MASTERARBEIT / MASTER THESIS

Titel der Masterarbeit / Title of the Master Thesis

"A normal form theorem for regular singular differential operators in positive characteristic"

verfasst von / submitted by

Florian Fürnsinn, BSc

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2022 / Vienna, 2022

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 066 821
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Mathematik
Betreut von / Supervisor:	Univ.-Prof. i.R. Mag. Dr. Herwig Hauser

Contents

Zusammenfassung

Es wird eine differentielle Erweiterung des univariaten Potenzreihenrings über Körpern positiver Charakteristik konstruiert. Es wird gezeigt, dass in dieser Erweiterung jeder lineare Differentialoperator der Ordnung n mit Potenzreihen als Koeffizienten äquivalent zu seiner Initialform ist, bis auf einen Automorphismus, der algorithmisch bestimmt werden kann. Dies ermöglicht die Konstruktion eines n-dimensionalen Vektoraums von Lösungen solcher Gleichungen über den Konstanten, der die Fuchs-Frobenius-Methode auf positive Charakteristik verallgemeinert. Einige bekannte Resultate über Lösungen von Differentialgleichungen in positiver Charakteristik werden im Licht des Normalformensatz betrachtet. Mögliche Anwendungen auf Grothendiecks p-Krümmungsvermutung werden diskutiert und anhand von Beispielen aufgezeigt.

Abstact

A differential extension of the univariate power series ring over fields of positive characteristic is constructed. It is shown that in this extension any linear differential operator of order n with power series coefficients is equivalent to its initial form, up to an automorphism which can be algorithmically determined. This allows the construction of an n-dimensional space of solutions of such equations over the constants, generalizing the Fuchs-Frobenius method to positive characteristic. Several well-known results on solutions of differential equations in positive characteristic are viewed in the light of the normal form theorem. Possible applications to the Grothendieck p-curvature conjecture are discussed.

Acknowledgements

First, I would like to express my deep gratitude to my supervisor Herwig Hauser. He took the time to present his own research in lecture courses at the University of Vienna and raised several related questions while doing so. Some of them I try to answer in this thesis. In long meetings Herwig patiently listened to my ideas and gave inspiring advice. Further, he organized two workshops on the algebraic aspects of differential equations in Steyr and Lisbon and gave me the opportunity to present my findings to an international audience there. Also, he leads the projects P-31338 and P-34765 by the Austrian science fund FWF which supported me financially during my work.

Moreover, I am indebted to Sergey Yurkevich. He helped me with some technical details and made me aware of some severe problems in an earlier version of the thesis.

Last, but not least, I would like to thank my colleagues Florian Lang, Niki Merkl, Markus Reibnegger, and Stephan Schneider. They had to listen to my complaints and made helpful comments.

1 Introduction

An ordinary linear differential equation over the complex numbers with meromorphic coefficients is said to have a *regular singularity* at a point, if the equation admits a basis of local solutions that grow at most polynomially as one approaches the singular point. This definition was introduced by Fuchs, who characterised regular singularities by the order of vanishing of the coefficients of the equation [Fuc66]. He then constructed a basis of local solutions at such a point using linear combinations of (multivalued) meromorphic functions and powers of logarithms. Frobenius and Fuchs later developed a method of obtaining this basis of solutions using local exponents [Fro73]. The full construction is tedious, especially in the case of resonance (i.e., when local exponents have integer differences). However, if one takes a slightly different viewpoint and focuses on the study of the differential operator itself instead of trying to describe its solutions, one can obtain a very elegant reformulation of Frobenius' method and an algorithm for the computation of a basis of solutions. Hauser proves, colloquially formulated, the following result [Hau22].

Theorem 1.1. *Let L be a linear differential operator with regular singularity at 0, holomorphic coefficients and initial form L_0. Then there is a space $\mathcal{F}$ of holomorphic functions and logarithms, depending on the local exponents of L on which L acts and there is an automorphism u of $\mathcal{F}$ with*

$$L \circ u^{-1} = L_0.$$

Moreover, $\mathcal{F}$ contains a basis of solutions over the constants of the equation $Ly = 0$. These solutions can be obtained by applying u^{-1} to a basis of solutions of $L_0 y = 0$.

The solutions to $L_0 y = 0$ can be computed by solving a polynomial equation and the automorphism u can be algorithmically determined.

A motivation for studying differential equations over fields with characteristic different from 0 was provided by Grothendieck. He conjectured that a linear differential equation with rational coefficients in characteristic 0, or equivalently a system of first order equations, has a full set of *algebraic* solutions, if and only if it has a full basis of solutions over the field with p elements for almost all prime numbers p. This is known as the Grothendieck p-curvature conjecture. Hauser's normal form theorem allows the construction of a basis of solutions of the equation in characteristic 0. We will develop a similar theorem in positive characteristic and try to compare the solutions obtained in characteristic 0 to the ones in positive characteristic. In particular, we will discuss applications of the normal form theorems in combination with a variant of the Grothendieck conjecture by Bézivin [Béz91].

The definition of a regular singular point of a differential equation using the growth of the local solutions cannot be translated to characteristic p. However, the equivalent formulation by Fuchs using the order of vanishing of the coefficients of the equation applies. Honda provided an elementary overview on what was known about the p-curvature conjecture around 1980 [Hon81]. He also proposed to extend the space of possible solutions of differential equations in characteristic p by introducing a new variable z with derivative $1/x$. Still, Frobenius' method cannot be carried over to characteristic p in this way, as the existence of a full basis of solutions in this space is not guaranteed.

In the following we will introduce more generally countably many new variables $z_1, z_2, \ldots$

to extend the space of solutions to linear differential equations with regular singularities in characteristic p. Those new variables will behave like the k-fold iteration of the logarithm with respect to taking derivatives. This will allow us to formulate and prove the normal form theorem for differential operators in positive characteristic by carefully defining the "correct" space of solutions:

Theorem 1.2 (Normal form theorem in characteristic p, see Theorem 5.2 for details)**.** *Let $\Bbbk$ be a field of characteristic p and let $L \in \Bbbk[\![x]\!][\partial]$ be a linear differential operator with power series coefficients and initial form L_0. Then there is a space $\mathcal{F}$ depending on the local exponents of L on which L acts and which contains a basis of solutions of the equation $Ly = 0$. Further, there exists an automorphism u of $\mathcal{F}$ with*

$$L \circ u^{-1} = L_0.$$

The solutions of $Ly = 0$ then can be obtained by applying u^{-1} to a basis of solutions of $L_0 y = 0$.

We will construct such a space $\mathcal{F}$ explicitly together with the solutions of the differential equations $Ly = 0$. For example we will find a solution to the exponential differential equation $y' = y$ in characteristic 3, given by

$$1+x+2x^2+2x^3z_1+x^4(1+2z_1)+x^5z_1+2x^6z_1^2+x^7(1+2z_1+2z_1^2)+x^8(2+z_1^2)+x^9(2z_1+z_1^3z_2)+\dots,$$

where the coefficients of x^i can be algorithmically computed and the derivation of $\mathcal{F}$ is given by

$$z_1' = \frac{1}{x}, \quad z_2' = \frac{1}{x}\frac{1}{z_1}, \quad z_k' = \frac{1}{x}\frac{1}{z_1 \cdots z_{k-1}}.$$

2 Singular points of differential equations in characteristic 0 and p

Let $\Bbbk$ be a field. Let

$$L = p_n(x)\partial^n + \ldots + p_1(0)\partial + p_0(x) \in \Bbbk[\![x]\!][\partial]$$

with $p_n \neq 0$ be a differential operator of order n with formal power series coefficients. We will consider differential equations of the form $Ly = 0$ for such operators L.

We can rewrite the operator L as

$$L = \sum_{j=0}^{n} \sum_{i=0}^{\infty} c_{ij} x^i \partial^j$$

and rearrange the terms to write $L = L_0 + L_1 + \ldots$, where

$$L_k = \sum_{i-j=\tau_k} c_{ij} x^i \partial^j$$

is an *Euler operator*. We call $\tau_k \in \mathbb{Z}$ the *shift* of the operator L_k. The operator L_0 of smallest shift is called the *initial form* of L at 0 and $\tau \coloneqq \tau_0$ is called the *shift* of L itself. As multiplying an operator by $x^{-\tau}$ does not change the solutions of the differential equation $Ly = 0$ we may assume without loss of generality that $\tau = 0$, which we will do in the following. We say that L has a *singularity at* $x = 0$ if at least one of the quotients $p_i(x)/p_n(x)$ has negative order at 0 as a Laurent series in x. We say that the singularity is *regular* if the order of x in $p_i(x)/p_n(x)$ is greater than or equal to $i - n$. It is easy to show that this is equivalent to requiring that the order of L_0 is the same as the order of L, i.e., that $c_{nn} \neq 0$.

The *indicial polynomial* of L is defined by

$$\chi_L(s) = \sum_{i=0}^{n} c_{ii} s^{\underline{i}},$$

where $s^{\underline{i}} = s(s-1)\cdots(s-i+1)$ denotes the falling factorial. The roots ρ in the algebraic closure $\overline{\Bbbk}$ of $\Bbbk$ of $\chi_L = \chi_{L_0}$ are called the *local exponents* of L at 0 and we will denote their multiplicity by $m_\rho \in \mathbb{N}$. In the following we will assume for simplicity that $\Bbbk$ is algebraically closed. However, if all local exponents are contained in $\Bbbk$, this assumption is not necessary. In fact, in many of our examples we will pick $\Bbbk = \mathbb{F}_p$ or $\Bbbk = \mathbb{Q}$.

Remark 2.1. We can rewrite any differential operator with positive shift in terms of $\delta \coloneqq x\partial$, the *Euler derivative*. The base change between $x^n\partial^n$ and δ is given by the Stirling numbers of the second kind $S_{n,k}$. This is readily verified using the recursion relation $S_{n+1,k} = kS_{n,k} + S_{n,k-1}$. This allows to read off the indicial polynomial of an operator: If the initial form of an operator L is given by $L_0 = \varphi(\delta)$ for some polynomial φ, then the indicial polynomial of the operator is $\chi_L = \varphi$.

We recall some basic facts from differential algebra. If (R, ∂) is a differential ring (or field), a *constant* is an element $r \in R$, such that $\partial r = 0$. The set of constants of R forms a subring (or field). A linear differential equation of order n has at most n linearly independent solutions in any differential field R over its field of constants. This is a simple corollary of the Wronski lemma, see [SP03], p. 9 or [Hon81]. A set of n such solutions is called a *full basis of solutions* of the equation in R.

Let us first consider the complex case. For Euler equations, i.e., equation of the form $Ly = 0$ for some Euler operator L, the solutions at 0 are obvious. They are of the form $x^\rho \log(x)^k$ where $\rho \in \mathbb{C}$ ranges over the local exponents of L and k is a natural number smaller than the multiplicity of ρ. Let us describe the solutions in a more algebraic setting. We search for solutions in spaces of the form $x^\rho \mathbb{C}(\!(x)\!)[z]$, where we introduce a new variable z to represent the logarithm. Here $\mathbb{C}(\!(x)\!) = \mathrm{Quot}(\mathbb{C}[\![x]\!])$ denotes the field of formal Laurent series. The important thing about the logarithm in our setting is that its derivative is $1/x$. We equip $x^\rho \mathbb{C}(\!(x)\!)[z]$ with the derivation ∂ such that

$$\partial : \mathbb{C}(\!(x)\!)[z] \to \mathbb{C}(\!(x)\!)[z],$$
$$\partial x^\rho := \rho x^{\rho-1}$$
$$\partial z := \frac{1}{x}$$

We define ∂^k to be the k-fold composition of ∂ with itself. The action of any differential operator $L \in \mathbb{C}[\![x]\!][\partial]$ extends naturally to $\mathbb{C}(\!(x)\!)[z]$. We call this the *extension* of L. In this notation the space of solutions of $Ly = 0$ is spanned by the set of monomials

$$\{x^\rho z^k \mid \rho \text{ is a local exponent of } L,\ 0 \leq k < m_\rho\}.$$

The local solutions to general regular singular equations over $\mathbb{C}$ are of the form $\sum_{k=0}^{m} x^\rho z^k a(x)$, where $a(x) \in \mathbb{C}(\!(x)\!)$. These solutions are, however, in general not well-defined functions in 0; they can be interpreted only as multi-valued functions. In general fields, different from $\mathbb{C}$, there is no such interpretation of x^ρ as a function if ρ is an arbitrary element of the field.

From now on let $\Bbbk$ be a field of characteristic p. If we try to transfer the description of a basis of solutions of differential equations over $\mathbb{C}$ to fields of characteristic p, we run into troubles, as the following example shows.

Example 2.2. Let $n \in \mathbb{N}$ and let

$$L = \delta^n = (x\partial)^k = x^n\partial^n + S_{n,n-1}x^{n-1}\partial^{n-1} + S_{n,2}x^{n-2}\partial^{n-2} + \ldots + S_{n,1}x\partial + S_{n,0}.$$

If we interpret L as a differential operator in $\mathbb{C}[\![x]\!][\partial]$ and solve the equation $Ly = 0$ in $\mathbb{C}(\!(x)\!)[z]$, we obtain a full basis of solutions $\{1, z, \ldots, z^{n-1}\}$ over $\mathbb{C}$. In characteristic p the field of constants of $\Bbbk(\!(x)\!)[z]$ clearly contains $\Bbbk(\!(x^p)\!)[z^p]$. So for $n > p$ the set $\{1, z, \ldots, z^{n-1}\}$ cannot be a full basis of solutions, as 1 and z^p are linearly dependent over the field of constants. In fact the situation is even worse. There can only exist p^2 monomials of the form $x^i z^j$ that are linearly independent over the constants. Hence if $n > p^2$, there cannot exist a monomial basis of n solutions of any Euler equation of order n.

