

where r denotes the largest integer such that $A(x)$ is r -th power in $k_{\mathfrak{p}}(x)$.

Proof. By what precedes, we know that $H_0(x)$ is a $(q-1)$ -th root of the polynomial $A(x) \in \mathbb{F}_p[x] \subseteq k_{\mathfrak{p}}(x)$. Since $k_{\mathfrak{p}}$ contains all the $(q-1)$ -th roots of unity, Kummer's theory tells us that $\text{Gal}(H_0(x) \mid k_{\mathfrak{p}}(x))$ embeds into $\mu_{q-1}(k_{\mathfrak{p}}(x)) = k_{\mathfrak{p}}^\times$ and that its order is $\frac{q-1}{\gcd(r, q-1)}$. \square

After Proposition 3.3.1, we are led to determine when $A(x)$ is a perfect power. In general, we do not expect this to occur, although it could happen “by accident.” There is, however, one important case where this happens systematically, namely in the case when ℓ_p is even and $-p^{e_p} \in D$.

In all what follows, if $\gamma \in \mathbb{Z}_{(p)}$, we let $\gamma^{(0)}, \gamma^{(1)}, \dots$ denote the “digits” of the p -adic integer $(-\gamma)$, i.e., $\gamma^{(k)} \in \{0, \dots, p-1\}$ for all k and the following expansion

$$-\gamma = \gamma^{(0)} + p\gamma^{(1)} + p^2\gamma^{(2)} + \dots$$

holds in the ring of p -adic integers. When $\gamma = (\gamma_1, \gamma_2)$, we also let $B(\gamma; x) \in \mathbb{F}_p[x]$ be the truncation at x^p of ${}_2F_1(\gamma, (1); x) \bmod p$. By definition, we thus have $B_k(x) = B(\alpha_k; x)$.

Lemma 3.3.2. *Let $\gamma = (\gamma_1, \gamma_2) \in (\mathbb{Z}_{(p)} \cap (0, 1))^2$. Then*

$$\begin{aligned} \deg B(\gamma; x) &= \min(\gamma_1^{(0)}, \gamma_2^{(0)}), \\ \deg B(1 - \gamma; x) &= p - 1 - \max(\gamma_1^{(0)}, \gamma_2^{(0)}). \end{aligned}$$

Moreover, we have the relation

$$B(\gamma; x) = (1 - x)^{\gamma_1^{(0)} + \gamma_2^{(0)} - (p-1)} \cdot B(1 - \gamma; x). \quad (3.3.3)$$

Proof. Set $\delta = \min(\gamma_1^{(0)}, \gamma_2^{(0)})$. By definition, the coefficient of x^r for $r < p$ in $B(\gamma; x)$ is $\frac{(\gamma_1)_r (\gamma_2)_r}{(r!)^2}$. Hence it vanishes modulo p if and only if the numerator does. When $r > \delta$, the numerator contains the factor $(\gamma_1 + \delta) \cdot (\gamma_2 + \delta)$, and so it vanishes modulo p . On the contrary, when $r = \delta$, we have

$$(\gamma_1)_r (\gamma_2)_r = \gamma_1(\gamma_1 + 1) \cdots (\gamma_1 + \delta - 1) \cdot \gamma_2(\gamma_2 + 1) \cdots (\gamma_2 + \delta - 1),$$

and, again by definition of δ , none of the above factors vanish. We conclude that $B(\gamma; x)$ has degree δ , as claimed. The second statement on the degree of $B(1 - \gamma; x)$ is proved similarly.

Thanks to Euler’s transformation, we know that

$${}_2F_1(\gamma, (1); x) = (1 - x)^{1 - \gamma_1 - \gamma_2} \cdot {}_2F_1(1 - \gamma, (1); x).$$

We now note that the exponent $1 - \gamma_1 - \gamma_2$ is congruent to $\gamma_1^{(0)} + \gamma_2^{(0)} - (p - 1)$ modulo p . Therefore,

$$B(\gamma; x) \equiv (1 - x)^{\gamma_1^{(0)} + \gamma_2^{(0)} - (p-1)} \cdot B(1 - \gamma; x) \pmod{x^p}.$$

If $\gamma_1^{(0)} + \gamma_2^{(0)} \geq p - 1$, both sides are polynomials of degree at most p , and we can conclude that they are indeed equal. On the contrary, when $\gamma_1^{(0)} + \gamma_2^{(0)} \leq p - 1$, we rewrite the above congruence as

$$B(1 - \gamma; x) \equiv (1 - x)^{(p-1) - \gamma_1^{(0)} - \gamma_2^{(0)}} \cdot B(\gamma; x) \pmod{x^p}$$

and we conclude similarly. \square

We introduce one more numerical invariant attached to the situation; it is the integer m defined by

$$m := \frac{d}{\gcd(d, a_1 + a_2)}$$

where we have written $\alpha_i = a_i/d$ for $i = 1, 2$. We note that m is also the denominator of the irreducible fraction representing $\alpha_1 + \alpha_2$.

Proposition 3.3.3. *We assume that ℓ_p is even and that $-p^{e_p} \in D$. Then*

$$A(x) = (1-x)^{(1+p^{e_p})(1-\alpha_1-\alpha_2)} \left(B_{e_p} B_{e_p+1} \cdots B_{\ell_p-1}^{p^{e_p-1}} \right)^{1+p^{e_p}}.$$

It is a perfect power with exponent $\frac{1+p^{e_p}}{m}$.

