Factorization of Linear Differential Operators

een wetenschappelijke proeve op het gebied van de
Wiskunde en Informatica

Proefschrift

ter verkrijging van de graad van doctor aan de Katholieke Universiteit Nijmegen, volgens besluit van het College van Decanen in het openbaar te verdedigen op woensdag 27 november 1996, des ochtends om 11.00 uur precies

door

Marinus Hubertus Franciscus van Hoeij

geboren op 16 augustus 1969 te Someren

Promotor:
  Prof. Dr. A.H.M. Levelt

Manuscriptcommissie:
  Prof. Dr. M. van der Put (University of Groningen).
  Prof. Dr. M.F. Singer (North Carolina State University).
  Dr. F. Ulmer (University of Rennes).

ISBN: 90-9010028-8

Dankwoord

In de eerste plaats wil ik bedanken mijn promotor Professor Levelt voor advies en ondersteuning, en de familie en vrienden voor het veraangenamen van de tijd waarin dit proefschrift is geschreven.

Verder wil ik nog bedanken mijn collega's, in het bijzonder Harm Derksen en Jacques-Arthur Weil, de leden van de manuscriptcommissie en de medewerkers van de vakgroep wiskunde voor wetenschappelijke discussies die belangrijk waren voor de totstandkoming van dit proefschrift.

Contents

Chapter 1

Introduction

1.1 What is the use of Factorization Algorithms?

Suppose one is asked to solve the following equation

$$x^7 - 12x^6 - 30x^5 + 1150x^4 - 7449x^3 + 21990x^2 - 30294x + 14796 = 0. \tag{1.1}$$

One way to start with this problem is to try to factor the polynomial $x^7 - 12x^6 - 30x^5 + 1150x^4 - 7449x^3 + 21990x^2 - 30294x + 14796$ in $\mathbb{Q}[x]$. This polynomial turns out to be reducible. When given a factorization of this polynomial, the problem of solving the corresponding equation is reduced to smaller problems, namely to solve equations of a lower degree. So the problem of solving this equation becomes easier when a factorization is known. It is particularly useful if the factorization contains factors of degree 1, because these immediately give a solution. Note that it may not be so easy to compute a factorization by hand, it is more convenient to use a computer for such problems.

What is observed here for polynomial equations holds for linear differential operators as well, namely that computing a factorization of a differential operator is useful for the problem of solving differential equations. Factorization does not solve this problem in general, but reduces it to smaller problems. Consider for example the following differential operator

$$\begin{aligned} f = \quad & 2(15x^4 - 4x^2 + 3)(x^8 - 12x^5 + 2x^4 - 6x^2 - 12x + 1)\partial^4 + \\ & (480x^{11} - 144x^9 - 3060x^8 + 480x^7 + 1008x^6 - 308x^5 - 360x^4 + \\ & 144x^3 + 48x^2 - 164x - 180)\partial^3 + (1980x^{10} - 756x^8 - 5400x^7 + \\ & 1024x^6 + 2952x^5 + 93x^4 - 2904x^3 + 520x^2 + 72x - 171)\partial^2 + \\ & (1800x^9 - 960x^7 - 1080x^6 + 800x^5 + 900x^4 - 1992x^2 + \\ & 56x + 180)\partial - 180x^6 - 332x^2 + 150x^4 + 30 \qquad \in \overline{\mathbb{Q}}(x)[\partial] \end{aligned} \tag{1.2}$$

where ∂ stands for $\frac{d}{dx}$. This operator corresponds to the following differential equation

$$f(y) = 0.$$

We can try to search for exact symbolic solutions of this equation. Or we can use numerical methods to find approximate solutions. Both are generally easier for equations of smaller order. So if one can reduce this equation to other equations of lower order, then the problem of finding symbolic or numerical solutions becomes easier. To reduce the order of the differential equation $f(y) = 0$, we try to compute one or several factorizations of the differential operator f in the non-commutative ring $\overline{\mathbb{Q}}(x)[\partial]$. In 1894 Beke gave a method for factorization in this ring. Several people have given improved variations on this method.

Factorization by hand is not very pleasant for operators like (1.2) so we prefer to use a computer. However, even on a computer Beke's method (and the variations on it) will most likely not result in a factorization of (1.2) but only in an "out of memory" message. To find a factor of (1.2) via Beke's method, one must first compute another operator g (the second exterior power) and then compute a first order right-hand factor of g. However, in this example g is about 15 times larger than f (measured in the amount of paper it takes to print it). To find the first order factors of g, Beke's algorithm will compute in the splitting field of the polynomial $x^8 - 12x^5 + 2x^4 - 6x^2 - 12x + 1$. According to the computer algebra system GAP this field has degree 1152 over $\mathbb{Q}$. Computations over such complicated fields are not feasible in practise. To find a factorization a different approach is needed, which is not (like all previous implementations) based on Beke's method. Two of such approaches are given in this thesis.