In order to resolve this issue in positive characteristic, we construct a differential extension of $\Bbbk(\!(x)\!)(z)$ which will contain a full basis of solutions for any linear differential operator with regular singularity at 0. Regularity of the differential operator is required to have as many local exponent, counted with multiplicity, as the order of the differential operator. For each $\rho \in \Bbbk$ let t^ρ be a symbol. It will play the role of the monomial x^ρ from before; if ρ lies in the prime field of $\Bbbk$ we may substitute x for t to recover the classical setting. We will call ρ the exponent of t in t^ρ. Further, let

$$\mathcal{R} = \bigoplus_{\rho \in \Bbbk} t^\rho \Bbbk(z_1, z_2, \ldots)(\!(x)\!),$$

the direct sum of Laurent series in x with coefficients in the field of rational functions over $\Bbbk$ in countably many variables z_i. We will simply write $\Bbbk(\mathrm{z})$ instead of $\Bbbk(z_1, z_2, \ldots)$.

We consider $\mathcal{R}$ as a ring with respect to the obvious addition and the multiplication given by

$$(t^\rho f) \cdot (t^\sigma g) = t^{\rho+\sigma}(f \cdot g)$$

for $\rho, \sigma \in \Bbbk$, $f, g \in \Bbbk[\mathrm{z}][\![x]\!]$. We equip $\mathcal{R}$ with the derivation $\partial = \partial_R$ satisfying:

$$\begin{aligned} \partial x &= 1, \\ \partial t &= t\frac{1}{x} \\ \partial t^\rho &= \rho t^\rho \frac{1}{x}, \end{aligned}$$
$$\partial z_1 = \frac{1}{x}, \quad \partial z_2 = \frac{1}{x}\frac{1}{z_1}, \quad \partial z_k = \frac{1}{x}\frac{1}{z_1 \cdots z_{k-1}}, \ \forall k \geq 1.$$

This turns $\mathcal{R}$ into a differential ring.

The action of ∂ on z_i is chosen to mimic the usual derivation of the i-fold composition $\log(\ldots(\log(x))\ldots)$ of the complex logarithm with itself.[1] Indeed we have, writing $\log^{[i]}$ for the i-fold repetition of the logarithm

$$\left(\log^{[i]}(x)\right)' = \frac{1}{x}\frac{1}{\log(x) \cdot \log(\log(x)) \cdots \log^{[i-1]}(x)}.$$

Remark 2.3. (i) The ring $\mathcal{R}$ is not an integral domain. Indeed, $(1+t+\ldots+t^{p-1})(1-t) = 0$. Thus, we are not able to form its quotient field and use the machinery of differential fields, as e.g. the Wronski Lemma and the concept of a basis of solutions. Still, in the course of the next sections, we will be able to provide a precise description of all solutions of a differential equation $Ly = 0$ in $\mathcal{R}$.

(ii) The derivation ∂ commutes with the direct sum, i.e., one has $\partial\left(t^\rho \Bbbk(\mathrm{z})(\!(x)\!)\right) \subseteq t^\rho \Bbbk(\mathrm{z})(\!(x)\!)$. This is the reason for not simply defining $\partial t^\rho = \rho t^{\rho-1}$.

(iii) Note that the elements of $\mathcal{R}$ may have unbounded degree in each of the variables z_i, only the coefficient of a given power of x has finite degree. This differs from the situation in characteristic 0 where the exponent of the logarithm in a solution of the equation $Ly = 0$ is bounded for each differential operator.

(iv) The doubly iterated logarithm $\log(\log(x))$ does not satisfy any homogeneous linear differential equation with holomorphic coefficients, but only the non-linear equation

$$xy'' + y' + x(y')^2 = 0.$$

[1] After the finishing of this text, we became aware that Bernard Dwork already considered iterated logarithms in positive characteristic in [Dwo90] p. 752. Apparently he did not exploit the full repertoire of this extension.

Alternatively, it satisfies the equation

$$x \log(x) y' = 1$$

in which the standard logarithm appears as a coefficient.

For elements of $\mathcal{R}$ the exponents of x are integers, while the exponents of t are elements of the field $\Bbbk$ of characteristic p (formally t^ρ for $\rho \in \Bbbk$ is just a symbol). However, we will see that the exponents of x and t interact in a certain way. We will use the following convention: In case that ρ is in the prime field $\mathbb{F}_p$ of $\Bbbk$, we will write $x^{\rho_*} = x^\rho$ where $\rho_* \in \{0, 1, \dots, p-1\}$ is a representative of ρ in $\mathbb{Z}$. Conversely we will write $t^{k^*} = t^k$ for some $k \in \mathbb{Z}$, where $k^* \in \mathbb{F}_p$ is the reduction of k modulo p.

Before we proceed, we will determine the constants of $\mathcal{R}$. Denote by $\Bbbk(\mathrm{z}^p)$ the field $\Bbbk(z_1^p, z_2^p, \dots)$ of the field of rational functions $\Bbbk(\mathrm{z})$.

Proposition 2.4. *The ring of constants of $(\mathcal{R}, \partial)$ is*

$$\mathcal{C} := \bigoplus_{\rho \in \mathbb{F}_p} t^\rho x^{p-\rho} \Bbbk(\mathrm{z}^p)(\!(x^p)\!),$$

where $\mathbb{F}_p$ denotes the prime field of $\Bbbk$. Moreover, $\mathcal{C}$ is a field.

Proof. Let $f \in \bigoplus_{\rho \in \Bbbk} t^\rho \Bbbk(\mathrm{z})(\!(x)\!)$ and assume that

$$\partial f = 0.$$

Taking derivatives in $\mathcal{R}$ commutes with the direct sum, so it suffices to find constants of the form $t^\rho h$ for some $\rho \in \Bbbk$ and $h \in \Bbbk(\mathrm{z})(\!(x)\!)$.

Fix some $\rho \in \Bbbk$. As for all $k \in \mathbb{Z}$ the derivation ∂ maps $t^\rho \Bbbk(\mathrm{z}) x^k$ into $t^\rho \Bbbk(\mathrm{z}) x^{k-1}$ by definition, it further suffices to find constants of the form $t^\rho h x^k$, where $h \in \Bbbk(\mathrm{z})$. Therefore we are reduced to search for elements $t^\rho h x^k$ of $\mathcal{R}$ with $\partial(t^\rho h x^k) = 0$. Write $h = g_1/g_2$ for $g_1, g_2 \in \Bbbk[\mathrm{z}]$. Then $\partial(t^\rho h x^k) = 0$ is equivalent to $\partial(t^\rho g_1 g_2^{p-1} x^k) = 0$, as g_2^p is a constant. So without loss of generality we may assume that $h \in \Bbbk[\mathrm{z}]$ is a polynomial. We expand:

$$0 = \partial(t^\rho h x^k) = t^\rho((\partial h)x + (k+\rho)h)x^{k-1}. \tag{1}$$

Let l be minimal such that $h \in \Bbbk[z_1, \dots, z_l]$. Consider the leading monomial of h with respect to the inverse lexicographic ordering in $\mathbb{N}^l$. That is $(\alpha_1, \dots, \alpha_l) \leq (\beta_1, \dots, \beta_l)$ if $\beta_l > \alpha_l$ or $\beta_l = \alpha_l$ and $(\alpha_1, \dots, \alpha_{l-1}) \leq (\beta_1, \dots, \beta_{l-1})$ in the inverse lexicographic ordering. We write

$$h = c z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_l^{\alpha_l} + r,$$

for some $c \in \Bbbk$ and some $r \in \Bbbk[z_1, \dots, z_l]$, where the exponents of all monomials in r are smaller than α.

Taking the derivative ∂ of a monomial decreases the exponents of at least one of the z_i, therefore yields a sum of smaller monomials with respect to the chosen ordering. Thus, in $x\partial h$ the coefficient of $z_l^{\alpha_l} z_{l-1}^{\alpha_{l-1}} \cdots z_1^{\alpha_1}$ vanishes by the maximality of the exponents α_i. If we compare coefficients of $t^\rho x^{k-1} z_l^{\alpha_l} z_{l-1}^{\alpha_{l-1}} \cdots z_1^{\alpha_1}$ in Equation (1) we get $k + \rho = 0$. So it follows that $\rho \in \mathbb{F}_p$ and that $k \equiv \rho \mod p$. Moreover we see from Equation (1) that $\partial h = 0$. This is clearly equivalent to $h \in \Bbbk[\mathrm{z}^p]$. Together with the reductions from above this proves that the ring of constants of $\mathcal{R}$ is indeed

$$\bigoplus_{\rho \in \mathbb{F}_p} t^\rho x^{p-\rho} \Bbbk(\mathrm{z}^p)(\!(x^p)\!).$$

Finally, we show that $\mathcal{C}$ is a field. Let

$$f = \sum_{\rho \in \mathbb{F}_p} t^\rho x^{p-\rho} f_\rho \in \mathcal{C},$$

where $f_\rho \in \Bbbk(\mathrm{z}^p)(\!(x^p)\!)$. Then we have

$$f^p = \sum_{\rho \in \mathbb{F}_p} t^{p\rho} x^{p^2-p\rho} f_\rho^p = \sum_{\rho \in \mathbb{F}_p} x^{p^2-p\rho} f_\rho^p \in \Bbbk(\mathrm{z}^p)(\!(x^p)\!),$$

where $f_\rho^p \in \Bbbk(\mathrm{z}^{p^2})(\!(x^{p^2})\!)$. The element f^p vanishes precisely if f_ρ vanishes for all $\rho \in \mathbb{F}_p$, as the exponents of x in each of the summands are from a different residue class modulo p^2. Thus, f^p is a unit for all $f \neq 0$ and we see that $(f^{p-1})(f^p)^{-1}$ is an inverse to f. □

Let us come back to Example 2.2 with $k = p+1$ and the operator $L = (x\partial)^{p+1} \in \Bbbk[x][\partial]$. In $\mathcal{R}$ we have

$$(x\partial)^{p+1}(z_1^p z_2) = 0.$$

So we have found another solution to the equation $Ly = 0$. This completes a basis of a $p+1-$dimensional vector space of solutions over the constants of $\mathcal{R}$, namely $\{1, z_1^1, z_1^2, \ldots, z_1^{p-1}, z_1^p z_2\}$, as those elements are $\mathcal{C}$ linearly independent.

Remark 2.5. (i) This example motivates the idea behind the definition of $\mathcal{R}$: we introduce new variables $z_1, z_2, \ldots$ to solve equations of the form $(x\partial)^k$ for all $k \in \mathbb{N}$. Having done so, we will see that this suffices to solve any differential equation with regular singularity.

(ii) From a different viewpoint, the problem of solving differential equations can be reduced to finding primitives. For power series in characteristic 0 the monomial $\frac{1}{x}$ has no integral and one introduces the logarithm to overcome this lack. In characteristic p monomials of the form x^{kp-1} for $k \in \mathbb{Z}$ have no integral, so introducing a variable z_1 with $\partial z_1 = \frac{1}{x}$ resolves the issue. However, then monomials of the form z_1^{kp-1} for $k \in \mathbb{Z}$ will again have no primitive, so we need to introduce z_2,z_3, etc. So in total we have to introduce countably many new variables z_i to obtain a ring that is closed under taking primitives.

3 Extensions of Euler operators to the ring $\mathcal{R}$

Our goal now is to prove that Euler operators admit "enough" solutions in the ring $\mathcal{R} = \bigoplus_{\rho\in\Bbbk} t^\rho \Bbbk(\mathrm{z})((x))$ and then to compute these solutions. For this we first investigate how Euler operators act on monomials $t^\rho z^\beta x^k$, see Lemma 3.3. For a multi-index $\beta \in \mathbb{Z}^{(\mathbb{N})} = \{(\beta_i)_{i\in\mathbb{N}} \mid \beta_i = 0 \text{ for almost all } i\}$ we write z^β for $z_1^{\beta_1}\cdots z_n^{\beta_n}$, if $\beta_j = 0$ for $j > n$. We define a partial ordering on $\mathbb{Z}^{(\mathbb{N})}$ by $\alpha \prec_e \beta$ if

$$e(\alpha) := \overline{\alpha_1} + p\overline{\alpha_2} + p^2\overline{\alpha_3} + \ldots < \overline{\beta_1} + p\overline{\beta_2} + p^2\overline{\beta_3} + \ldots =: e(\beta),$$

where $\overline{\alpha_1}, \overline{\beta_i} \in \{0, 1, \ldots, p-1\}$ are chosen such that $\alpha_i \equiv \overline{\alpha_i} \mod p$ respectively $\beta_i \equiv \overline{\beta_i} \mod p$. In other word $\prec_e$ is induced by the inverse lexicographic ordering on $\mathbb{F}_p^{(\mathbb{N})}$ via the element-wise reduction modulo p.

We also write $\mathrm{z}^\alpha \prec_e \mathrm{z}^\beta$ if $\alpha \prec_e \beta$.

Lemma 3.1. *Let $\beta \in \mathbb{Z}^{(\mathbb{N})}$. Then $(x\partial)z^\beta$ is a sum of monomials that are smaller than z^β with respect to $\prec_e$ and there is exactly one summand z^γ with $e(\gamma) = e(\beta) - 1$. In particular, $e(\beta)$ is the minimal number j such that $(x\partial)^j(z^\beta) = 0$.*

Proof. Let $\beta = (\beta_1, \beta_2, \ldots)$. We compute:

$$\partial \mathrm{z}^\beta = \frac{1}{x}\sum_{i=1}^{t} \beta_i \underbrace{z_1^{\beta_1-1} z_2^{\beta_2-1}\cdots z_i^{\beta_i-1} z_{i+1}^{\beta_{i+1}}\cdots z_t^{\beta_t}}_{=:\mathrm{z}^{\gamma_i}}$$

If $\beta_i \not\equiv 0 \mod p$, then clearly $\gamma_i \prec_e \beta$, otherwise its coefficient in $(x\partial)\mathrm{z}^\beta$ vanishes. A fast computation shows that if j is the least index, such that $\beta_j \neq 0$, then $e(\gamma_j) = e(\beta) - 1$. Moreover, $e(\gamma_j) < e(\beta) - 1$ for all other j. This proves in particular that $e(\beta)$ is the minimal number j such that $(x\partial)^j z^\beta = 0$. □

Let s be a variable and $k \in \mathbb{N}$. We define the *j-th Hasse derivative* or *divided derivative* by $(s^k)^{[j]} = \binom{k}{j} s^{k-j}$ and extend it linearly to $\Bbbk[s]$ [Jeo11]. We will apply it below to the indicial polynomial χ_L of an operator L, viewed as a polynomial in the variable s. The next three lemmata are inspired by Frobenius' "differentiation with respect to local exponents" [Fro73]. See also similar adeptions in characteristic 0 in [Hau22].