Proof. We recall from Lemma 3.2.1.(2) that the Dwork operator \mathfrak{D}_p acts by division by p on $\mathbb{Z}_{(p)}/\mathbb{Z}$. The assumption of the proposition then tells us that $\mathfrak{D}_p^{e_p}(\alpha) \equiv -\alpha \pmod{\mathbb{Z}}$, which implies more generally $\mathfrak{D}_p^{e_p+k}(\alpha) \equiv -\mathfrak{D}_p^k(\alpha) \pmod{\mathbb{Z}}$ for all k . Since our parameters are all in $(0, 1)$, we deduce that $\mathfrak{D}_p^{e_p+k}(\alpha) = 1 - \mathfrak{D}_p^k(\alpha)$. On the other hand, we recall from Lemma 3.2.1 that $\mathfrak{D}_p^k(\gamma)^{(0)} = \gamma^{(k)}$ for all k . Hence, Lemma 3.3.2 gives

$$B_k(x) = (1-x)^{\alpha_1^{(k)} + \alpha_2^{(k)} - (p-1)} B_{k+e_p}(x).$$

Coming back to the definition of $A(x)$, we find

$$\begin{aligned} A(x) &= \prod_{k=0}^{\ell_p-1} B_k(x)^{p^k} = \prod_{k=0}^{e_p-1} (1-x)^{p^k(\alpha_1^{(k)} + \alpha_2^{(k)} - (p-1))} B_{k+e_p}(x)^{p^k + p^{k+e_p}} \\ &= (1-x)^v \cdot \left(\prod_{k=0}^{e_p-1} B_{k+e_p}(x)^{p^k} \right)^{1+p^{e_p}}, \end{aligned}$$

where the exponent v is given by $v = \sum_{k=0}^{e_p-1} p^k u_k$ with $u_k = \alpha_1^{(k)} + \alpha_2^{(k)} - (p-1)$. Now, we remark that, for $\gamma \in \mathbb{Z}_{(p)}$, we have

$$-(1-\gamma) = -1 - \sum_{m=0}^{\infty} p^m \gamma^{(m)} = \sum_{m=0}^{\infty} p^m (p-1 - \gamma^{(m)}),$$

implying that $(1-\gamma)^{(m)} = p-1 - \gamma^{(m)}$ for all $m \in \mathbb{N}$. Applying this result with $\gamma = \mathfrak{D}_p^k(\alpha_i)$ ($i \in \{1, 2\}$) and remembering that $\mathfrak{D}_p^{e_p+k}(\alpha) = 1 - \mathfrak{D}_p^k(\alpha)$, we conclude that $u_{e_p+k} = -u_k$. Weighting by p^k and summing over k (and doing the computation in the ring of p -adic integers), we find

$$\sum_{k=0}^{\infty} p^k u_k = \left(\sum_{k'=0}^{\infty} (-1)^{k'} p^{e_p k'} \right) \cdot \left(\sum_{k=0}^{e_p-1} p^k u_k \right) = \frac{1}{1+p^{e_p}} \sum_{k=0}^{e_p-1} p^k u_k.$$

On the other hand, coming back to the definition, we have

$$\sum_{k=0}^{\infty} p^k u_k = \sum_{k=0}^{\infty} p^k (\alpha_1^{(k)} + \alpha_2^{(k)} - (p-1)) = 1 - \alpha_1 - \alpha_2.$$

Hence, we conclude that $v = (1+p^{e_p}) \cdot (1 - \alpha_1 - \alpha_2)$ and the first part of the proposition is proved.

We write $\alpha_1 + \alpha_2 = a/m$ with a coprime with m . We thus have

$$v = \frac{(1+p^{e_p})(m-a)}{m}.$$

Since $m-a$ is coprime with m , we deduce that m divides $1+p^{e_p}$ and then that v is a multiple of $r := \frac{1+p^{e_p}}{m}$. Given that $(1+p^{e_p})$ is also obviously a multiple of r , we conclude that $A(x)$ is a r -th power. \square

As a conclusion, we have proved the following.

Corollary 3.3.4. *Let \mathfrak{p} be a prime of K above p . The Galois group $\text{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \mid k_{\mathfrak{p}}(x))$ embeds in $k_{\mathfrak{p}}^{\times}$ and hence is a cyclic group. Moreover, if ℓ_p is even and $-p^{e_p} \in D$, its cardinality divides $(p^{e_p} - 1) \cdot m$*

3.3.2 Uniformizing the Galois groups

We now aim at finding a common origin of the Galois groups given by Corollary 3.3.4 in the terms of Conjecture 2.2.6. For this, we shall consider several subgroups of $\text{GL}_1(K) = K^{\times}$. The first one is $\boldsymbol{\mu}_m(K)$, the group of m -th roots of unity in K . The following lemma ensures that K contains all m -th roots of unity, meaning that $\boldsymbol{\mu}_m(K)$ is a cyclic group of cardinality m .

Lemma 3.3.5. *We have $\zeta_m \in K$.*

Proof. It follows immediately from the definition that m divides d . Hence $\zeta_m \in \mathbb{Q}(\zeta_d)$ and it is enough to prove that $\zeta_m = \zeta_m^{\lambda}$ for any $\lambda \in D$. Let $\lambda \in D$. By definition, the multiplication by λ induces a permutation of $\{\alpha_1, \alpha_2\}$ modulo \mathbb{Z} . Thus

$$\lambda \cdot (a_1 + a_2) \equiv a_1 + a_2 \pmod{d}$$

and we conclude that $\lambda \equiv 1 \pmod{m}$. The lemma follows. \square

The second subgroup of $\text{GL}_1(K)$ that will play a major role in what follows is the group $\text{GL}_1(K^+)$ where $K^+ := K \cap \mathbb{R}$. Since the complex conjugacy is represented by the element $-1 \in (\mathbb{Z}/d\mathbb{Z})^{\times}$, we deduce that K^+ is the subfield of $\mathbb{Q}(\zeta_d)$ cutted out by the subgroup

$$D^+ := D \cdot \{\pm 1\} \subseteq (\mathbb{Z}/d\mathbb{Z})^{\times}.$$

Definition 3.3.6. We define the subgroup G of $\text{GL}_1(K)$ by

$$G := \begin{cases} \text{GL}_1(K) & \text{if } K = K^+ \\ \text{GL}_1(K^+) \cdot \langle \xi - \bar{\xi} \rangle & \text{if } K \neq K^+ \text{ and } m = 2 \\ \text{GL}_1(K^+) \cdot \langle 1 + \zeta_m \rangle & \text{if } K \neq K^+ \text{ and } m \neq 2 \end{cases}$$

where ξ is an element of $K \setminus K^+$ and $\bar{\xi}$ is its complex conjugate.

Remark 3.3.7. The reason why the definition is slightly different when $m = 2$ comes simply from the fact that $1 + \zeta_m$ vanishes in this case. We notice moreover that, as soon as $\xi \in K \setminus K^+$, the element $\xi - \bar{\xi}$ is a nonzero real multiple of $\mathbf{i} \in \mathbb{C}$. The group $\text{GL}_1(K^+) \cdot \langle \xi - \bar{\xi} \rangle$ is then the subgroup

$$(K^{\times} \cap \mathbb{R}) \sqcup (K^{\times} \cap \mathbb{R}\mathbf{i}) \subseteq K^{\times}.$$

In particular, it does not depend on the choice of ξ , and so Definition 3.3.6 is not ambiguous.