In chapter 3 we will give a new factorization method that has several advantages over Beke's method. One advantage is that it needs not work with splitting fields. It will compute in a field extension of degree 8 instead of degree 1152 in the example (1.2); it needs to work with only one root of $x^8 - 12x^5 + 2x^4 - 6x^2 - 12x + 1$ instead of all roots. Furthermore, in most cases (including this example) it does not need to compute with exterior powers of f, but only with f itself which is a much smaller expression.

In [47] Singer shows how in a number of cases (the example (1.2) is one of these cases) factorization can be reduced to solving an equation that will be called the mixed equation. In chapter 5 an efficient method is given to compute the solutions of this equation. The algorithms in chapters 3 and 5 are implemented. Both algorithms are efficient enough to produce a factorization of (1.2), even on a relatively small computer.

Implementation of these methods costs a lot of time, often even more time than finding the method and writing a paper on it. However, to be sure that the method really works on large complicated examples, one can not avoid implementing the algorithm on a computer. So the implementation is an important part of the work. This thesis discusses the mathematical aspects of the methods. To get an idea of the rest of the work it is recommended to down-load the most recent version of the implementation from the following URL's and to try it on some examples.
`http://www-math.sci.kun.nl/math/compalg/diffop/`
or
`http://daisy.uwaterloo.ca/~mvanhoei`

1.2 Outline of the thesis

Chapter 2, 3, 4 and 5 of this thesis each consist of one paper [26, 27, 28, 29]. These chapters are organized as follows: The title of this thesis refers to chapter 3. The topic of that chapter is of factorization of differential operators with rational functions coefficients. The approach is first to study differential operators locally, because then the problems tend to be mathematically easier (but at the same time more technical and harder to implement!) and have already been solved in large part.

The purpose of chapter 2 is to provide all ingredients that are needed in chapter 3. It contains a precise study of local differential operators. This is done in a general way; the field of constants is not necessarily algebraically closed. The concepts that are introduced in chapter 2 are the following: semi-regular parts (section 2.6.1), exponential parts (section 2.6), their relation with the Newton polynomials (section 2.6), with factorization (lemma 4 and 5, theorem 1 and 2) and with formal solutions (theorem 3). These concepts form the basis of this thesis, all other chapters use this terminology. The topics treated in chapter 2 are quite technical. They are easier to understand when one already knows what their purpose is, and so it can be advisable first to read parts of chapter 3. In particular, reading chapter 2 may be easier after having read section 3.3, although the proofs of the statements in section 3.3 are found in chapter 2. Furthermore chapter 2 becomes much easier if one is already familiar with computing Puiseux expansions (cf. [11, 18]), because the main ingredients for local factorization (the Newton polygon and Newton polynomial) are used for computing Puiseux expansions as well.

The topic of chapter 4 is computing invariants of differential operators. Chapter 4 is joint work with Jacques-Arthur Weil. Results in his thesis combined with the terminology introduced in chapter 2 and section 3.3 turn out to be very useful for computing invariants.

In chapter 5 the topic is to compute solutions of a certain differential equation called the mixed equation. This can be applied to factor differential operators in a number of cases. A nice application of chapter 5 for the factorization algorithm is found in lemma 24. This tells us that the method in chapter 5 is applicable whenever algebraic extensions are needed to factor the differential operator. Hence we can apply the method in chapter 3 with the extra assumption (which speeds up the computation significantly) that no algebraic extensions are needed, and afterwards apply the method in chapter 5 to handle the remaining cases. By combining chapter 3 and chapter 5 in this way we obtain a more efficient factorization algorithm. Another advantage of this combination is that the factorizations from chapter 5 often only use a minimal algebraic extension of the constants.

1.3 What is new?

What is, besides algorithmic improvements that make factorization of (1.2) possible, mathematically new in this thesis? A notion like exponential parts is not new, see for example the normalized eigenvalues in [52]. However, what is new is that they can be defined without using differential modules and the Jordan-Hölder theorem, without using formal solutions, using only a substitution map S_e and the Newton polynomial N_0. This makes exponential parts easier to compute and hence more convenient for algorithmic purposes.

We use exponential parts to express various properties of local factorizations (lemma 4 and 5, theorem 1 and 2). For this purpose it is convenient that the multiplicity $\mu_e(f)$ of the exponential part e in f is defined in terms of the tools S_e and N_0 of local factorization. In section 2.8 these properties are related to properties of formal solutions, in particular in theorem 3. This way we can use local factorizations in the algorithms, but think of these in terms of formal solutions. The former are more convenient to compute with and the latter are easier to understand. It makes the algorithm in chapter 3 much easier to explain. The first two paragraphs of section 3.5 would not be clear when written in the way that the implementation works, which is using local factorizations and no formal solutions. Making the argument in these two paragraphs clear was the reason for introducing exponential parts the way it is done in chapter 2. Even though chapter 2 treats a topic that in itself is not new, the way that this topic is treated is new and leads more conveniently to new results, like chapters 3, 4 and 5.