Lemma 3.2. *Let $k, l \in \mathbb{N}$. Then we have*

$$(s^{\underline{k}})^{[l]} + (s^{\underline{k}})^{[l+1]}(s-k) = (s^{\underline{k+1}})^{[l+1]}.$$

Proof. Let $q, r \in \Bbbk[s]$. The Hasse derivatives satisfy the product rule $(qr)^{[l]} = \sum_i q^{[i]} r^{[l-i]}$. Applying this to $s^{\underline{k+1}} = s^{\underline{k}}(s-k)$ and using that $(s-k)^{[i]} = 0$ for $i > 2$ we obtain the result. □

Lemma 3.3. *Let $j \in \mathbb{N}, k \in \mathbb{Z}, \beta \in \mathbb{Z}^{(\mathbb{N})}$. Then we have*

$$\partial^j(t^s x^k \mathrm{z}^\beta) = t^s x^{k-j}\left((s+k)^{\underline{j}}\mathrm{z}^\beta + ((s+k)^{\underline{j}})^{[1]} x\partial \mathrm{z}^\beta + \ldots + ((s+k)^{\underline{j}})^{[j]}(x\partial)^j \mathrm{z}^\beta\right).$$

Proof. The proof uses induction on j. For $j = 0$ the claim is obvious. Assume now the formula holds for some $j \geq 0$. Applying ∂ yields

$$\begin{aligned}
\partial^{j+1}(t^s x^k \mathrm{z}^\beta) &= \partial\left(t^s x^{k-j}\left((s+k)^{\underline{j}}\mathrm{z}^\beta + ((s+k)^{\underline{j}})^{[1]}x^1\partial\mathrm{z}^\beta + \ldots + ((s+i)^{\underline{j}})^{[j]}(x\partial)^j\mathrm{z}^\beta\right)\right)\\
&= t^s x^{k-j-1}(s+k-j)\left((s+k)^{\underline{j}}\mathrm{z}^\beta + ((s+k)^{\underline{j}})^{[1]}x\partial\mathrm{z}^\beta + \ldots + ((s+k)^{\underline{j}})^{[j]}(x\partial)^j\mathrm{z}^\beta\right) +\\
&\qquad + t^s x^{k-j}\left((s+k)^{\underline{j}}\partial\mathrm{z}^\beta + ((s+k)^{\underline{j}})^{[1]}\partial(x\partial)\mathrm{z}^\beta + \ldots + ((s+k)^{\underline{j}})^{[j]}\partial(x\partial)^j\mathrm{z}^\beta\right)\\
&= t^s x^{k-j-1}\left((s+k-j)(s+k)^{\underline{j}} + \left((s+k-j)((s+k)^{\underline{j}})^{[1]} + (s+k)^{\underline{j}}\right)x\partial\mathrm{z}^\beta + \ldots\right)\\
&= t^s x^{k-j-1}\left((s+k)^{\underline{j+1}}\mathrm{z}^\beta + ((s+k)^{\underline{j+1}})^{[1]}x\partial\mathrm{z}^\beta + \ldots + ((s+k)^{\underline{j+1}})^{[j+1]}(x\partial)^{j+1}\mathrm{z}^\beta\right),
\end{aligned}$$

where we have used the previous lemma in the last step. □

Lemma 3.4. *Let L be an Euler operator of order n with indicial polynomial χ_L. Then for any $\beta \in \mathbb{Z}^{(\mathbb{N})}$, $k \in \mathbb{Z}$ and $\rho \in \Bbbk$ we have*

$$L(t^\rho x^k \mathrm{z}^\beta) = t^\rho x^k\left(\chi_L(\rho+k)\mathrm{z}^\beta + \chi_L'(\rho+k)x\partial(\mathrm{z}^\beta) + \ldots + \chi_L^{[n]}(\rho+k)(x\partial)^n(\mathrm{z}^\beta)\right) \tag{2}$$

Proof. For two differential operators L, M we clearly have $\chi_{L+M}(s) = \chi_L(s) + \chi_M(s)$. Substituting $s = \rho$ in Lemma 3.3, this gives the result. □

For a field K of characteristic 0 a polynomial $q \in K[s]$ has a j-fold root at $\alpha \in \overline{K}$ if and only if the first $j-1$ derivatives of q vanish in α, but the j-th derivative does not. This very statement is false in characteristic p, but if one replaces derivatives with Hasse derivatives it holds true.

Lemma 3.5. *Let $q \in \Bbbk[s]$ be a polynomial. Then α is a j-fold root of q if and only if $q^{[i]}(\alpha) = 0$ for $i < j$, but $q^{[j]}(\alpha) \neq 0$.*

Proof. Write $q(s) = (s-\alpha)^j r(s)$ for some $j \in \mathbb{N}$, $r \in \Bbbk[s]$, where $r(\alpha) \neq 0$. Then

$$q^{[i]}(s) = \sum_{l=0}^{i}((s-\alpha)^j)^{[l]}r^{[i-l]}(s).$$

If $i < j$, then $((s-\alpha)^j)^{[l]}|_{s=\alpha} = 0$ for all $l < i$ and thus $q^{[i]}$ vanishes in α. Moreover $q^{[j]}(s)|_{s=\alpha} = r(\alpha) \neq 0$ and therefore the first implication is clear. For the other implication write $q(s) = (s-\alpha)^k r(s)$, where $r(\alpha) \neq 0$. As $q(\alpha) = 0$ we have $k \geq 1$. From the vanishing of the l-th Hasse derivative, where $l < j$, we can conclude recursively that $k \geq l$. Then, from $q^{[j]}(\alpha) \neq 0$ it follows that $k = j$. □

With these results we can finally solve Euler equations over our ring $\mathcal{R}$. We prove that, similar to the complex case, the solutions form a vector space of dimension n over the constants $\mathcal{C} \subseteq \mathcal{R}$.

Proposition 3.6. *Let L be an Euler operator of order n acting on $\mathcal{K}$ and let $\Omega \coloneqq \{\rho_1, \ldots, \rho_k\}$ be the set of local exponents of L at 0 and let $m_{\rho_1}, \ldots, m_{\rho_k}$ be their multiplicities. The solutions of $Ly = 0$ form a free $\mathcal{C}$-subspace of $\mathcal{R}$ of dimension n. A basis of this vector space is given by*

$$\left\{ y_{\rho,i} \coloneqq t^\rho \mathrm{z}^{\beta(i)} \middle| \rho \in \Omega,\ i < m_\rho \right\},$$

where

$$\beta(i) = (i, \lfloor i/p \rfloor, \lfloor i/p^2 \rfloor, \lfloor i/p^3 \rfloor, \ldots) \in \mathbb{Z}^{(\mathbb{N})}.$$

Before we prove the proposition let us consider an example.

Example 3.7. Consider the differential operator $L = x^4\partial^4 + x^3\partial^3 + x^2\partial^2 \in \mathbb{F}_2[x][\partial]$ with indicial polynomial $\chi_L(s) = (s-1)^3 s$. As the operator has order 4 one expects 4 solutions of $Ly = 0$, independent over $\mathcal{C}$. The proposition asserts that a basis is given by $1, x, xz_1, xz_1^2 z_2$. Indeed, one easily verifies that all these monomials are solutions and are $\mathcal{C}$-linearly independent.

Proof. The operator L is $\mathcal{C}$-linear and maps $t^\rho x^k \Bbbk(\mathrm{z})$ into itself. Therefore it suffices to find solutions of $Ly = 0$ of the form $t^\rho f(\mathrm{z}) x^k$, where $f \in \Bbbk(\mathrm{z})$. Further we can argue similar as in Proposition 2.4: we write $f = g_1/g_2$ for $g_1, g_2 \in \Bbbk[\mathrm{z}]$. If $t^\rho f(\mathrm{z}) x^k$ is a solution, then so is

$$g_2(\mathrm{z})^p \left(t^\rho f(\mathrm{z}) x^k\right) = t^\rho g_1(\mathrm{z}) g_2(\mathrm{z})^{p-1} x^k,$$

as $g_2^p \in \Bbbk[\mathrm{z}^p] \subseteq \mathcal{C}$. So we may assume without loss of generality that $0 \neq f \in \Bbbk[\mathrm{z}]$.

Let z^β be the largest monomial of $f(\mathrm{z})$ with respect to the ordering $\prec_e$. By Lemma 3.4 and the linearity of L we obtain

$$L(t^\rho f(\mathrm{z}) x^k) = t^\rho \left(\chi_L(\rho + k) f(\mathrm{z}) + \chi_L^{[1]}(\rho + k)(x\partial) f(\mathrm{z}) + \ldots + \chi_L^{[n]}(\rho + k)(x\partial)^n f(\mathrm{z}) \right).$$

Hence $L(t^\rho f(\mathrm{z}) x^k)$ vanishes if and only if

$$\chi_L(\rho + k) f(\mathrm{z}) + \chi_L^{[1]}(\rho + k)(x\partial) f(\mathrm{z}) + \ldots + \chi_L^{[n]}(\rho + k)(x\partial)^n f(\mathrm{z})$$

vanishes. We compare the coefficients of monomials in z starting with the largest. All appearing monomials are smaller than or equal to z^β by Lemma 3.1 and for all monomials z^γ in the summand $\chi_L(\rho + k)(x\partial)^j$ we have $e(\gamma) \leq e(\beta) - j$. So in order for the sum to vanish, $\chi_L(\rho + k)$ has to vanish by comparing coefficients of z^β. Further, by comparing coefficients of the next smaller monomials, we obtain $\chi_L^{[1]}(\rho + k) = 0$ or $(x\partial) z^\beta = 0$, i.e. $e(\beta) = 1$. Inductively we obtain that the sum vanishes, if and only if $\chi_L^{[l]}(\rho + k) \neq 0$ implies that $e(\beta) < l$. Put differently, by Lemma 3.5, if $\rho + k$ is a local exponent of L of multiplicity $m_{\rho+k}$, then $e(\beta) < m_{\rho+k}$. Thus we can give a complete description of the elements in the kernel of L. They are of the form $t^\rho x^k z^\beta$, where $e(\beta) < m_{\rho+k}$.

A quick calculation using Lemma 3.1 shows that the last condition is fulfilled for multi-indices, whose entries differ by multiples of p from $\beta(i)$ for $i = 0, \ldots, m_{\rho+k} - 1$. This shows on the one hand that the elements $y_{\rho,i}$ are indeed solutions of $Ly = 0$. On the other hand, the elements $y_{\rho,i}$ are chosen such that ρ ranges over all local exponent of L exactly once. For $\rho + k$ to be a local exponent, i.e., a zero of χ_L, we may add multiples of p to k, or subtract an element of the prime field from ρ and add it to k. Those transformations can be realized by multiplying a solution $t^\rho x^k f(\mathrm{z})$ by an element from $\mathcal{C}$. So indeed, all solutions of $Ly = 0$ are linear combinations of the elements $y_{\rho,i}$; that is they generate the $\mathcal{C}$-vector space of solutions.

Assume now that a $\mathcal{C}$-linear relation between the solutions $y_{\rho,i}$ exists. Let

$$\mathcal{D} := \bigoplus_{\rho\in\mathbb{F}_p} t^\rho x^{p-\rho}\mathbb{k}[\mathrm{z}^p][\![x^p]\!]$$

As $\mathcal{C} = \mathrm{Quot}\mathcal{D}$, it suffices to consider a relation with coefficients in $\mathcal{D}$. Let $\Omega = \bigsqcup_j \Omega_j$ be the set of all local exponents, where two local exponents ρ, σ are in the same subset Ω_j if and only if their difference is in the prime field. Assume that

$$\sum_j \sum_{\substack{\rho\in\Omega_j\\ i<m_\rho}} y_{\rho,i}\cdot d_{\rho,i} = 0$$

for some $d_{\rho,i} \in \mathcal{D}$. As the exponents of t of elements of $\mathcal{D}$ are in the prime field of $\mathbb{k}$, it follows that for each j the sum

$$\sum_{\substack{\rho\in\Omega_j\\ i<m_\rho}} y_{\rho,i}\cdot d_{\rho,i}$$

vanishes. So it suffices to focus on relations between solutions corresponding to local exponents in the same set set Ω_j. Without loss of generality $\Omega_j = \mathbb{F}_p$, the prime field of $\mathbb{k}$. We consider now a relation of the form

$$\sum_{\substack{\rho\in\mathbb{F}_p\\ i<m_\rho}} y_{\rho,i}\cdot d_{\rho,i} = 0.$$

Without loss of generality we may assume that at least one of the constants $d_{\rho,i}$ has order 0 in x and let $f_{\rho,i} \in \mathbb{k}[\mathrm{z}^p]$ be their constant term. Taking the coefficient of the monomial with smallest degree with respect to x in the sum above, we obtain a relation of the form

$$\sum_{\substack{\rho\in\mathbb{F}_p\\ i<m_\rho}} t^\rho z^{\beta_i}\cdot f_{\rho,i} = 0.$$

This sum vanishes if and only if the summand for each $\rho \in \mathbb{F}_p$ vanishes. Furthermore the multi-exponents $\beta(i) = (i, \lfloor i/p\rfloor, \lfloor i/p^2\rfloor, \ldots)$ are defined such that no two of them differ by multiples of p in every component. Thus $f_{\rho,i} = 0$ for all ρ and i, as required.