We are going to prove that the group G fulfills the requirements of Conjecture 2.2.6. We start by a lemma that reformulates the condition of Corollary 3.3.4 in more abstract terms.

Lemma 3.3.8. *Let \mathfrak{p} be a prime in K above p and let $k_{\mathfrak{p}}$ (resp. $k_{\mathfrak{p}}^+$) denote the residue field of K (resp. K^+) at \mathfrak{p} . The extension $k_{\mathfrak{p}}/k_{\mathfrak{p}}^+$ is nontrivial if and only if ℓ_p is even and $-p^{e_p} \in D$. Moreover, when this occurs, it has degree 2.*

Proof. Let P denote the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p . We know from the proof of Proposition 3.2.11 that $\text{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) = P/(D \cap P)$, and similarly one proves that $\text{Gal}(k_{\mathfrak{p}}^+/\mathbb{F}_p) = P/(D^+ \cap P)$. Hence the extension $k_{\mathfrak{p}}/k_{\mathfrak{p}}^+$ is trivial if and only if

$$D \cap P = D^+ \cap P. \quad (3.3.4)$$

If $-1 \in D$, we have $D = D^+$ and the condition (3.3.4) is obviously satisfied. On the other hand, still assuming that $-1 \in D$, the condition $-p^{e_p} \in D$ is equivalent to $p^{e_p} \in D$, which cannot be true by minimality of ℓ_p . The equivalence stated in the lemma is then proved in this case.

We now assume that $-1 \notin D$. Then D^+ is the disjoint union of D and $(-D)$, from what we deduce that the condition (3.3.4) is equivalent to the fact that P does not meet $(-D)$. Clearly, if $-p^{e_p} \in D$, then P meets $(-D)$. Conversely, let us assume that $P \cap (-D) = \emptyset$, i.e., that there exists an exponent $e \in \mathbb{N}$ such that $-p^e \in D$. Then $p^{2e} \in D$ and it follows that $2e$ needs to be a multiple of ℓ_p : there exists an integer n such that $2e = n\ell_p$. Necessarily n has to be odd because otherwise, we would deduce that ℓ_p divides e and, consequently, that $p^e \in D$; this cannot be true given that $-p^e \in D$ and $-1 \notin D$ by assumption. It follows that ℓ_p is even. Now, writing $n = 2n' + 1$, we get $p^e = p^{n'\ell_p + e_p} \equiv p^{e_p} \pmod{d}$ and so $-p^{e_p} \in D$.

Finally, the fact that $k_{\mathfrak{p}}/k_{\mathfrak{p}}^+$ has degree at most 2 follows from the fact that $D \cap P$ has index at most 2 in $D^+ \cap P$. \square

Following Conjecture 2.2.6, for any place \mathfrak{p} of K , we set

$$G_{\mathfrak{p}} := \text{image}(G \cap \text{GL}_1(\mathcal{O}_{(\mathfrak{p})}) \longrightarrow \text{GL}_1(k_{\mathfrak{p}})) \quad (3.3.5)$$

where $\mathcal{O}_{(\mathfrak{p})}$ denotes the localization of the ring of integers of K at \mathfrak{p} and $k_{\mathfrak{p}} = \mathcal{O}_{(\mathfrak{p})}/\mathfrak{p}\mathcal{O}_{(\mathfrak{p})}$ is the residue field.

Proposition 3.3.9. *Let \mathfrak{p} be a prime ideal above p . Then $G_{\mathfrak{p}}$ is equal to $\text{GL}_1(k_{\mathfrak{p}})$ if ℓ_p is odd or $-p^{e_p} \notin D$; otherwise, it is its cyclic subgroup of order $(p^{e_p} - 1) \cdot m$.*

Proof. We only write the proof when $m \neq 2$, the case $m = 2$ being treated in a similar fashion.

To start with, we observe that G contains $\mu_m(K)$, which follows from writing

$$\zeta_m = (\zeta_m + 1)^2 \cdot (\zeta_m + \zeta_m^{-1} + 2)^{-1}$$

and noticing that the second factor lies in $\text{GL}_1(K^+)$ since it is invariant under the transformation $\zeta_m \mapsto \zeta_m^{-1}$. Therefore, we equally have $G = \text{GL}_1(K^+) \cdot H$ with $H := \mu_m(K) \cdot \langle 1 + \zeta_m \rangle$. We note that the former equality also holds when $K = K^+$ since $G = \text{GL}_1(K)$ in this case.

We now compute the intersection $G \cap \text{GL}_1(\mathcal{O}_{(\mathfrak{p})})$. Given that p is coprime with d , and hence with m , Hensel's lemma ensures that the morphism $\mu_m(K) \rightarrow \mu_m(k_{\mathfrak{p}})$ is an isomorphism. Thus ζ_m , which is a generator of $\mu_m(K)$, reduces modulo \mathfrak{p} to a generator of $\mu_m(k_{\mathfrak{p}})$. Therefore $1 + \zeta_m$ does not vanish in $k_{\mathfrak{p}}$. This shows that the group H sits inside $\text{GL}_1(\mathcal{O}_{(\mathfrak{p})})$ and, consequently, that $G \cap \text{GL}_1(\mathcal{O}_{(\mathfrak{p})}) = \text{GL}_1(\mathcal{O}_{(\mathfrak{p})}^+) \cdot H$ where $\mathcal{O}_{(\mathfrak{p})}^+$ is the localization at \mathfrak{p} of the ring of integers of K^+ . Reducing modulo \mathfrak{p} , we finally find

$$G_{\mathfrak{p}} = \text{GL}_1(k_{\mathfrak{p}}^+) \cdot H_{\mathfrak{p}}$$

where $H_{\mathfrak{p}}$ is the reduction of H modulo \mathfrak{p} .

When ℓ_p is odd or $-p^{e_p} \notin D$, Lemma 3.3.8 shows that $k_{\mathfrak{p}} = k_{\mathfrak{p}}^+$ and so $G_{\mathfrak{p}} = \text{GL}_1(k_{\mathfrak{p}})$ as claimed.