Another thing which is new in chapter 2 is the definition of the *semi-regular parts* of differential operators. And the definition of the *coprime index* of factorizations in filtered rings, and corresponding to that a generalization of the Hensel lifting algorithm.

In chapter 3, sections 3.5 and 3.6 we give a new efficient factorization algorithm for differential operators with rational functions coefficients. For operators with many singularities and for operators with factors of order > 1 this algorithm is much more efficient than the previous algorithms that are based on Beke's algorithm. Our algorithm is not complete, however. In section 3.7 we show how it can be completed to the case of factors of order 1. Using results from the literature the algorithm can then be completed for higher order factors as well. The terminology of exponential parts, in the way it is treated in chapter 2, is needed to describe the algorithm.

Our approach of exponential parts has more applications as well, it is also used in chapter 4 and chapter 5. In chapter 4 one of the problems that is treated is to determine bounds on the integer exponents of a certain operator M (a symmetric power of a given operator L), without actually computing M. Good bounds have the following properties: they can be computed quickly and are as sharp as possible. There is not a suitable relation between the exponents of L and the exponents of M. There is, however, a relation between the solution spaces of L and M. The relation between the solutions and *generalized exponents* (which, like the exponential parts, are defined in terms of N_0 and S_e) gives a good way to compute these bounds. Furthermore this approach restricts the number of monomials that need to be considered in the algorithm in chapter 4 (see the lemma in section 4.4.1), which is beneficial for the efficiency as well.

Chapter 5 deals with the problem of computing the eigenring of a differential operator, by solving the so-called *mixed equation*. The elements of this eigenring are differential operators with rational function coefficients. The main mathematical difficulty for determining these rational functions in an efficient way is to find a bound on their valuations at every place on P^1. One can quickly derive a bound, expressed in terms of the Newton polynomial, for the regular singular case. However, we want to have a bound for the general case. As we have seen in the previous chapters, the regular singular case can often be generalized by using the terminology of exponential parts and generalized exponents. We want to do this in chapter 5 as well. The key result that we need in chapter 5 is equation (3.3) on page 48, which says that the sum of the multiplicities of the generalized exponents of f equals order(f).

In previous chapters one of the ideas was to relate the multiplicity (which was defined in terms of N_0 and S_e) of exponential parts to a property of formal solutions; the *multiplicity of an exponential part* is the dimension of the corresponding component of the solution space. So in chapter 5 the idea is to do the same for generalized exponents, to relate their multiplicities (which are easiest defined in terms of N_0 and S_e) to a property of formal solutions. For this purpose the property *degl* of a formal solution is introduced. This notion is used for the computation of the bound (the result of this computation is proposition 5). This bound is the mathematical ingredient that is needed to find an efficient algorithm.

A few remarks on formal solutions and exponential parts: Traditionally, a basis of formal solutions is given where each element is represented in the following form

$$\exp(p)x^{\lambda}s \quad \text{where} \quad s \in k((x))[p, \lambda, \log(x)], \quad \lambda \in \overline{k}, \quad p \in \bigcup_n x^{-1/n}\overline{k}[x^{-1/n}].$$

We propose the following form instead

$$\mathrm{Exp}(e)s \quad \text{where} \quad s \in k((x))[e, \log(x)], \quad e \in \bigcup_n \overline{k}[x^{-1/n}]. \tag{1.3}$$

Here $\mathrm{Exp}(e)$ stands for $\exp(\int \frac{e}{x}dx)$. In the expression $\mathrm{Exp}(e)s$ we call e the exponential part and s the semi-regular part. So (p, λ) is grouped together in the exponential part e. Consequently, the distinction between $p = 0$ and $p \neq 0$ (regular singular and irregular singular) is no longer relevant, we only distinguish $e \in \mathbb{Z}$ (= semi-regular case = trivial exponential part) and $e \notin \mathbb{Z}$. We propose to drop the notion of regular singular as much as possible, and introduce the notion of semi-regular operators. The motivation is to generalize algorithms that are designed for the regular singular case to the irregular singular case. Therefore, we want to treat regular singular and irregular singular in exactly the same way. For the formal solutions that means representing them as in (1.3). The benefits of this approach are found in chapters 3, 4 and 5. After having treated the necessary technicalities in chapter 2, the irregular singular case is no longer harder or easier than the regular singular case in chapters 3, 4 and 5.