Finally, note that $\sum_{\rho\in\Omega} m_\rho = n$, as χ_L is a polynomial of degree n. So the dimension of the space of solutions is indeed n. □

4 The ρ-function space associated to an operator L

We have seen that a basis of solutions of Euler equations is of a very special form. It is not to be expected that solutions of general differential equations with regular singularities are similarly simple. We now try to find a description of the solutions of differential equations L based on the basis of monomial solutions of their initial form L_0. In the following let ρ be a fixed local exponent of L at 0. We define a function $\xi = \xi_L^\rho : \mathbb{N} \to \mathbb{N}$:

$$\xi(0) = m_\rho, \qquad \xi(k+1) = \xi(k) + m_{\rho+k+1},$$

where $m_{\rho+k} = 0$, if $\rho + j$ is not a root of the indicial polynomial. In other words:

$$\xi(k) = m_\rho + m_{\rho+1} + \ldots + m_{\rho+k}.$$

Note here that if $k > p$ the summand m_ρ appears at least twice in the sum. Moreover we define the *ρ-function space $\mathcal{F} = \mathcal{F}_L^\rho$ associated to L* as

$$\mathcal{F} := t^\rho \sum_{k=0}^{\infty} \bigoplus_{\beta \in \mathcal{B}(k)} \mathbb{k} z^\beta x^k,$$

where

$$\mathcal{B}(k) := \left\{ \beta \in \mathbb{N}^{(\mathbb{N})} \middle| \beta_1 < \xi(k), \beta_{j+1} \leq \beta_j / p \quad \forall j \in \mathbb{N} \right\}$$

is a finite subset of $\mathbb{N}^{(\mathbb{N})}$. Note that $\mathcal{F}$ only depends on the initial form of the differential operator L, more precisely only on the multiplicity of all local exponents of L that differ from ρ by an element of the prime field of $\mathbb{k}$.

Example 4.1. Consider the differential operator $L = x^3\partial^3 + 2x^2\partial^2 + \widetilde{L} \in \mathbb{F}_3[\![x]\!][\partial]$, where $\widetilde{L} \in \mathbb{F}_3[\![x]\!][\partial]$ has positive shift. The local exponents of L are 0 with multiplicity 2 and 1 with multiplicity 1. The monomials included in $\mathcal{F}_L^0$ are depicted below in Figure 1.

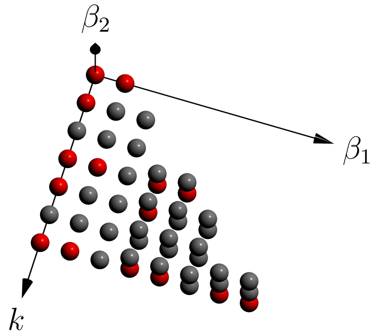

FIGURE 1: The set of exponents (k, β_1, β_2) of monomials $x^k z_1^{\beta_1} z_2^{\beta_2}$ in $\mathcal{F}_L^0$ with $k \leq 6$, exponents of monomials in $\mathrm{Ker}(L_0)$ in red. They are $1, z_1, x, x^3, x^3 z_1, x^3 z_1^3, x^3 z_1^4, x^4, x^4 z_1^3, x^6, x^6 z_1, x^6 z_1^3, x^6 z_1^4, x^6 z_1^6, x^6 z_1^7$.

Lemma 4.2. *Let $L \in \mathbb{k}[\![x]\!][\partial]$ be a linear differential operator and let ρ be one of its local exponents. The space $\mathcal{F}_L^\rho = \mathcal{F}$ is invariant under all differential operators with non-negative shift. In particular we have $L\mathcal{F} \subseteq \mathcal{F}$.*

Proof. We can rewrite any differential operator with non-negative shift in terms of the operator $\delta = x\partial$ instead of ∂, where the base change between $x^n\partial^n$ and δ^n is given by the Stirling numbers, see Remark 2.1. So we investigate the action of δ on a monomial $t^\rho x^i z^\beta \in \mathcal{F}$, where $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{N}^{(\mathbb{N})}$. We compute as in Lemma 3.1:

$$\delta(t^\rho x^k z^\beta) = x\partial(t^\rho x^k z^\beta) = t^\rho x^k \left((k+\rho)z^\beta + \sum_{j=1}^{n} \beta_j z_1^{\beta_1 - 1} \cdots z_j^{\beta_j - 1} z_{j+1}^{\beta_{j+1}} \cdots z_n^{\beta_n} \right)$$

We want to show that all exponents of monomials with non-zero coefficient in the sum above are in $\mathcal{B}(k)$. It is clear that $\beta \in \mathcal{B}(k)$ by assumption, so it is left to prove that if $\beta_j \not\equiv 0 \mod p$ then

$$(\beta_1 - 1, \ldots, \beta_j - 1, \beta_{j+1}, \ldots, \beta_n) \in \mathcal{B}(k)$$

for $j = 1, \ldots, n$. If $\beta_{l+1} \leq \beta_l/p$ then also $\beta_{l+1} - 1 \leq (\beta_l - 1)/p$ for $l < j$. It remains to show that $\beta_{j+1} > (\beta_j - 1)/p$ implies $\beta_j \equiv 0 \mod p$. For this we see that from

$$\beta_j - 1 < p\beta_{j+1} \leq \beta_j$$

it follows indeed that p divides $\beta_j = p\beta_{j+1}$. □

Proposition 4.3. *Let $L \in \Bbbk[\![x]\!][\partial]$ be a linear differential operator with local exponent ρ and associated ρ-function space $\mathcal{F}$. Then $L_0(\mathcal{F}) = x \cdot \mathcal{F}$.*

Proof. First we show that any monomial in $\mathcal{F}$ gets mapped to $x\cdot\mathcal{F}$ under L_0. Let $t^\rho x^k z^\beta \in \mathcal{F}$. By Lemma 3.4 we have

$$L_0(t^\rho x^k \mathrm{z}^\beta) = t^\rho x^k \left(\chi_L(\rho+k)\mathrm{z}^\beta + \chi_L'(\rho+k)x\partial(\mathrm{z}^\beta) + \ldots + \chi_L^{[n]}(\rho+k)(x\partial)^n(\mathrm{z}^\beta) \right).$$

By Lemma 4.2 this expression is contained in $\mathcal{F}$. The first $m_{\rho+k}$ summands of the sum vanish due to Lemma 3.5. In the remaining summands $x\partial$ is applied at least $m_{\rho+k}$ times to z^β, decreasing the exponent of z_1 by at least $m_{\rho+k}$. Thus for each monomial with non-zero coefficient in

$$\chi_L^{[m_{\rho+k}]}(\rho+k)(x\partial)^{m_{\rho+k}}(\mathrm{z}^\beta) + \ldots + \chi_L^{[n]}(\rho+k)(x\partial)^n(\mathrm{z}^\beta)$$

the exponents of z are in $\mathcal{B}(k-1)$ and thus $L_0(t^\rho x^k \mathrm{z}^\beta) \in x \cdot \mathcal{F}$.

Now we show that every monomial of $x \cdot \mathcal{F}$ is in the image of $\mathcal{F}$ under L_0. We proceed by induction on $e(\beta) = \overline{\beta_1} + p\overline{\beta_2} + p^2\overline{\beta_3} + \ldots$ Let $t^\rho x^{k+1} z^\beta \in x \cdot \mathcal{F}$; that is $\beta \in \mathcal{B}(k)$. Assume that $\rho + k + 1$ is an l-fold root of χ_L, where l is set equal to 0 if $\rho + k + 1$ is not a root at all. We define an element $\alpha \in \mathcal{B}(k+1)$ such that $L_0(t^\rho x^{k+1}\mathrm{z}^\alpha) = t^\rho x^{k+1}\mathrm{z}^\beta + r$, where r is a sum of smaller monomials with respect to $\prec_e$. Set

$$\alpha_1 = \beta_1 + l, \qquad \alpha_j = \beta_j + \lfloor \alpha_{j-1}/p \rfloor - \lfloor \beta_{j-1}/p \rfloor.$$

As $t^\rho x^k \mathrm{z}^\beta \in \mathcal{F}$, we have $\beta_1 < \xi(k)$ and therefore $\alpha_1 = \beta_1 + l < \xi(k+1)$. Moreover, we know that $\beta_j \leq \lfloor \beta_{j-1}/p \rfloor$ and therefore also $\alpha_j = \beta_j + \lfloor \alpha_{j-1}/p \rfloor - \lfloor \beta_{j-1}/p \rfloor \leq \alpha_{j-1}/p$. By construction we have $\alpha_1 = \beta_1 + l$ and thus $\alpha_1 < \xi(k+1)$. Altogether this proves $\alpha \in \mathcal{B}(k+1)$.

Finally we show that $L_0(t^\rho x^{k+1}\mathrm{z}^\alpha)$ is of the desired form. Again by Lemma 3.4 we have

$$L_0(t^\rho x^{k+1}\mathrm{z}^\alpha) = t^\rho x^{k+1} \left(\chi_L(\rho+k+1)\mathrm{z}^\alpha + \ldots + \chi_L^{[n]}(\rho+k+1)(x\partial)^n(\mathrm{z}^\alpha) \right)$$

As $\rho+k+1$ has multiplicity l as a zero of χ_L, the first l summands of this expansion vanish, according to Lemma 3.5. If one expands the further summands using the Leibniz rule one gets a sum of monomials of the form $c_\gamma t^\rho x^{k+1} \mathrm{z}^\gamma$, with $c_\gamma \in \Bbbk$. The exponents γ are in $\mathcal{B}(k)$ and by Lemma 3.1 we have $e(\gamma) \leq e(\alpha) - l = e(\beta)$. Only one of these summands fulfils $e(\gamma) = e(\beta)$. It is of the form $c_\beta t^\rho x^{k+1} \mathrm{z}^\beta$ by construction. Now by the induction hypothesis, all other summands are in the image of $\mathcal{F}$ under L_0; they are in $x \cdot \mathcal{F}$ because of Lemma 4.2. Thus, $t^\rho x^{k+1} \mathrm{z}^\beta \in L_0(\mathcal{F})$, which concludes the proof. □

Remark 4.4. The proof of the surjectivity of L_0 is constructive: For each monomial $t^\rho x^k z^\beta$ in $x \cdot \mathcal{F}$ one constructs a monomial $t^\rho x^k z^\alpha$ in $\mathcal{F}$, such that $L_0(t^\rho x^k z^\alpha) = ct^\rho x^k z^\beta + r$, where r is a sum of smaller monomials. If $r = 0$ we divide by c and are done. Otherwise we iterate the construction for all monomials in r and subtract the monomials obtained this way from $c^{-1} t^\rho x^k z^\alpha$. After at most $e(\beta)$ steps $r = 0$ and we have constructed an element of $\mathcal{F}$ which is sent to $t^\rho x^k z^\beta$ by L_0.

5 The normal form theorem

Recall that the constants of $\mathcal{R}$ are, according to Proposition 2.4, given by

$$\mathcal{C} = \bigoplus_{\rho \in \mathbb{F}_p} t^\rho x^{p-\rho} \Bbbk(\mathrm{z}^p)(\!(x^p)\!).$$

Further, recall that we have described in Proposition 3.6 the kernel of L_0 in $\mathcal{R}$. Let us investigate the situation in $\mathcal{F}$.

Lemma 5.1. *The kernel of the restriction of L_0 to $\mathcal{F} = \mathcal{F}_L^\rho$ is topologically spanned over $\Bbbk$ by monomials of the form $t^\rho x^k z^\beta$, where*

$$\beta \in \mathcal{B}(k) = \left\{ \beta \in \mathbb{N}^{(\mathbb{N})} \middle| \beta_1 < \xi(k), \beta_{j+1} \leq \beta_j / p \quad \forall j \in \mathbb{N} \right\}$$

with $\mathrm{e}(\beta) < m_{\rho+k}$. Consequently, a direct complement $\mathcal{H}$ of $\ker L_0|_{\mathcal{F}}$ is topologically spanned by monomials of the form $t^\rho x^k z^\beta$, where $\beta \in \mathcal{B}(k)$.

Proof. We have seen that $e(\beta)$ is the least number k, such that $(x\partial)^k \mathrm{z}^\beta = 0$. So every monomial $t^\rho x^k z^\beta$ with $e(\beta) < m_{\rho+k}$ is in the kernel of L_0 according to Lemma 3.4. Arguing as in the proof of Proposition 3.6 we see that those elements indeed span $\ker L_0|_{\mathcal{F}}$. □

Now we are ready to state and prove the normal form theorem.

Theorem 5.2 (Normal Form Theorem in Characteristic p)**.** *Let $\Bbbk$ be an algebraically closed field of characteristic 0. Let $L \in \Bbbk[\![x]\!][\partial]$ be a differential operator with initial form L_0 and shift $\tau = 0$ acting on $\mathcal{R}$. Let ρ be a local exponent of L at 0 and $\mathcal{F} = t^\rho \sum_{k=0}^\infty \bigoplus_{\beta \in \mathcal{B}(k)} \Bbbk \mathrm{z}^\beta x^k$ the associated ρ-function space.*

(i) The map $L_0|_{\mathcal{H}} : \mathcal{H} \to x \cdot \mathcal{F}$ is bijective and the composition of its inverse $(L_0|_{\mathcal{H}})^{-1} : x \cdot \mathcal{F} \to \mathcal{H}$ composed with the inclusion $\mathcal{H} \subseteq \mathcal{F}$ defines a $\mathcal{C}$-linear right inverse $S : x \cdot \mathcal{F} \to \mathcal{F}$ of L_0.