We now consider the case where ℓ_p is even and $-p^{e_p} \in D$. Applying Lemma 3.3.8 again, we find that the cardinality of $\text{GL}_1(k_{\mathfrak{p}}^+)$ is $p^{e_p} - 1$ and so the cardinality of the quotient $\text{GL}_1(k_{\mathfrak{p}})/\text{GL}_1(k_{\mathfrak{p}}^+)$

is $p^{e_p} + 1$. Moreover, both of these groups are cyclic. We then reduced to prove that the image of H_p in $\mathrm{GL}_1(k_p)/\mathrm{GL}_1(k_p^+)$ has cardinality m . For this, we observe that the kernel of $\mu_m(k_p) \rightarrow \mathrm{GL}_1(k_p)/\mathrm{GL}_1(k_p^+)$ is $\mu_m(k_p^+)$, which is a cyclic group of order $\gcd(m, p^{e_p} - 1) = \gcd(m, 2)$ because m divides $p^{e_p} + 1$.

By what precedes, it is enough to show that the order of $1 + \zeta_m$ in the quotient group $\mathrm{GL}_1(k_p)/\mathrm{GL}_1(k_p^+)\mu_m(k_p)$ is 1 when m is odd and 2 when m is even. For this, we first notice that

$$(\zeta_m + 1)^2 = \zeta_m \cdot (\zeta_m + \zeta_m^{-1} + 2) \in \mathrm{GL}_1(k_p^+)\mu_m(k_p)$$

since the first factor is in $\mu_m(k_p)$ and the second factor lies in k_p^+ . Hence the order of $1 + \zeta_m$ is 1 or 2. Now, we observe that $1 + \zeta_m$ lies in $\mathrm{GL}_1(k_p^+)\mu_m(k_p)$ if and only if there exists an integer a such that $\zeta_m^a(1 + \zeta_m)$ is invariant by the transformation $\zeta_m \mapsto \zeta_m^{-1}$. After simplification, this further reduces to $\zeta_m^{2a+1} = 1$. When m is odd, such an element a obviously exists (we can take $a = \frac{m-1}{2}$). On the contrary, when m is even, it does not exist because ζ_m has order m in $\mathrm{GL}_1(k_p^+)$ and m cannot divide the odd number $2a + 1$. \square

Combining Proposition 3.3.9 with Corollary 3.3.4, we get the first part of Theorem 1.2 of the introduction.

3.3.3 Approaching the Galois group from below

Up until now, we have only bounded the Galois groups of reductions of hypergeometric series from above. We now develop also bounds from below, that will eventually give a complete proof of Theorem 1.2.

We recall from Proposition 3.3.1 that the order of the Galois group of $\mathrm{Gal}({}_2F_1(\alpha, 1; x) \mid k_p(x))$ with $\alpha = (\alpha_1, \alpha_2)$ is given by

$$\frac{q-1}{\gcd(r, q-1)},$$

where $q = p^{\ell_p}$ and r is the largest integer such that the polynomials $A(x)$ introduced in Equation (3.3.2), is a perfect r -th power. To estimate r , we rely on the fact that r must divide the valuation of $A(x)$ at any point, and also its degree (*i.e.*, its valuation at infinity).

Valuation at singular points. The degree, which we denote by ν_∞ , has been already essentially computed in Subsection 3.3.1. Precisely, we recall from there that $B_k(x)$ is defined as the truncation at x^p of ${}_2F_1(\mathfrak{D}_p^k(\alpha), 1; x) \bmod p$. Then, Lemma 3.3.2 shows that $B_k(x)$ has degree $\min(\alpha_1^{(k)}, \alpha_2^{(k)})$, where $\alpha_i^{(k)}$ denotes the k -th digit in the p -adic expansion of $-\alpha_i$ for $i \in \{1, 2\}$. Therefore

$$\nu_\infty = \sum_{k=0}^{\ell_p-1} \min(\alpha_1^{(k)}, \alpha_2^{(k)}) \cdot p^k. \quad (3.3.6)$$

The valuation at 1 of $A(x)$ can be computed similarly. As in Subsection 3.3.1, we write $B(\gamma; x)$ for the truncation of ${}_2F_1(\gamma, 1; x) \bmod p$ at x^p .

Lemma 3.3.10. *Let $\gamma = (\gamma_1, \gamma_2) \in (\mathbb{Z}_{(p)} \cap (0, 1))^2$. Then*

$$\mathrm{val}_1(B(\gamma; x)) = \max(0, \gamma_1^{(0)} + \gamma_2^{(0)} - p + 1)$$

where val_1 denotes the valuation at 1.

Proof. We know from Lemma 3.3.2 that

$$B(\gamma; x) = (1-x)^{\gamma_1^{(0)} + \gamma_2^{(0)} - p + 1} \cdot B(1-\gamma; x).$$

Without loss of generality, we assume that $\gamma_1^{(0)} + \gamma_2^{(0)} \geq p-1$; otherwise we exchange the roles of γ and $1-\gamma$. The local exponents at 1 of $\mathcal{H}(\gamma, (1)) \bmod p$ are 0 and $\gamma_1^{(0)} + \gamma_2^{(0)} - p - 1$, while that of $\mathcal{H}(1-\gamma, 1) \bmod p$ are 0 and $-1 - (\gamma_1^{(0)} + \gamma_2^{(0)})$; besides $B(\gamma; x)$ are $B(1-\gamma; x)$ are solutions of the associated differential equations respectively. The only option to conceal these conditions is to have

$$\begin{aligned} \text{val}_1(B(1-\gamma; x)) &\equiv -1 - (\gamma_1^{(0)} + \gamma_2^{(0)}) \pmod{p} \\ \text{val}_1(B(\gamma; x)) &\equiv \gamma_1^{(0)} + \gamma_2^{(0)} - p + 1 + \text{val}_1(B(1-\gamma; x)) \equiv 0 \pmod{p}. \end{aligned}$$

Since, moreover, $\text{val}_1(B(\gamma; x)) \leq \deg B(\gamma; x) < p$, we conclude that $\text{val}_1(B(\gamma; x)) = 0$. \square

Applying the previous lemma with $\gamma = \mathfrak{D}_p^k(\alpha)$ for k varying between 0 and $\ell_p - 1$, we find

$$\nu_1 := \text{val}_1(A(x)) = \sum_{k=0}^{\ell_p-1} \max(0, \alpha_1^{(k)} + \alpha_2^{(k)} - p + 1) \cdot p^k. \quad (3.3.7)$$

Apart from the singular points 1 and ∞ , the last singular point of the hypergeometric differential equation is 0. However, the valuation at 0 of $A(x)$ is clearly 0, by definition so this does not provide any further information in our quest to determine r .

Valuation at ordinary points. Equation (3.3.1) ensures that we can apply Lemma 2.1.3 to $B(\gamma; x)$ and conclude that each $\xi \in \mathbb{F}_p$ different from 1 is at most a simple root of each of the polynomials $B_k(x)$. Then, each root of $A(x)$ different from 1 has multiplicity

$$\varepsilon_0 + \varepsilon_1 \cdot p + \cdots + \varepsilon_{\ell_p-1} p^{\ell_p-1} \quad (3.3.8)$$

for some $\varepsilon_i \in \{0, 1\}$.

Assuming now, that $A(x)$ is a perfect r -th power, we know that for each of its roots, the expression (3.3.8) must be divisible by r . We use this information in a very special case. For each k , we let b_k be the number of distinct roots of $B_k(x)$ different from 1, and we order them by size:

$$b_{j_1} < \cdots < b_{j_\ell}.$$

We underline that the values of the b_k can obviously be deduced from the degrees of $B_k(x)$ and the multiplicity of 1 as a root of each of them, two quantities we have already computed previously. We take c maximal such that $b_{j_1} + \cdots + b_{j_c} < b_{j_\ell}$. Then there exists a root ξ_0 of $B_{j_\ell}(x)$, that is not a root of any of the polynomials $B_{j_1}(x), \dots, B_{j_c}(x)$. Set $J := \{j_{k+1}, \dots, j_{\ell-1}\}$, so that the multiplicity of ξ_0 as a root of $A(x)$ is given by

$$\nu_{J'} := p^{j_\ell} + \sum_{j \in J'} p^j$$

for some subset $J' \subseteq J$.

Putting all the constraints together, we conclude that r has to be a divisor of

$$g_{J'} := \gcd(\nu_\infty, \nu_1, \nu_{J'}, p^{\ell_p} - 1)$$

for some $J' \subseteq J$. Consequently, the index of $\text{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \mid k_{\mathfrak{p}}(x))$ in the conjectured group $G_{\mathfrak{p}}$ of Proposition 3.3.9 is bounded from above by $g_{J'}/h$ where

$$h := \begin{cases} p^{e_p} + 1 & \text{if } \ell_p \text{ is even and } p^{-e_p} \in D \\ 1 & \text{otherwise.} \end{cases}$$

Of course, the set J' is *a priori* not known, but we can even bound the index by taking the maximum (or the least common multiple) of all the previous quantities when J' varies.

Uniformity in p . To make statements about all primes simultaneously, we need to study the behavior of g with respect to p . The key observation is that $\alpha_1^{(k)}$ and $\alpha_2^{(k)}$ depend only on $s := \lfloor p/d \rfloor$ and $t := p \bmod d$, as shown by the following lemma.

Lemma 3.3.11. *Let $\gamma \in \mathbb{Z}_{(p)} \cap (0, 1)$ with denominator d , and let $t \in \{1, \dots, d-1\}$ with $\gcd(t, d) = 1$. Then there exists a polynomial $\Gamma_t(x) \in \mathbb{Z}[x]$ of degree at most 1 such that, for all positive integer s such that $p = ds + t$ is a prime number, $\Gamma_t(s)$ is the unique representative of $(-\gamma) \bmod p$ in the interval $[0, p)$.*

Proof. We write $p = ds + t$. We consider a Bézout relation $ut + vd = 1$ with $u, v \in \mathbb{Z}$ and notice that $us - v \equiv -\frac{1}{d} \pmod{p}$ for all s since

$$-d(us - v) \equiv ut + vd = 1 \pmod{p}.$$

If $\gamma = \frac{a}{d}$, we now define

$$\Gamma_t(x) := aux - av - \left\lfloor \frac{au}{d} \right\rfloor (dx + t).$$

Clearly, $\Gamma_t(x)$ is a polynomial with integral coefficients of degree at most 1, and $\Gamma_t(s) \equiv -\gamma \pmod{p}$ for all s . Besides the constant coefficient of $\Gamma_t(x)$ is in the range $[0, d)$, while its linear coefficient is in $[0, t)$ given that

$$-1 < -\gamma = -av - \frac{au}{d}t \leq -av - \left\lfloor \frac{au}{d} \right\rfloor t < -av - \left(\frac{au}{d} - 1 \right)t = t - \gamma.$$

Therefore $0 \leq \Gamma_t(s) < ds + t = p$ for all s . □

Applying Lemma 3.3.11 with $\gamma = \mathfrak{D}_p^k(\alpha_i)$ (with $i \in \{1, 2\}$), we find that each $\alpha_i^{(k)}$ is a polynomial of degree at most 1 in s (for each fixed congruence class t modulo d). Given that ℓ_p also only depends on the congruence of p modulo d , we find that all the quantities $\nu_{\infty}, \nu_1, p^{\ell_p} - 1$ and all $\nu_{J'}$ are polynomials in s as well. If the greatest common divisor of these polynomials computed in $\mathbb{Q}[s]$ is equal to h for all J' , we derive that the index of $\text{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \mid k_{\mathfrak{p}}(x))$ in $G_{\mathfrak{p}}$ is bounded independently of p , and we can even explicitly compute a bound by writing down Bézout relations between these polynomials. In some cases, this bound is equal to 1, so that we can conclude that $\text{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \mid k_{\mathfrak{p}}(x)) = G_{\mathfrak{p}}$ for all prime p which is congruent to t modulo d .