(ii) Let $T = L_0 - L : \mathcal{F} \to x \cdot \mathcal{F}$. Then the map

$$u = \mathrm{Id}_{\mathcal{F}} - S \circ T : \mathcal{F} \to \mathcal{F}$$

is a continuous $\mathcal{C}$-linear automorphism of $\mathcal{F}$ with inverse $v = \sum_{j=0}^\infty (S \circ T)^j : \mathcal{F} \to \mathcal{F}$.

(iii) The automorphism v of $\mathcal{F}$ transforms L into L_0, i.e.

$$L \circ v = L_0.$$

Proof. For (i) note that by Proposition 4.3 the map $L_0 : \mathcal{F} \to x \cdot \mathcal{F}$ is surjective and thus the restriction to a direct complement of its kernel is bijective. Clearly S then defines a right inverse of L_0. One easily checks that the construction of preimages of L_0 mentioned in Remark 4.4 is $\mathcal{C}$-linear.

The assertions (ii) and (iii) use modifications of the perturbation lemma to our setting, although we are not working in a normed vector space [Hau22]. We view elements of $\mathcal{F}$

as power series in x and equip $\mathcal{F}$ with the x-adic topology, which turns it into a complete metric space. The operator T has positive shift by definition and thus increases the order in x of a monomial $t^\rho x^k z^\beta$ and thus of any element of $\mathcal{F}$. The operator S maintains the order in x of a monomial as L_0 does so. T maps $\mathcal{F}$ to $x \cdot \mathcal{F} = \mathrm{Im}(L_0)$. Because of this and the completeness of $\mathcal{F}$ the series $v(f) = \sum_{j=0}^{\infty}(S \circ T)^j(f)$ is well-defined for each $f \in \mathcal{F}$. If f and g agree up to order N, so do $v(f)$ and $v(g)$, thus v is continuous. A standard argument shows that v is an inverse to u and thus u is a continuous automorphism. Both S and T are $\mathcal{C}$-linear and so is u.

It is left to show that v transforms L into L_0. As $L_0 \circ S = \mathrm{Id}_{x\cdot\mathcal{F}}$ we have $L_0 \circ S \circ L_0 = L_0$. Moreover $L = L_0 - T$, so $\mathrm{Im}L \subseteq \mathrm{Im}L_0$. This implies that $S \circ L$ is well-defined and $L_0 \circ S \circ L = L$ holds. Then

$$\begin{aligned}
L_0 \circ u &= L_0 \circ (\mathrm{Id}_{\mathcal{F}} - S \circ T) \\
&= L_0 \circ (\mathrm{Id}_{\mathcal{F}} - S \circ (L_0 - L)) \\
&= L_0 \circ (\mathrm{Id}_{\mathcal{F}} - S \circ L_0 + S \circ L) \\
&= L_0 - L_0 \circ S \circ L_0 + L_0 \circ S \circ L \\
&= L_0 \circ S \circ L \\
&= L.
\end{aligned}$$

Composing with v yields part (iii). □

6 Solutions of regular singular equations

The normal form theorem allows us to describe all solutions of differential equations with regular singularities.

Corollary 6.1. *Let $L \in \Bbbk[\![x]\!][\partial]$ be a linear differential operator with regular singularity at* 0 *acting on $\mathcal{R}$. Let $\rho \in \Bbbk$ be a local exponent of L. Denote by $u_\rho : \mathcal{F}_L^\rho \to \mathcal{F}_L^\rho$ the automorphism associated to ρ given in (ii) of the normal form theorem. The solutions of the differential equation $Ly = 0$ in $\mathcal{R}$ form an n-dimensional $\mathcal{C}$-vector space. A basis is given by*

$$y_{\rho,i} = u_\rho^{-1}(t^\rho z^{\beta(i)}),$$

where ρ varies over the local exponents of L at 0 *and $0 \le i < m_\rho$ and $\beta(i) = (i, \lfloor i/p \rfloor, \lfloor i/p^2 \rfloor, \ldots)$.*

Proof. By the normal form theorem and the description of the solutions of Euler equations (Proposition 3.6), we have

$$L(y_{\rho,i}) = L \circ u_\rho^{-1}(t^\rho z^{\beta(i)}) = L_0(t^\rho z^{\beta(i)}) = 0,$$

so these functions clearly are solutions of the differential equation $Ly = 0$. Assume now that there is another solution y that is linearly independent to the solutions $y_{\rho,i}$ over $\mathcal{C}$. Again, as L commutes with the direct sum decomposition of

$$\mathcal{R} = \bigoplus_{\rho \in \Bbbk} t^\rho \Bbbk(\mathrm{z})(\!(x)\!)$$

and upon multiplication with constants of the form x^{kp} we may assume that y is of the form $y = t^\rho \left(\sum_{k=0}^\infty f_k(\mathrm{z}) x^k\right)$ for $f_k \in \Bbbk(\mathrm{z})$. If we write $L = L_0 - T$ we obtain

$$L_0 y - Ty = 0,$$

where T has positive shift, i.e., it strictly increases the order in x. Thus, $t^\rho f_0(\mathrm{z})$ is a solution to the Euler equation $Ly = 0$ and therefore

$$t^\rho f_0(\mathrm{z}) = \sum_{(\sigma,i)} c_{\sigma,i} t^\sigma \mathrm{z}^{\beta_i},$$

where σ varies over the local exponents, $0 \le i < m_\sigma$, and $c_{\sigma,i} \in \mathcal{C}$ is homogeneous of order 0 in x. We compute

$$L\left(y - \sum_{(\sigma,i)} c_{\sigma,i} y_{\rho,i}\right) = L\left(-\sum_{(\sigma,i)} c_{\sigma,i} u_\sigma^{-1}(t^\sigma \mathrm{z}^{\beta_i})\right) = -\sum_{(\sigma,i)} c_{\sigma,i} L(u_\sigma^{-1}(t^\rho \mathrm{z}^{\beta(i)})) = 0.$$

Note that for all $f \in \mathcal{F}$ we have $\mathrm{ord}_x(f - u(f)) > \mathrm{ord}_x f$, i.e., the monomial of order 0 remains unchanged under u. So $y - \sum_{(\sigma,i)} c_{\sigma,i} y_{\sigma,i}$ has positive order in x. Iteration yields constants $d_{\sigma,i} \in \mathcal{C}$ with $y = \sum_{(\sigma,i)} d_{\sigma,i} y_{\sigma,i}$. Thus, y is a linear combination of $y_{\sigma,i}$. Conversely, any such linear combination is a solution of $Ly = 0$. This proves that the solutions of $Ly = 0$ in $\mathcal{R}$ form an n-dimensional $\mathcal{C}$-vector space with basis $y_{\rho,i}$, where ρ varies over the local exponents and $0 \le i < m_\rho$. □

Remark 6.2. We have assumed for convenience that our field $\Bbbk$ is algebraically closed. If this is not the case, e.g., in the case of a finite field $\mathbb{F}_p$, there is no need to pass to the entire algebraic closure. In the constructions involved in the normal form theorem for an operator L we have to find the roots of the characteristic polynomial $\chi_L \in \Bbbk[s]$, the local exponents ρ. Further we have to evaluate the characteristic polynomial at the values $\rho+k$ for elements k of the prime field of $\Bbbk$. Thus, if χ_L splits over $\Bbbk$ the normal form theorem works without problems within $\Bbbk$. Otherwise it is sufficient to pass to a splitting field of χ_L to describe a full basis of solutions.

Example 6.3 (Exponential function in characteristic 3)**.** We consider the equation $y' = y$. Solving over the holomorphic functions, or in $\mathbb{C}[\![x]\!]$ one obtains the exponential function as a solution. However there is no reduction of this function modulo any prime, as all prime numbers appear in the denominators of the expansion of the exponential function. But one can obtain solutions modulo p for any prime in $\mathcal{R}$ using the normal form theorem. Pick for example $p = 3$. Write $L = x\partial - x = \delta - x$, so our equation is equivalent to $Ly = 0$. The only local exponent of the equation is 0, thus one needs to compute the series

$$\sum_{n=0}^{\infty}(S \circ T)^n(1).$$

The operator T is simply given by the multiplication by x, where S is, as constructed above, a right-inverse of $L_0 = x\partial$. One obtains:

$$\begin{aligned}
(S\circ T)^1(1) &= S(x) &&= x,\\
(S\circ T)^2(1) &= S(x^2) &&= 2x^2,\\
(S\circ T)^3(1) &= S(2x^3) &&= 2x^3 z_1,\\
(S\circ T)^4(1) &= S(2x^4 z_1) &&= 2x^4 z_1 + x^4,\\
(S\circ T)^5(1) &= S(2x^5 z_1 + x^5) &&= x^5 z_1,\\
(S\circ T)^6(1) &= S(x^6 z_1) &&= 2x^6 z_1^2,\\
(S\circ T)^7(1) &= S(2x^7 z_1^2) &&= 2x^7 z_1^2 + 2x^7 z_1 + x^7,\\
(S\circ T)^8(1) &= S(2x^8 z_1^2 + 2x^8 z_1 + x^8) &&= x^8 z_1^2 + 2x^8,\\
(S\circ T)^9(1) &= S(x^9 z_1^2 + 2x^9) &&= x^9 z_1^3 z_2 + 2x^9 z_1.
\end{aligned}$$

One gets the solution

$$1+x+2x^2+2x^3z_1+x^4(1+2z_1)+x^5z_1+2x^6z_1^2+x^7(1+2z_1+2z_1^2)+x^8(2+z_1^2)+x^9(2z_1+z_1^3z_2)+\dots,$$

which could be considered as the exponential function in characteristic 3. Note that obtaining the rightmost column needs some computational effort. One has to follow the steps described in Remark 4.4. There seems to be no obvious pattern in the coefficients of the obtained power series.

Similarly, one can compute the exponential functions $\exp_p$ for other characteristics p. For $p = 2$ the first terms are

$$1+x+x^2z_1+x^3(z_1+1)+x^4(z_1^2z_2+z_1)+x^5z_1^2z_2+x^6(z_1^3z_2+z_1^3)+x^7(z_1^3z_2+z_1^2z_2+z_1^3+z_1+1)+\dots$$

and for $p = 5$ we get

$$1+x+3x^2+x^3+4x^4+4x^5z_1+x^6(4z_1+1)+x^7(2z_1+2)+x^8(4z_1+1)+x^9z_1+3x^{10}z_1^2+\dots$$

Example 6.4. We consider the minimal complex differential equation $Ly = 0$ for

$$y(x) = -\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots \in \mathbb{C}[\![x]\!].$$

It is given by $L = x^2\partial^2 - (x^2\partial + x^3\partial^3)$. The local exponents are $0, 1$ and a basis of solutions in $\mathbb{C}[\![x]\!]$ is given by $\{1, y\}$. Reducing L modulo a prime number p one again finds the local exponents $0, 1$. Clearly $y_{0,0} = u_0^{-1}(1) = 1$. Further we compute

$$y_{1,0} = u_1^{-1}(t^1) = \sum_{k=0}^{\infty}(S \circ T)(t^1) = t\left(1 + \frac{x}{2} + \frac{x^2}{3} + \ldots + \frac{x^{p-2}}{p-1} + x^{p-1}z_1\right).$$

Here only adjoining the variable z_1 instead of countably many z_i is necessary to obtain enough solutions. In the next section we will describe the class of operators, where the addition of finitely many of the variables z_i suffice.

Remark 6.5. (i) The space $\mathcal{R}$ provides us with n linearly independent solutions for any operator with a regular singularity at 0 in characteristic p. It is minimal in the following sense: we only introduce a new variable z_i, when the algorithm constructing solutions would get "stuck", i.e., when we would be forced to divide by p. However, it is possible to choose a system of representatives $\Lambda \subseteq \mathbb{k}$ of the set $\mathbb{k}/\mathbb{F}_p$. Without loss of generality assume that $0 \in \Lambda$. We can define

$$\widetilde{\mathcal{R}} := \bigoplus_{\rho \in \Lambda} t^\rho \mathbb{k}(\mathrm{z})(\!(x)\!),$$

which suffices to construct solutions to any linear differential equation $Ly = 0$ having a regular singularity at 0, similar to above. For example, if $\sigma \in \mathbb{k}$ is a local exponent of an Euler operator and there is $\rho \in \Lambda$ with $\rho + k = \sigma$ for some $\sigma \in \mathbb{F}_p$ and $k \in \mathbb{F}_p$, then $t^\rho x^k$ is a solution of the equation $Ly = 0$. This construction has the advantage that the constants are much simpler, as they are given by

$$\mathcal{C}_{\widetilde{\mathcal{R}}} = \mathbb{k}(\mathrm{z}^p)(\!(x^p)\!).$$

However it involves a choice of a system of representatives of $\mathbb{k}/\mathbb{F}_p$.

(ii) In characteristic 0 a minimal extension of $\mathbb{k}(\!(x)\!)$ in which every regular singular equation has a full basis of solutions is the universal Picard-Vessiot ring or field for differential equations with regular singularities, discussed in [SP03].