Example 3.3.12. For any parameter $\boldsymbol{\alpha}$, and any prime number p for which $\ell_p = 1$, we immediately obtain from Lemma 2.1.3 that if $A(x) = {}_2F_1(\boldsymbol{\alpha}, (1); x) \bmod p$, x^p is not of the form $(x-1)^{2d}$ for some d , then $A(x)$ is not a perfect power and so $\text{Gal}({}_2F_1(\boldsymbol{\alpha}, (1); x) \mid k_{\mathfrak{p}}(x)) = \mathbb{F}_p^{\times}$ for any prime ideal \mathfrak{p} over p . This is one particular instance on our ideas used for zeroes of $A(x)$ that

	ℓ	$-p^{\frac{\ell}{2}} \in D?$	ν_{∞}	ν_1	$\text{lcm}(\nu_{J'})$	$\text{lcm}(g_{J'})$	h
$p = 8s + 1$	1	-	s	0	1	1	1
$p = 8s + 3$	1	-	s	0	1	1	1
$p = 8s + 5$	2	no	$8s^2 + 10s + 3$	$4s + 3$	$8s + 5$	1	1
$p = 8s + 7$	2	yes	$8s^2 + 12s + 4$	$4s + 4$	$64s^2 + 88s + 30$	$4s + 4$	$4s + 4$

TABLE 1: Proof that for $\alpha = (\frac{1}{8}, \frac{3}{8})$ the Galois group is cyclic of order $\frac{p^{\ell p} - 1}{h}$

are nonsingular points of the associated differential equation. For example, taking $\alpha = (\frac{1}{2}, \frac{1}{2})$ we have seen the very same argument for hypergeometric function

$${}_2F_1(\alpha, (1); 4x) = \sum_{n=0}^{\infty} \binom{2n}{n}^2 x^n$$

in Subsection 2.1.3.

Example 3.3.13. Let us take $\alpha = (\frac{1}{8}, \frac{3}{8})$. Table 1 shows for each congruent class of p modulo d , the values of ℓ_p , ν_{∞} , ν_1 , the lcm of $\nu_{J'}$ for the relevant J' and the corresponding value for g . We see that the last two columns agree, which proves that the actual Galois groups agree with the conjectured ones.

Example 3.3.14. Let us now take $\alpha = (\frac{1}{7}, \frac{3}{7})$. In Table 2, we again investigate for all congruence classes of p modulo 7 the implications on the size on the Galois groups. We display the ratio $\text{lcm}(g_{J'})/h$ measuring the discrepancy between the expected size of the Galois group and the bound we prove. The quotient is 1 if and only if we succeeded to prove that the Galois group $\text{Gal}({}_2F_1(\alpha, (1); x) \mid k_{\mathbb{p}}^{\times}(x))$ is of index h in $k_{\mathbb{p}}^{\times}$. We also display $\text{gcd}(\nu_{\infty}, \nu_1, p^{\ell} - 1)/h$ to emphasize the benefit of the computation of the $\nu_{J'}$ in finding bounds for the size.

	ℓ	$-p^{\frac{\ell}{2}} \in D?$	$\text{gcd}(\nu_{\infty}, \nu_1, p^{\ell} - 1)/h$	$\text{lcm}(g_{J'})/h$	h
$p = 7s + 1$	1	-	s	1	1
$p = 7s + 2$	3	-	4	2	1
$p = 7s + 3$	6	yes	1	1	$49s^3 + 63s^2 + 27s + 4$
$p = 7s + 4$	3	-	5	1	1
$p = 7s + 5$	6	yes	1	1	$49s^3 + 105s^2 + 75s + 18$
$p = 7s + 6$	2	yes	1	1	$s + 1$

TABLE 2: For $\alpha = (\frac{1}{7}, \frac{3}{7})$ and prime numbers congruent to 2 modulo 7 the techniques presented do not suffice to prove that $A_p(x)$ is not a square.

Example 3.3.15. From the previous examples one might hope, that using our methods for any set of parameters we are able to find a fixed bound, valid for all prime numbers, on the maximal index of the Galois group in the cyclic group of order $(p^{\ell p} - 1)/h$. However, taking $\alpha = (\frac{1}{15}, \frac{11}{15})$ dashes this hope. Writing $p = 15s + t$, for each value of $t \in \{2, 7, 8, 13, 14\}$, we find each time a subset J' for which $g_{J'}(\alpha)$ is a nonconstant polynomials in s .

We have implemented the methods described in this chapter in SageMath², to carry out the necessary computations for the examples and to test the bounds given for small values of the

²The code is available at <https://plmlab.math.cnrs.fr/caruso/gal-Dfin-modp>

common denominator of the parameters. Doing this, we showed that the equality

$$\text{Gal}({}_2F_1(\alpha, (1); x) \mid k_{\mathfrak{p}}(x)) = G_{\mathfrak{p}}$$

holds whenever $d \in \{2, 3, 4, 6, 8, 12, 24\}$, which completes the proof of Theorem 1.2 of the introduction. Similarly, we also proved by computations that the index of $\text{Gal}({}_2F_1(\alpha, (1); x) \mid k_{\mathfrak{p}}(x))$ in $G_{\mathfrak{p}}$ is always at most 5 when $d \leq 12$.