7 Equations with local exponents in the prime field

The situation becomes easier if we consider a linear differential equation $Ly = 0$, whose local exponents are all contained in the prime field $\mathbb{F}_p \subseteq \Bbbk$. In this case there is no need to introduce monomials t^ρ with exponents $\rho \in \Bbbk$. We define the differential subfield $\mathcal{K}$ of $\mathcal{R}$ as

$$\mathcal{K} := \Bbbk(\mathrm{z})(\!(x)\!).$$

One easily checks that $\mathcal{K}$ is indeed differentially closed with respect to $\partial_{\mathcal{R}}$. Moreover, its field of constants is given by

$$\mathcal{C}_{\mathcal{K}} = \Bbbk(\mathrm{z}^p)(\!(x^p)\!).$$

The assumption on the local exponents allows one to modify the normal form theorem to use the function space

$$\mathcal{G}_L^\rho := x^\rho \sum_{k=0}^{\infty} \bigoplus_{\beta \in \mathcal{B}(k)} \Bbbk \mathrm{z}^\beta x^k,$$

instead of

$$\mathcal{F}_L^\rho = t^\rho \sum_{k=0}^{\infty} \bigoplus_{\beta \in \mathcal{B}(k)} \Bbbk \mathrm{z}^\beta x^k,$$

by "substituting $t = x$" and analogously one obtains a full basis of solutions over $\mathcal{C}_{\mathcal{K}}$ in $\mathcal{K}$: For each local exponent ρ one computes $u^{-1}(x^\rho)$ instead of $u^{-1}(t^\rho)$, where u is the automorphism described in the normal form theorem.

One class of operators with all local exponents in the prime field of $\Bbbk$ are operators with *nilpotent p-curvature.* The *p-curvature* of an operator L can be defined as the action of multiplication by ∂^p on the space $\Bbbk[x][\partial]/\Bbbk[x][\partial]L$. An alternate description of these operators was provided by Honda [Hon81]: We say that an equation $Ly = 0$ of order n has *sufficiently many solutions in the weak sense* if $Ly = 0$ has one solution $y_1 \in \Bbbk[\![x]\!]$ and recursively the equation in u' of order $n-1$ obtained from $Ly = 0$ by the ansatz $y = y_1 u$ has sufficiently many solutions in the weak sense.

Theorem 7.1 (Honda, [Hon81], p. 201)**.** *A linear differential operator L has nilpotent p-curvature if and only if the equation $Ly = 0$ has sufficiently many solutions in the weak sense.*

And indeed, the following theorem holds:

Theorem 7.2. *Let $L \in \Bbbk[x][\partial]$ be a differential operator with nilpotent p-curvature. Then its local exponents are in the prime field $\mathbb{F}_p \subseteq \Bbbk$.*

For a proof, see [Hon81] p. 179. Further, there is another interesting characterisation of operators with nilpotent p-curvature due to Dwork [Dwo90].

Theorem 7.3 (Dwork, [Dwo90], p. 756)**.** *An operator $L \in \Bbbk[x][\partial]$ has nilpotent p-curvature if and only if there is $l \in \mathbb{N}$ such that $Ly = 0$ has a full basis of solutions in $\Bbbk(z_1, \ldots, z_l)(\!(x)\!)$ over its field of constants $\Bbbk(z_1^p, \ldots, z_l^p)(\!(x^p)\!)$.*

This is a generalisation of a result of Honda, who proved the result for $l = 1$ and operators of order smaller than p, see [Hon81] p. 186.

For example, the operator annihilating $\log(1-x)$, discussed in Example 6.4, has nilpotent p-curvature.

8 Polynomial solutions

It is well-known that if a Laurent series solution $y \in \mathbb{F}_p((x))$ to $Ly = 0$ for an operator $L \in \mathbb{F}_p[x][\partial]$ with polynomial coefficients exists, then there already exists a polynomial solution to the equation, e.g. see [Hon81] p. 174. We generalize the result to solutions avoiding all but finitely many of the variables z_i.

Lemma 8.1. *Let $\Bbbk$ be a field of characteristic p. Let $L \in \Bbbk[x][\partial]$ be a differential operator with local exponent $\rho \in \Bbbk$. Let $y \in t^\rho \Bbbk[z_1, \dots, z_l][\![x]\!]$ a solution of the differential equation $Ly = 0$. Let $c \in \mathbb{N}$. Then there exists a polynomial $q \in \Bbbk[x, z_1, \dots, z_l]$, such that $L(t^\rho q) = 0$ and $y - t^\rho q \in t^\rho x^{c+1} \Bbbk[z_1, \dots, z_l][\![x]\!]$. In particular, if a basis of power series solutions of $Ly = 0$ in $\bigoplus_\rho t^\rho \Bbbk[z_1, \dots, z_l][\![x]\!]$ exists, then there already exists a basis of polynomial solutions in $\bigoplus_\rho t^\rho \Bbbk[z_1, \dots, z_l, x]$.*

We will give two proofs of the statement. The first one is an adaptation of the proof presented by Honda.

Proof 1. Let $y = t^\rho \left(a_0 + a_1 x + a_2 x^2 + \dots\right) \in t^\rho \Bbbk[\![x]\!]$ with $a_i \in \Bbbk[z_1, \dots, z_l]$ and $a_0 \neq 0$. We write L as the sum of finitely many Euler operators and let j be the maximal shift of them. Thus, if j consecutive coefficients a_i of a solution y vanish, say $a_{N+1}, \dots, a_{N+j}$, then

$$t^\rho \left(a_0 + a_1 x + \dots + a_N x^N\right)$$

is a solution of the equation as well. Indeed, this can be seen by rewriting the equation as a recursion for the coefficients a_i.

The space of j-tuples of elements of $\Bbbk[z_1, \dots, z_l]$ is jp^l-dimensional, hence finite dimensional, over $\Bbbk[z_1^p, \dots, z_l^p]$. Let $m = jp^l$. So there are $k_1 < \dots < k_m < k_{m+1}$ such that $(k_{m+1} - k_m)p > c$ and $b_1, \dots, b_m \in \Bbbk[z_1^p, \dots, z_l^p]$ with

$$\begin{aligned} &(a_{pk_{m+1}}, a_{pk_{m+1}+1}, \dots, a_{pk_{m+1}+j-1}) = \\ &= b_1(a_{pk_1}, a_{pk_1+1}, \dots, a_{pk_1+j-1}) + \dots + b_m(a_{pk_m}, a_{pk_m+1}, \dots, a_{pk_m+j-1}). \end{aligned}$$

Thus for

$$q \coloneqq y \cdot \left(1 - b_1 x^{p(k_{m+1}-k_1)} - \dots - b_m x^{p(k_{m+1}-k_m)}\right)$$

j consecutive coefficients vanish. Moreover, it is the product of y and a constant in $\Bbbk[z_1^p, \dots, z_l^p, x^p]$, so it is a solution and it agrees up to order c with y. This proves the assertion. □

Proof 2. (Hauser). We consider $t^\rho \Bbbk[z_1, \dots, z_l][\![x]\!]$ as a free $\Bbbk[z_1^p, \dots, z_l^p][\![x^p]\!]$-module of rank p^{l+1} with basis $\mathcal{G} = \{t^\rho x^k z^\beta | k \in \{0, 1, \dots, p-1\}, \beta \in \{0, 1, \dots, p-1\}^l\}$. Without loss of generality assume that $\rho = 0$. We can write

$$y(x) = \sum_{g \in \mathcal{G}} y_g(z_1^p, \dots, z_l^p, x^p) g$$

with series $y_g \in \Bbbk[z_1, \dots, z_l][\![x]\!]$. Then

$$Ly = \sum_{g \in \mathcal{G}} y_g(z_1^p, \dots, z_l^p, x^p) L(g) = 0$$

implies that the series $y_g(z_1^p, \ldots, z_l^p, x^p)$ form a $\Bbbk[z_1^p, \ldots, z_l^p][\![x^p]\!]$-linear relation between the polynomials $L(g)$ in the finite free $\Bbbk[z_1^p, \ldots, z_l^p, x^p]$-module $\Bbbk[z_1, \ldots, z_l, x]$ for $g \in \mathcal{G}$. By the flatness of $\Bbbk[z_1^p, \ldots, z_l^p][\![x^p]\!]$ over $\Bbbk[z_1^p, \ldots, z_l^p, x^p]$ there are polynomials $q_g(z_1^p, \ldots, z_l^p, x^p) \in \Bbbk[z_1^p, \ldots, z_l^p, x^p]$ approximating $y_g(z_1^p, \ldots, z_l^p, x^p)$ up to any prescribed degree and such that

$$\sum_{g \in \mathcal{G}} q_g(z_1^p, \ldots, z_l^p, x^p) L(g) = 0.$$

Now set

$$q(z_1, \ldots, z_l, x) = \sum_{g \in \mathcal{G}} q_g(z_1^p, \ldots, z_l^p, x^p) g$$

to get the required polynomial solution of $Ly = 0$. □

Remark 8.2. (i) Assume that $L \in \Bbbk[x][\partial]$, where $\Bbbk$ is a finite field of characteristic p with algebraic closure $\overline{\Bbbk}$. Then if $y \in t^\rho \overline{\Bbbk}[\![x]\!]$ is a solution obtained by the normal form theorem, we already have $y \in t^\rho \Bbbk(\rho)[\![x]\!]$, where $\Bbbk(\rho)$ is a finite extension of $\Bbbk$. Recall the operators S and T from the normal form theorem: S is a right inverse to L_0 and $T = L - L_0$. It holds $S(x^{\rho+k+p}) = x^p S(x^{\rho+k})$ and $T(x^{\rho+k+p}) = x^p T(x^{\rho+k})$. There are only finitely many n-tuples of elements from $\Bbbk(\rho)$. Write $y = t^\rho(a_0 + a_1 + a_2x^2 + \ldots)$. Two n-tuples of consecutive coefficients a_i of y, starting at powers of an index divisible by p, have to agree. Thus the sequence $(a_i)_{i \in \mathbb{N}}$ becomes periodic. Hence it suffices to take a suitable sufficiently large k to obtain a polynomial solution $(1 - x^{kp})y$ of $Ly = 0$, which approximates y to a prescribed degree c, as in the first proof of Lemma 8.1.

(ii) The algorithm from the normal form theorem may but need not provide us with a polynomial solution of $Ly = 0$, when applied to an operator L in $\mathbb{F}_p[x][\partial]$. To see this consider the following two examples:

(a) Let $L = x\partial - x^2\partial - x$ and

$$y_L(x) = \frac{1}{1-x}$$

the solution of the equation $Ly = 0$. Over $\mathbb{F}_p$ we compute using the algorithm from the normal form theorem with $L_0 = x\partial$ and $T = x^2\partial + x$ and obtain $u^{-1}(1) = \sum_{k=0}^\infty (S_L \circ T_L)^k = 1 + x + x^2 + \ldots + x^{p-1} \in \mathbb{F}_p[x]$, a polynomial solution.

So we obtain $u^{-1}(1) = \sum_{k=0}^\infty (S_L \circ T_L)^k = 1 + x + x^2 + \ldots + x^{p-1} \in \mathbb{F}_p[x]$, a polynomial solution.

(b) Let now $M = (-x - 2x^4) + (x + x^2 + -2x^4 - x^5 + x^7)\partial$. The equation $My = 0$ is satisfied by the algebraic function $1 + \frac{x}{1-x^3}$. Reducing modulo 3 we get

$$T = (x + 2x^2\partial) + (2x^4\partial) + (2x^4 + x^5\partial) + (2x^7\partial) = T_1 + T_3 + T_4 + T_6$$

and the initial form $M_0 = x\partial$. We compute the solution

$$u^{-1}(1) = \sum_{i=0}^\infty a_i x^i \sum_{i=0}^\infty (S \circ T)^i(1) = 1 + x + x^4 + x^7 + x^{10} + \ldots$$

Because the maximal shift of T is 6 and $(a_1, a_2, a_3, a_4, a_5, a_6) = (a_4, a_5, a_6, a_7, a_8, a_9)$ the sequence of coefficients of this series becomes periodic, as described in (i), with period length 3. Thus, the solution obtained by the normal form theorem in characteristic p agrees with the reduction modulo p of the solution obtained in characteristic 0.

(iii) The latter of the two examples from above illustrates that the degree of a minimal degree polynomial solution of a differential equation in characteristic p need not be $p-1$, as one could expect. Indeed using the periodicity of the coefficients of the solution from above one obtains that

$$\widehat{y}(x) = u^{-1}(1) - x^3 u^{-1}(1) = 1 + x - x^3$$

is a polynomial solution. Any other polynomial solution has to be a multiple of $\widehat{y}$ with a constant. Indeed, making the ansatz

$$(1 + x - x^3) \cdot (1 + c_1 x^3 + c_2 x^6 + \cdots) = 1 + ax + bx^2$$

one immediately obtains $c_1 = 1$, which leads to a contradiction. Therefore no polynomial solution of degree less than 3 exists.

9 The Grothendieck p-curvature conjecture

We now turn to the Grothendieck p-curvature conjecture and want to discuss a prospective approach using the normal form theorems in characteristic 0 and p. In the following let $L \in \mathbb{Q}[x][\partial]$ be a differential operator defined over $\mathbb{Q}$ and denote by $L_p \in \mathbb{F}_p$ the differential operator that arises from reducing the coefficients of L modulo p, whenever this is defined. The reduction L_p is defined for all but finitely many prime numbers p. We are interested in the interplay between solutions of the equations $Ly = 0$ and $L_p y = 0$. Most prominent here is the Grothendieck p-curvature conjecture. A very simple formulation is the following:

Conjecture 9.1 (Grothendieck p-curvature conjecture, [Hon81])**.** *Let $L \in \mathbb{Q}[x][\partial]$. Assume that $L_p y = 0$ has a basis of $\mathbb{F}_p[\![x^p]\!]$-linearly independent solutions in $\mathbb{F}_p[\![x]\!]$ for almost all prime numbers p. Then there exists a basis of $\mathbb{Q}$-linearly independent algebraic solutions of $Ly = 0$ in $\mathbb{Q}[\![x]\!]$.*

Remark 9.2. (i) One can easily generalize this conjecture to number fields, by replacing $\mathbb{Q}$ with $K = \mathbb{Q}(\alpha)$ and $\mathbb{F}_p$ by the residue fields modulo prime ideals $\mathfrak{p} \subseteq \mathcal{O}_K$.