References

- [AB13] B. Adamczewski and J. Bell. “Diagonalization and rationalization of algebraic Laurent series”. *Ann. Sci. Éc. Norm. Supér.* 46 (2013), pp. 963–1004. DOI: [10.24033/asens.2207](https://doi.org/10.24033/asens.2207).
- [ABC23] B. Adamczewski, A. Bostan, and X. Caruso. *A Sharper Multivariate Christol’s Theorem with Applications to Diagonals and Hadamard Products*. 2023. DOI: [10.48550/arXiv.2306.02640](https://doi.org/10.48550/arXiv.2306.02640).
- [Apé79] R. Apéry. “Irrationalité de $\zeta(2)$ et $\zeta(3)$ ”. *Astérisque* 61 (1979), pp. 11–13. URL: https://www.numdam.org/book-part/AST_1979__61__11_0/.
- [AVZ11] G. Almkvist, D. Van Straten, and W. Zudilin. “Generalizations of Clausen’s Formula and Algebraic Transformations of Calabi–Yau Differential Equations”. *Proceedings of the Edinburgh Mathematical Society* 54.2 (2011), pp. 273–295. DOI: [10.1017/S0013091509000959](https://doi.org/10.1017/S0013091509000959).
- [AZ06] G. Almkvist and W. Zudilin. “Differential equations, mirror maps and zeta values”. *Mirror symmetry V. Proceedings of the BIRS workshop on Calabi-Yau varieties and mirror symmetry, December 6–11, 2003*. Providence, RI: American Mathematical Society (AMS); Somerville, MA: International Press, 2006, pp. 481–515. DOI: [10.1090/amsip/038](https://doi.org/10.1090/amsip/038).
- [BCR24] A. Bostan, X. Caruso, and J. Roques. “Algebraic Solutions of Linear Differential Equations: An Arithmetic Approach”. *Bulletin of the American Mathematical Society* 61.4 (2024), pp. 609–658. DOI: [10.1090/bull/1835](https://doi.org/10.1090/bull/1835).
- [Beu02] F. Beukers. “On Dwork’s Accessory Parameter Problem”. *Mathematische Zeitschrift* 241.2 (2002), pp. 425–444. DOI: [10.1007/s00209-002-0424-8](https://doi.org/10.1007/s00209-002-0424-8).
- [BH89] F. Beukers and G. Heckman. “Monodromy for the Hypergeometric Function ${}_nF_{n-1}$ ”. *Inventiones Mathematicae* 95.2 (1989), pp. 325–354. DOI: [10.1007/BF01393900](https://doi.org/10.1007/BF01393900).
- [BY22] A. Bostan and S. Yurkevich. “On a Class of Hypergeometric Diagonals”. *Proceedings of the American Mathematical Society* 150.3 (2022), pp. 1071–1087. DOI: [10.1090/proc/15693](https://doi.org/10.1090/proc/15693).
- [CC85] D. V. Chudnovsky and G. V. Chudnovsky. “Applications of Padé Approximations to Diophantine Inequalities in Values of G-functions”. *Number Theory*. Ed. by D. V. Chudnovsky, G. V. Chudnovsky, H. Cohn, and M. B. Nathanson. Vol. 1135. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 9–51. DOI: [10.1007/BFb0074600](https://doi.org/10.1007/BFb0074600).
- [Chr+80] G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. “Suites Algébriques, Automates et Substitutions”. *Bulletin de la Société mathématique de France* 79 (1980), pp. 401–419. DOI: [10.24033/bsmf.1926](https://doi.org/10.24033/bsmf.1926).
- [Chr79] G. Christol. “Ensembles presque périodiques k -reconnaissables”. *Theoret. Comput. Sci.* 9.1 (1979), pp. 141–145. DOI: [10.1016/0304-3975\(79\)90011-2](https://doi.org/10.1016/0304-3975(79)90011-2).

- [Chr86a] G. Christol. “Fonctions et éléments algébriques”. *Pacific Journal of Mathematics* 125.1 (1986), pp. 1–37. DOI: [10.2140/pjm.1986.125.1](https://doi.org/10.2140/pjm.1986.125.1).
- [Chr86b] G. Christol. “Fonctions hypergéométriques bornées”. *Groupe de travail d’analyse ultramétrique*. exp. no 8 14 (1986–1987), pp. 1–16.
- [Cla28] T. Clausen. “Über die Fälle, wenn die Reihe von der Form $y = 1 + \frac{\alpha}{1} \cdot \frac{\beta}{\gamma} x + \frac{\alpha \cdot (\alpha+1)}{1 \cdot 2} \cdot \frac{\beta \cdot (\beta+1)}{\gamma \cdot (\gamma+1)} x^2 + \text{etc}$ ein Quadrat von der Form $z = 1 + \frac{\alpha'}{1} \cdot \frac{\beta'}{\gamma'} \cdot \frac{\delta'}{\varepsilon'} x + \frac{\alpha' \cdot (\alpha'+1)}{1 \cdot 2} \cdot \frac{\beta' \cdot (\beta'+1)}{\gamma' \cdot (\gamma'+1)} \cdot \frac{\delta' \cdot (\delta'+1)}{\varepsilon' \cdot (\varepsilon'+1)} x^2 + \text{etc}$ hat.” *J. Reine Angew. Math.* 3 (1828), pp. 89–91. DOI: [10.1515/crll.1828.3.89](https://doi.org/10.1515/crll.1828.3.89).
- [Del84] P. Deligne. “Intégration sur un cycle évanescant”. *Invent. Math.* 76 (1984), pp. 129–143. DOI: [10.1007/BF01388496](https://doi.org/10.1007/BF01388496).
- [DL87] J. Denef and L. Lipshitz. “Algebraic power series and diagonals”. *J. Number Theory* 26 (1987), pp. 46–67. DOI: [10.1016/0022-314X\(87\)90095-3](https://doi.org/10.1016/0022-314X(87)90095-3).
- [DM82] P. Deligne and J. S. Milne. *Tannakian categories*. Hodge cycles, motives, and Shimura varieties, Lect. Notes Math. 900, 101–228 (1982). 1982.
- [Dom60] C. Domb. “On the theory of cooperative phenomena in crystals”. *Advances in Physics* 9.35 (1960), pp. 245–361. DOI: [10.1080/00018736000101199](https://doi.org/10.1080/00018736000101199).
- [DRR17] E. Delaygue, T. Rivoal, and J. Roques. “On Dwork’s p -Adic Formal Congruences Theorem and Hypergeometric Mirror Maps”. *Memoirs of the American Mathematical Society* 246.1163 (2017). DOI: [10.1090/memo/1163](https://doi.org/10.1090/memo/1163).
- [Dwo90] B. Dwork. “Differential Operators with Nilpotent p -Curvature”. *American Journal of Mathematics* 112.5 (1990), pp. 749–786. DOI: [10.2307/2374806](https://doi.org/10.2307/2374806).
- [FH23] F. Fürnsinn and H. Hauser. “Fuchs’ Theorem on Linear Differential Equations in Arbitrary Characteristic” (2023). DOI: [10.48550/arXiv.2307.01712](https://doi.org/10.48550/arXiv.2307.01712).
- [Fis04] S. Fischler. “Irrationalité de valeurs de zêta (d’après Apéry, Rivoal, ...)”. *Séminaire Bourbaki. Volume 2002/2003. Exposés 909–923*. Paris: Société Mathématique de France, 2004, 27–62, ex. URL: <https://eudml.org/doc/252133>.
- [Fur67] H. Furstenberg. “Algebraic functions over finite fields”. *J. Algebra* 7 (1967), pp. 271–277. DOI: [10.1016/0021-8693\(67\)90061-0](https://doi.org/10.1016/0021-8693(67)90061-0).
- [FY24] F. Fürnsinn and S. Yurkevich. “Algebraicity of Hypergeometric Functions with Arbitrary Parameters”. *Bulletin of the London Mathematical Society* (2024), blms.13103. DOI: [10.1112/blms.13103](https://doi.org/10.1112/blms.13103).
- [Gal81] A. I. Galochkin. “Hypergeometric Siegel Functions and E-Functions”. *Mathematical Notes of the Academy of Sciences of the USSR* 29.1 (1981), pp. 3–8. DOI: [10.1007/BF01142505](https://doi.org/10.1007/BF01142505).
- [Ges82] I. Gessel. “Some congruences for Apéry numbers”. *Journal of Number Theory* 14.3 (1982), pp. 362–368. DOI: [10.1016/0022-314X\(82\)90071-3](https://doi.org/10.1016/0022-314X(82)90071-3).
- [Har88] T. Harase. “Algebraic elements in formal power series rings”. *Israel J. Math.* 63 (1988), pp. 281–288. DOI: [10.1007/BF02778035](https://doi.org/10.1007/BF02778035).
- [Kat72] N. M. Katz. “Algebraic Solutions of Differential Equations (p -Curvature and the Hodge Filtration)”. *Inventiones Mathematicae* 18.1-2 (1972), pp. 1–118. DOI: [10.1007/BF01389714](https://doi.org/10.1007/BF01389714).
- [Kat73] N. M. Katz. “ p -adic Properties of Modular Schemes and Modular Forms”. *Modular Functions of One Variable III*. Ed. by W. Kuyk and J.-P. Serre. Berlin, Heidelberg: Springer Berlin Heidelberg, 1973, pp. 69–190.

- [Kat90] N. M. Katz. *Exponential Sums and Differential Equations*. Annals of Mathematics Studies 124. Princeton, N.J: Princeton Univ. Press, 1990. 430 pp. DOI: [10.1515/9781400882434](https://doi.org/10.1515/9781400882434).
- [Ked10] K. S. Kedlaya. *p-adic differential equations*. Vol. 125. Camb. Stud. Adv. Math. Cambridge: Cambridge University Press, 2010. DOI: [10.1017/CB09780511750922](https://doi.org/10.1017/CB09780511750922).
- [Ked22] K. S. Kedlaya. “Frobenius structures on hypergeometric equations”. *Arithmetic, geometry, cryptography, and coding theory, AGC2T. 18th international conference, Centre International de Rencontres Mathématiques, Marseille, France, May 31 – June 4, 2021*. Providence, RI: American Mathematical Society (AMS), 2022, pp. 133–158. DOI: [10.1090/conm/779/15673](https://doi.org/10.1090/conm/779/15673).
- [Lev61] A. Levelt. “Hypergeometric Functions”. *Indagationes Mathematicae (Proceedings)* 64 (1961), pp. 361–372. DOI: [10.1016/S1385-7258\(61\)50037-6](https://doi.org/10.1016/S1385-7258(61)50037-6).
- [Mat09a] B. H. Matzat. “Frobenius modules and Galois representations”. *Ann. Inst. Fourier* 59.7 (2009), pp. 2805–2818. DOI: [10.5802/aif.2508](https://doi.org/10.5802/aif.2508).
- [Mat09b] B. H. Matzat. “From Frobenius structures to differential equations”. *DART II Proceedings* (2009). URL: <https://archiv.ub.uni-heidelberg.de/volltextserver/8075/1/Frobenius2.pdf>.
- [Rob00] A. M. Robert. *A course in p-adic analysis*. Vol. 198. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+437. DOI: [10.1007/978-1-4757-3254-2](https://doi.org/10.1007/978-1-4757-3254-2).
- [Sal86] O. Salou. “Suites automatiques à multi-indices”. *Sém. Théorie Nombres Bordeaux (1986-1987)*, Exposé 4 (1986), pp. 1–27.
- [Sal87] O. Salou. “Suites automatiques à multi-indices et algébricité”. *C. R. Acad. Sci. Paris Sér. I Math.* 305 (1987), pp. 501–504.
- [Sta80] R. Stanley. “Differentiably Finite Power Series”. *European Journal of Combinatorics* 1.2 (1980), pp. 175–188. DOI: [10.1016/S0195-6698\(80\)80051-5](https://doi.org/10.1016/S0195-6698(80)80051-5).
- [SW88] H. Sharif and C. F. Woodcock. “Algebraic functions over a field of positive characteristic and Hadamard products”. *J. London Math. Soc. (2)* 37 (1988), pp. 395–403. DOI: [10.1112/jlms/s2-37.3.395](https://doi.org/10.1112/jlms/s2-37.3.395).
- [Var21] D. Vargas-Montoya. “Algébricité modulo p , séries hypergéométriques et structures de Frobenius fortes”. *Bulletin de la Société mathématique de France* (2021). DOI: [10.24033/bsmf.2834](https://doi.org/10.24033/bsmf.2834).
- [Var24] D. Vargas-Montoya. “Algebraicity modulo p of Generalized Hypergeometric Series ${}_nF_{n-1}$ ”. *Journal of Number Theory* 259 (2024), pp. 273–321. DOI: [10.1016/j.jnt.2024.01.004](https://doi.org/10.1016/j.jnt.2024.01.004).
- [Zag09] D. Zagier. “Integral Solutions of Apéry-like Recurrence Equations”. *Groups and Symmetries*. Ed. by J. Harnad and P. Winternitz. Vol. 47. CRM Proceedings and Lecture Notes. Providence, Rhode Island: American Mathematical Society, 2009, pp. 349–366. DOI: [10.1090/crmp/047](https://doi.org/10.1090/crmp/047).

CNRS; IMB, UNIVERSITÉ DE BORDEAUX, 351 COURS DE LA LIBÉRATION, 33405 TALENCE, FRANCE
 Email: xavier@caruso.ovh

FACULTY OF MATHEMATICS, UNIVERSITY OF VIENNA, OSKAR-MORGENSTERN-PLATZ 1, 1090 VIENNA, AUSTRIA

Email: florian.fuernsinn@univie.ac.at

INSTITUT DE MATHÉMATIQUES DE TOULOUSE, UNIVERSITÉ PAUL SABATIER, 118 ROUTE
DE NARBONNE, 31062 TOULOUSE CEDEX 9, FRANCE

Email: daniel.vargas-montoya@math.univ-toulouse.fr