(ii) Let $\Bbbk$ be a field of characteristic p. Recall that the p-curvature of a differential operator $L \in \Bbbk[\![x]\!][\partial]$ is the action of ∂^p on the space $\Bbbk[\![x]\!][\partial]/\Bbbk[\![x]\!][\partial]\cdot L$. A lemma of Cartier shows that L has a basis of solutions in $\Bbbk[\![x]\!]$ if and only if the p-curvature of L vanishes, or equivalently L divides ∂^p. It can be found in an abstract formulation for example in [Kat70], or more "down-to-earth" in [SP03]. This explains the name of the conjecture.

A weaker statement than the Grothendieck conjecture was conjectured by Bézivin.

Conjecture 9.3 (Bézivin conjecture, [Béz91])**.** *Let $L \in \mathbb{Q}[x][\partial]$ be a differential operator. Assume that $Ly = 0$ has a basis of $\mathbb{Q}$-linearly independent solutions in $\mathbb{Z}[\![x]\!]$. Then these solutions are algebraic over $\mathbb{Q}(x)$.*

Lemma 9.4. *The validity of the Grothendieck p-curvature conjecture implies the validity of the Bézivin conjecture.*

In other words: The hypothesis of the Bézivin conjecture implies the hypothesis of the Grothendieck p-curvature conjecture.

Proof. Assume that $y \in \mathbb{Z}[\![x]\!]$ is an integral solution of $Ly = 0$. Its reduction modulo all prime numbers is well-defined and a solution to $L_p y = 0$. For p larger than the maximal difference of the local exponents of L, a basis of solutions of $Ly = 0$ gets mapped by reduction to a basis of solution modulo p. The condition on p is necessary to ensure that the reductions of the solutions do not become linearly dependent over $\mathbb{F}_p(\!(x^p)\!)$. Thus by the Grothendieck p-curvature conjecture $Ly = 0$ has a basis of algebraic solutions and y, as a linear combination of those algebraic solutions, is algebraic itself. □

A substantial advance towards the Grothendieck p-curvature conjecture would be to prove the inverse implication of Lemma 9.4: in fact it would transfer the problem from positive characteristic to characteristic 0. To approach the converse implication, it is reasonable to compare the algorithm of the normal form theorem in characteristic 0 applied to an operator

L to the algorithm of the normal form theorem in characteristic p, applied to the reduction L_p of the operator L modulo p. We investigate in the next paragraphs how the normal form theorems could be used to achieve this. For this we state the normal form theorem in characteristic 0 and a number theoretic result, we will use:

Theorem 9.5 (Normal form theorem in characteristic 0, Hauser, [Hau22])**.** *Let K be a field of characteristic 0. Let $L \in K[\![x]\!][\partial]$ be a linear differential operator with power series coefficients, initial form L_0 and shift $\tau = 0$. Denote by $\Omega = \{\rho_1, \ldots, \rho_r\}$ a set of increasingly ordered local exponents ρ_k, with integer differences and multiplicities m_k. Set $n_k = m_1 + \ldots + m_k$ and*

$$\mathcal{F} = \mathcal{F}_L^\Omega = \sum_{k=1}^{r} K[\![x]\!]x^{\rho_k}[z]_{<n_k}.$$

Let L, L_0 act on $\mathcal{F}$ via $\partial x = 1$ and $\partial z = x^{-1}$.

(i) The map L sends $\mathcal{F}$ into $x \cdot \mathcal{F}$.

(ii) The map L_0 has image $x \cdot \mathcal{F}$. Its kernel $\ker(L_0) = \bigoplus_{k=1}^r Kx^{\rho_k}[z]_{<m_k}$ has direct complement

$$\mathcal{H} = \bigoplus_{k=2}^{r} \bigoplus_{i=m_k}^{n_k-1} Kx^{\rho_k} z^i \oplus \bigoplus_{k=1}^{r-1} \bigoplus_{e=1}^{\rho_{k+1}-\rho_k-1} Kx^{\rho+e}[z]_{<n_k} \oplus \bigoplus_{i=0}^{n_r-1} K[\![x]\!]x^{\rho_r+1}z^i$$

in $\mathcal{F}$. The restriction of L_0 to $\mathcal{H}$ defines a linear automorphism between $\mathcal{H}$ and $x \cdot \mathcal{F}$.

(iii) The composition of the inverse $(L_0|_{\mathcal{H}})^{-1} : x \cdot \mathcal{F} \to \mathcal{H}$ of $L_0|_{\mathcal{H}}$ with the inclusion $\mathcal{H} \hookrightarrow \mathcal{F}$ defines a right inverse $S : x \cdot \mathcal{F} \to \mathcal{F}$ of L_0. Let $T : \mathcal{F} \to x \cdot \mathcal{F} = L_0 - L$. The map

$$u = \mathrm{Id}_{\mathcal{F}} - S \circ T : \mathcal{F} \to \mathcal{F}$$

is a linear automorphism of $\mathcal{F}$, with inverse $v = u^{-1} = \sum_{k=0}^{\infty}(S \circ T)^k : \mathcal{F} \to \mathcal{F}$.

(iv) The automorphism v of $\mathcal{F}$ transforms L into L_0:

$$L \circ v = L_0.$$

(v) The space of solutions of the equation $L_0 y = 0$ in $\mathcal{F}$ is given by

$$\ker(L_0) = \bigoplus_{\rho \in \Omega} \bigoplus_{i=0}^{m_\rho - 1} Kx^\rho z^i.$$

(vi) Assume that L has a regular singularity at 0. Then a K-basis of solutions of $Ly = 0$ at 0 is given by

$$y_{\rho,i} = u_\Omega^{-1}(x^\rho z^i)$$

where Ω varies over all sets of local exponents, u_Ω is the automorphism of assertion (iii) corresponding to Ω, $\rho \in \Omega$ is a local exponent and $0 \le i < m_\rho$.

For a proof see [Hau22].

Theorem 9.6 (Kronecker, [Kro80], Frobenius, [Fro96]). *Let $f \in \mathbb{Q}[x]$ be a polynomial of degree n, let $s \in \mathbb{N}$ and $n_1, \ldots, n_s$ with $n_1 + \ldots + n_s = n$. The density of prime numbers p for which the reduction of f splits into k factors of degrees $f_1, \ldots, f_k$ is equal to the number of permutations of the roots of f in the Galois group of f consisting of s cycles of lengths $f_1, \ldots, f_s$. In particular, f splits into linear factors over $\mathbb{Q}[x]$ if and only if its reduction modulo p splits in $\mathbb{F}_p[x]$ into linear factors for almost all primes p.*

This version was proven by Frobenius, while similar results were formulated by Kronecker before. It is also an easy corollary of the Chebotarev density theorem.

We now describe consequences of the hypothesis of the Grothendieck p-curvature conjecture. They were already collected by Honda and we refer for parts of the proof to his article. However, for the last assertion we give a different proof. It compares the two algorithms obtained from the normal form theorems in characteristics 0 and p. This approach demonstrates how the normal form theorems could be used to show the equivalence of the Grothendieck p-curvature conjecture and the Bézivin conjecture.

We say that a power series $g \in \mathbb{F}_p[\mathrm{z}][\![x]\!]$ *depends on logarithms*, if it is not the product of a power series in $\mathbb{F}_p[\![x]\!]$ and a constant from $\mathbb{F}_p[\mathrm{z}^p][\![x^p]\!]$. In particular, if a power series is independent of logarithms, every exponent of the variables z_i is divisible by p. If $L \in \mathbb{F}_p[x][\partial]$ is an operator and the equation $Ly = 0$ has a basis of solutions in $\mathbb{F}_p[\![x]\!]$ then any solution of $Ly = 0$ is independent of logarithms.

Proposition 9.7 (Honda, [Hon81], p. 177ff., p. 190ff.). *Let $L \in \mathbb{Q}[x][\partial]$ be an operator of order n. Assume that $L_p y = 0$ has a basis of n $\mathbb{F}_p[\![x^p]\!]$-linearly independent power series solutions in $\mathbb{F}_p[\![x]\!]$ for almost all prime numbers p. Then*

(i) The operator L has a regular singularity at 0.

(ii) The local exponents of L at 0 are pairwise distinct rational numbers.

(iii) There is a basis of Puiseaux series solutions of $Ly = 0$ in $\sum_{\rho_i} x^{\rho_i}\mathbb{Q}[\![x]\!]$, where ρ_i ranges over the local exponents of L. In particular, there is a basis of n solution in $\mathcal{R}$, independent of the variables t and z_i.

Proof. For (i) we only sketch the reasoning presented by Honda. One first proves that the reduction L_p has a regular singularity at 0 for all p for which it has a full basis of solutions. For the details see Honda [Hon81], where the regularity is proven for operators L_p having sufficiently many solutions in the weak sense for almost all primes p. This is a weaker assumption than having a basis of solutions in $\mathbb{F}_p[\![x]\!]$: Indeed, $L_p y = 0$ having sufficiently many solutions in the weak sense is equivalent to the nilpotence of its p-curvature, by 7.1. On the other hand, the existence of basis of a basis of n solutions in $\mathbb{F}_p[\![x]\!]$ is equivalent to the vanishing of the p-curvature of L_p, by Cartier's lemma. So we may assume that L_p has a regular singularity for almost all p. Equivalently, the initial form of L_p has order n for almost all p. So the initial form of L has order n and thus the singularity of L is regular.

We proceed by showing (ii). As a consequence of (i) there are n local exponents of L, counted with multiplicity. Moreover for almost all prime numbers the local exponents of L_p have to be elements of the prime field. Indeed for any local exponent $\rho \notin \mathbb{F}_p$ we obtain using

Corollary 6.1 a solution of the form $t^\rho f \in t^\rho \mathbb{F}[\![x]\!]$, contradicting the existence of a basis of n solutions of $L_p y = 0$ in $\mathbb{F}[\![x]\!]$.

We show, as Honda [Hon81], that the local exponents of L are pairwise incongruent modulo almost all prime numbers. The indicial polynomial χ_L of L has coefficients in $\mathbb{Q}$ and it splits into linear factors over $\mathbb{F}_p$ when reduced modulo p for almost all primes p. Thus, by Theorem 9.6, χ_L splits into linear factors over $\mathbb{Q}$ and so all local exponents are rational. Assume now that two local exponents are congruent modulo some p. Then their reduction modulo p is a local exponent of L_p of multiplicity at least 2. So, Corollary 6.1 together with the remarks in section 7 to avoid the variable t yield a solution of the form $u^{-1}(x^\rho z_1)$, where u is the automorphism associated to the function space $\mathcal{G}_L^\rho$. This solution is in contradiction to our assumption of a basis of solutions in $\mathbb{F}_p[\![x]\!]$. In particular all local exponents in characteristic 0 have to be distinct.

For (iii) the normal form theorem in characteristic 0 provides us with a basis of solutions for $Ly = 0$ in

$$\sum_{\rho_i} x^{\rho_i} \mathbb{Q}[\![x]\!][z],$$

as all local exponents are rational numbers. So we only have to prove that the solutions of $Ly = 0$ are independent of z. Assume there is a solution f involving a logarithm, i.e., $f \in \sum_\rho x^\rho \mathbb{Q}[z][\![x]\!] \setminus \sum_\rho x^\rho \mathbb{Q}[\![x]\!]$. Without loss of generality we may assume that

$$f = u^{-1}(x^\rho) = x^\rho(1 + a_1 x + a_2 x^2 + \ldots)$$

for some local exponent ρ of L and some $a_i \in \mathbb{Q}[z]$. Let $k \in \mathbb{N}$ be minimal, such that a_k is dependent on z.

We will proceed by choosing a suitable prime p and a solution g of $L_p y = 0$, which agrees with the reduction of f up to degree $k - 1$. This we will use show that the g necessarily depends on logarithms, a contradiction.

We choose a prime p, subject to the following conditions:

- p is larger than the order n of L.
- There is a basis of solutions of $L_p y = 0$ in $\mathbb{F}_p[\![x]\!]$.
- p does not divide any of the denominators of the local exponents of L, which are rational by (ii).
- p does not divide any of the denominators of $a_1, \ldots, a_k$.

We only excluded finitely many primes, so almost all p fulfil this.

Let Λ be the set of positive integers l smaller than k such that $\rho + l$ is a local exponent of L_p. Here we write ρ as well for its reduction modulo p, an element of $\{0, 1, \ldots, p-1\}$. We define

$$g = u_p^{-1}\left(x^\rho\left(1 + \sum_{l\in\Lambda} \overline{a_l} x^l\right)\right) = x^\rho(1 + b_1 x + b_2 x^2 + \ldots),$$

where u_p is the automorphism of $\mathcal{G}_{L_p}^\rho$ from the normal form theorem, Theorem 5.2. We show now that g is a solution of $L_p y = 0$. Recall that $L_p \circ u_p^{-1} = L_{p,0}$, where $L_{p,0}$ denotes the initial form of L_p. The monomial $x^{\rho+l}$ is a solution of $L_{p,0}y = 0$ whenever $\rho + l$ is a local exponents of L_p. So indeed $Lg = 0$ holds.

Next we prove inductively that $b_i = \overline{a_i}$. For this we first investigate how the operators involved in the normal form theorems interact with the reduction modulo p.

Denote by $T_0 = L - L_0 : \mathbb{Z}_{(p)}[x] \to \mathbb{Z}_{(p)}[x]$ the tail of the operator L and by $T_p = L_p - L_{p,0} : \mathbb{F}_p[x] \to \mathbb{F}_p[x]$ the tail of L_p, both restricted to acting on polynomials for which the denominators of the coefficients are not divisible by p. We write $T_0 = T_{0,1} + \ldots + T_{0,M}$ and $T_p = T_{p,1} + \ldots T_{p,M}$ as sum of Euler operators with positive shift. Further denote by $\pi : \mathbb{Z}_{(p)}[x] \to \mathbb{F}_p[x]$ the reduction of the coefficients modulo p. One easily verifies that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{Z}_{(p)}[x] & \xrightarrow{T_{0,m}} & \mathbb{Z}_{(p)}[x] \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ \mathbb{F}_p[x] & \xrightarrow{T_{p,m}} & \mathbb{F}_p[x] \end{array}$$

for each $m = 1, \ldots, M$. In particular,

$$\begin{array}{ccc} \mathbb{Z}_{(p)}[x] & \xrightarrow{T_{0}} & \mathbb{Z}_{(p)}[x] \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ \mathbb{F}_p[x] & \xrightarrow{T_{p}} & \mathbb{F}_p[x] \end{array}$$

commutes as well.

Moreover, denote by $S_0 = (L_0|_{\mathcal{H}})^{-1} : x \cdot \mathcal{F}_L^{\Omega} \to \mathcal{F}_L^{\Omega}$ the right inverse of L_0 described in the normal form theorem in characteristic 0, Theorem 9.5. Further let $S_p : x \cdot \mathcal{G}_{L_p}^{\rho} \to \mathcal{G}_{L_p}^{\rho}$ be the inverse of $L_{p,0}$. Then $S(x^l) = \frac{1}{\chi_L(l)} x^l$ whenever l is not a local exponent of L and $S_p(x^l) = \frac{1}{\chi_{L_p}(l)} x^l$, whenever l is not a local exponent of L_p. Further, we have that $\pi(\chi_L(l)) = \chi_{L_p}(l)$. In particular, if $\rho + l$ is not a local exponent of L_p, then the following diagram commutes:

$$\begin{array}{ccc} x^{\rho+l}\mathbb{Z}_{(p)} & \xrightarrow{S_{0}} & x^{\rho+l}\mathbb{Z}_{(p)} \\ \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\ x^{\rho+l}\mathbb{F}_p & \xrightarrow{S_{p}} & x^{\rho+l}\mathbb{F}_p \end{array}$$

If $\rho + l$ is a local exponent of L_p, then $S_p(x^{\rho+l})$ depends on the logarithm z_1.

Assume $b_i = \overline{a_i}$ holds for $i = 1, \ldots, l-1$. We will distinguish the two cases whether $\rho + l$ is a local exponent of L_p or not. Assume first that $\rho + l$ is not a local exponent. Rewriting the differential equations as a recursions we obtain

$$a_l = S_0 \left(\sum_{m=1}^{M} T_{0,m}(a_{l-m} x^{\rho+l-m}) \right)$$

and

$$b_l = S_p\left(\sum_{m=1}^{M} T_{p,m}(b_{l-m}x^{\rho+l-m})\right),$$

where both sums are homogeneous of degree $\rho + l$ in x. Thus the commutativity of the diagrams above yields that b_l indeed is the reduction of a_l modulo p.

If $\rho + l$ is a local exponent of L_p, then

$$b_l = S_p\left(\sum_{m=1}^{M} T_{p,m}(b_{l-m}x^{\rho+l-m})\right) + \overline{a_l}$$

by the definition of g and the recursion. As mentioned above, $S_p(x^{\rho+l})$ depends on z_1. So if $\sum_{m=1}^{M} T_{p,m}(b_{l-m}x^{\rho+l-m})$ does not vanish, the solution g contradicts the existence of a basis of solutions of $L_p y = 0$ not depending on the logarithms. Thus, b_l is the reduction of a_l in this case as well.

This allows us to show that b_k depends on z_1: As above we have

$$b_k = S_p\left(\sum_{m=1}^{M} T_{p,m}(b_{k-m}x^{\rho+l-m})\right)$$

and

$$a_k = S_0\left(\sum_{m=1}^{M} T_{0,m}(a_{k-m}x^{k+\rho-m})\right).$$

As a_k depends on z by assumption, $\rho + k$ necessarily is a local exponent of L and thus of L_p. So $S_p(x^{\rho+k})$ depends on z_1. If $\Sigma_p = \sum_{m=1}^{M} T_{p,m}(b_{k-m}x^{\rho+l-m}) \neq 0$, then b_k depends on z_1, contradicting the existence of a basis of solutions of $L_p y = 0$ not depending on the logarithms. However, Σ_p equals the reduction of $\Sigma_0 = \sum_{m=1}^{M} T_{0,m}(a_{k-m}x^{k+\rho-m})$ modulo p by the commutative diagrams from above. But $\Sigma_0 \neq 0$, because $S(\Sigma_0) = a_k \neq 0$. As we have only excluded finitely many prime numbers p so far, we can choose p not dividing Σ_0. This is a contradiction. Thus, no solution f of $Ly = 0$, depending on z may exist, which concludes the proof. □

Our proof of (iii) is certainly not the fastest. However, it illustrates the interplay between the normal form theorems in characteristic 0 and p. We illustrate what happens in the proof of (iii) with an example.

Example 9.8. The operator $L = x^2\partial^2 - 3x\partial - 3x - x^2 - x^3$ has the solution

$$f(x) = u^{-1}(1) = 1 + a_1x + a_2x^2 + \ldots = 1 - x + \frac{1}{2}x^2 - \frac{1}{2}x^3 - \frac{1}{2}x^4z + \ldots,$$

so $a_4 = -\frac{1}{2}z$ is the first coefficient, which depends on z. Assume that there was a full basis of solutions in $\mathbb{F}_3[\![x]\!]$. The local exponents in characteristic 3 are 0 and 1, so $\Lambda = \{1, 3\}$. We compute, using $T_3 = x^2 + x^3$ and $L_{3,0} = x^2\partial^2$, the expansion of the following solution

$$u_3^{-1}(1 + 2x + x^3) = 1 + 2x + 2x^2 + x^3 + \ldots,$$

which agrees with the reduction of f up to order 3. However, the next term in the expansion is $S_3(x^4) = x^4z_1$, so $u_3^{-1}(1 + 2x + x^3) \notin \mathbb{F}_3[\![x]\!]$.

10 Outlook

If one wants to pursue the goal of proving the equivalence of the Grothendieck p-curvature conjecture and the Bézivin conjecture, number theoretic obstacles occur.

A power series $y(x) \in \mathbb{Q}[\![x]\!]$ is called *globally bounded* if there is an integer N such that $y(Nx) \in \mathbb{Z}[\![x]\!]$. In other words, there are only finitely many prime numbers p appearing in the denominators of the coefficients of y and they only grow geometrically. A theorem of Eisenstein [Eis52] says that any algebraic power series is globally bounded.

To prove that the validity of the Bézivin conjecture implies the validity of the Grothendieck p-curvature conjecture it suffices to show that for a linear differential equation $Ly = 0$ whose reduction $L_p y = 0$ has a full basis of solutions in $\mathbb{F}_p[\![x]\!]$ the basis of solutions in characteristic 0 is globally bounded. For this it is natural to try to compare the algorithms from the normal form theorems in characteristic 0 and p further. Ideally, p would not appear in the denominators of solutions in characteristic p if and only if there is a basis of solutions in $\mathbb{F}_p[\![x]\!]$ of $L_p y = 0$, at least for almost all p. However, the situation is not as easy as one might hope, as the following two examples illustrate:

Example 10.1. (i) The first example shows that for finitely many primes it may happen that a full basis of solutions of the reduction of a linear differential equation modulo p exists, although p appears in the denominator of one of the solutions in characteristic 0. The solution of $\partial - nx^{n-1}$ for $n \in \mathbb{N}$ is e^{x^n}, a power series where each prime number appears eventually in the denominators. However, for all prime numbers p dividing n, the reduction of the equation modulo p is an Euler equation having the solution $1 \in \mathbb{F}_p[\![x]\!]$. As this can happen only for a finite number of primes, this does not contradict the Grothendieck p-curvature conjecture.

(ii) The next example shows that to rule out the appearance of the prime factor p in the denominators of a solution of $Ly = 0$ it is not sufficient to work on the level of individual solutions associated to a local exponent and its reduction. If possible at all, it has to take into account the existence of a full basis of solutions.

The power series

$$y(x) = \sum_{k=1}^{\infty} a_k x^k = \sum_{k=1}^{\infty} \frac{k(k+2)}{(k+1)} x^k = \frac{3}{2}x + \frac{8}{3}x^2 + \frac{15}{4}x^3 + \frac{24}{5}x^4 + \ldots = \frac{\log(1-x)}{x} + \frac{x}{(x-1)^2}$$

is annihilated by the third order operator

$$L = x^3\partial^3 + 4x^2\partial^2 + x\partial - 1 - (x^4\partial^3 + 8x^3\partial^2 + 13x^2\partial + 3x).$$

This operator L is *hypergeometric*, i.e., $T = L - L_0$ is an Euler operator with shift one. Moreover, y is annihilated by the second order operator

$$M = 3x^2\partial^2 + 3x\partial - 3 + (x^4 - 4x^3)\partial^2 + (3x - 12x^2)\partial + x^2 - 4x,$$

which is not hypergeometric. The operator M is a right divisor of L, as one verifies that

$$\left(-\frac{1}{x-3}x\partial - \frac{1}{x-3}\right) M = L.$$

Let us first concern ourselves with the operator L. Its local exponents are -1 with multiplicity two and 1 with multiplicity 1. We have $y = \frac{3}{2} \cdot u^{-1}(x)$, where u is the automorphism described in the normal form theorem in characteristic 0. Moreover we compute $u^{-1}(x^{-1}) = x^{-1}$ and $u^{-1}(x^{-1}z) = x^{-1}z$. Thus a basis of solutions of $Ly = 0$ is given by y, x^{-1} and $x^{-1}\log(x)$.

For all prime numbers p the coefficient of x^{p-2} in the expansion of y is divisible by p, while the denominators of $a_1, \dots, a_{p-2}$ are not. Thus

$$y_p := \sum_{k=1}^{p-2} a_k x^k$$

is well defined in characteristic p and a solution to the equation $L_p y = 0$. It is given as $u_p^{-1}(x)$ where u_p is the automorphism defined in the normal form theorem in characteristic p. The series y is not algebraic, as it is not globally bounded. In fact any prime number p appears in the denominators of the coefficients a_i. However, the solution in characteristic p corresponding to the reduction of the local exponent 1 is a genuine power series. Other linearly independent solutions in characteristic p are x^{-1} and $x^{-1}z_1$. We see that in neither characteristic there is a basis of power series solutions.

Let us now turn to the operator M, which has local exponents -1 and 1 as well, both with multiplicity 1. A basis of solutions is given by x^{-1} and y. This does not contradict the Grothendieck p-curvature conjecture, as y_p is not a solution of M. For L the construction was very dependent on the fact that the equation is hypergeometric, which is no longer the case for M.

There still remain several questions about linear differential equations over fields with positive characteristic. For linear differential equations with holomorphic coefficients there is a criterion by Fuchs characterizing regular singular points of an operator L [Fuc66]. A point $a \in \mathbb{P}^1_{\mathbb{C}}$ is at most a regular singularity of L if and only if there is a local basis of solutions of $Ly = 0$, which grows at most polynomially when approaching a. One would expect a similar criterion in characteristic p: an n-dimensional vector space of solutions in $\mathcal{R}$ over the constants $\mathcal{C}$ should suffice to conclude that 0 is a regular singular point of L.

Moreover, the solutions of differential equations in $\mathcal{R}$ need to be better understood. For example one would expect some kind of pattern in the exponential function in positive characteristic discussed in Example 6.3. However, no such structure seems obvious.

In addition there is hope to extract information about the p-curvature and the Galois group of linear differential equations in positive characteristics from the description of a full basis of solutions in the differential extension $\mathcal{R}$ of $\Bbbk$.

Finally, there remain, of course, the Grothendieck p-curvature conjecture and the Bézivin conjecture. As Example 10.1 shows, the algorithms of the normal form theorems in characteristic p and 0 show some unexpected discrepancy. The hope that solutions of the reduction of differential operators are reductions of solutions of the operator seems to be unfounded. However, the phenomena shown require further investigation.

References

[Béz91] J.-P. Bézivin. “Les suites q-récurrentes linéaires”. *Compositio Mathematica* 80.3 (1991), pp. 285–307.

[Dwo90] B. Dwork. “Differential Operators with Nilpotent p-Curvature”. *American Journal of Mathematics* 112.5 (1990), pp. 749–786.

[Eis52] G. Eisenstein. “Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen”. Berichte Königl. Preuss. Akad. Wiss. Berlin. 1852, pp. 441–443.

[Fro73] G. Frobenius. “Ueber die Integration der linearen Differentialgleichungen durch Reihen.” *Journal für die reine und angewandte Mathematik (Crelles Journal)* 76 (1873), pp. 214–235.

[Fro96] G. Frobenius. “Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe”. Berliner Sitzungsberichte. Springer, 1896, pp. 689–703.

[Fuc66] L. Fuchs. “Zur Theorie der linearen Differentialgleichungen mit veränderlichen Coefficienten.” *Journal für die reine und angewandte Mathematik (Crelles Journal)* 66 (1866), pp. 121–160.

[Hau22] H. Hauser. *A Normal Form Theorem for Fuchsian Differential Equations over Fields of Characteristic Zero.* preprint. 2022.

[Hon81] T. Honda. “Algebraic differential equations”. *Symposia Mathematica* 24 (1981), pp. 169–204.

[Jeo11] S. Jeong. “Calculus in positive characteristic p”. *Journal of Number Theory* 131 (2011), pp. 1089–1104.

[Kat70] N. Katz. “Nilpotent connections and the monodromy theorem: Applications of a result of Turrittin”. *Publications Mathématiques de l’IHÉS* 39 (1970), pp. 175–232.

[Kro80] L. Kronecker. “Über die Irreductibiliät von Gleichungen”. Monatsberichte der Königlichen Preussischen Akademie der Wissenschaften zu Berlin. 1880, pp. 155–163.

[SP03] M. Singer and M. van der Put. *Galois Theory of Linear Differential Equations.* Vol. 328. Grundlehren der mathematischen Wissenschaft. Springer, 2003.