1.4 List of Notations

Chapter 2:

f	A differential operator.
L	A left-hand factor of f.
R	A right-hand factor of f.
k	The field of constants (not necessarily algebraically closed).
$k((x))$	The field of formal Laurent series with finite pole order.
∂	$\frac{d}{dx}$
δ	The differential operator $x\partial$, cf. page 15.
$k((x))[\partial]$	Ring of differential operators with power series coefficients.
$k((x))[\delta]$	Same ring, but the elements are denoted in terms of δ instead of ∂ cf. section 2.3.2.
v_s	A valuation on $k((x))[\delta]$ defined in section 2.2.
D_n	For a fixed valuation v, $D_n = \{a \mid v(a) \geq n\}$, cf. section 2.2.
$\sigma_a(f)$	f up to accuracy a, which means f modulo $D_{a+v(f)}$
$\sigma_{a,s}(f)$	$\sigma_a(f)$ where the underlying valuation is v_s
coprime index	For a factorization $f = LR$ in a filtered ring D this measures how "coprime" L and R are, cf. section 2.2.
E	The set $\bigcup_{n\in\mathbb{N}} \overline{k}[x^{-1/n}] \subset \overline{k((x))}$, cf. page 16.
$\mathrm{ram}(e)$	The ramification index, cf. page 15.
$\sim$	$e_1 \sim e_2 \Longleftrightarrow e_1 - e_2 \in \frac{1}{\mathrm{ram}(e_1)}\mathbb{Z}$, cf. page 27.
S_e	Maps δ to $\delta + e$, cf. page 16.
$N(f)$	Newton polygon, cf. section 2.3.3 and the references therein.
regular	f is regular if $f = a \cdot g$ for some $a \in k((x))$ and monic $g \in k((x))[\partial]$.
regular singular	f is regular singular if $N(f)$ has only one slope equal to 0.
$N_s(f)$	Newton polynomial for slope s, cf. section 2.3.4.
T	Variable used for expressing the Newton polynomial.
V	Universal extension (as a ring) of $k((x))$, cf. page 16. In lemma 2.1.1 in [24] this is called R.
$V(f)$	$V(f) \subset V$ is the solution space of f, $\dim(V(f)) = \mathrm{order}(f)$.
$\mathrm{order}(f)$	Degree of f, as a non-commutative polynomial in ∂ or δ.
$\mathrm{Exp}(e)$	For $e \in E$ defined as $\exp(\int \frac{e}{x} dx) \in V$, cf. section 2.3.2.
V_e	$\mathrm{Exp}(e) \cdot (\overline{k} \cdot k((x))[e])[\log(x)]$, cf. section 2.8.3.
$V_e(f)$	$V(f) \bigcap V_e$, where $f \in k((x))[\delta]$ and e in E or in $E/\sim$.
$\overline{V}_e$	$\mathrm{Exp}(e) \cdot \overline{k((x))}[\log(x)]$.
$\overline{V}_e(f)$	$V(f) \bigcap \overline{V}_e$, where $f \in \overline{k((x))}[\delta]$ and e in E or in $E/\mathbb{Q}$.
$\mu_e(f)$	$\dim(V_e(f))$, cf. section 2.6 and theorem 3 on page 34.

$\overline{\mu}_e(f)$	$\dim(\overline{V}_e(f))$, cf. section 2.6 and theorem 3.
$\theta_{a,n}$	See page 16.
exponents	The roots of $N_0(f)$ in $\overline{k}$.
exponential part	An element e of $E/\sim$ for which $\mu_e(f) > 0$.
semi-regular	f is semi-regular over $k((x))[e]$ if f is regular singular and the exponents are elements of $\frac{1}{\mathrm{ram}(e)}\mathbb{Z}$.
semi-regular part	The semi-regular part R_e of f for $e \in E$ is the largest factor of $S_e(f)$ which is semi-regular over $k((x))[e]$, cf. section 2.6.1.
$\mathrm{pp}(r)$	For $r \in \overline{k((x))}$, $\mathrm{pp}(r)$ is the $e \in E$ for which $v(e-r) > 0$.
Riccati solution	r for which $\partial - r$ (or $\delta - r$ when using δ syntax) is a right-hand factor, cf. section 2.5.1.
LCLM	Least Common Left Multiple, cf. page 16.
$S_{\log}$	Maps $\log(x)$ to $\log(x) + 1$, cf. section 2.9.

Chapter 3:

$k(x)[\partial]$	Differential operators with rational functions coefficients.
$\nu_e(f)$	Multiplicity of the generalized exponent, defined as the multiplicity of the root 0 in $N_0(S_e(f))$.
generalized exponent[1]	$e \in E$ for $\nu_e(f) > 0$.
l_p	A map that moves the point p to 0, cf. section 3.3.4.
$\mu_*(f)$	Collection of all $\mu_e(l_p(f))$ data, cf. section 3.3.4.
$\sim_*$	$a \sim_* b$ if $a - b = y'/y$ for some $y \in \overline{k}(x)$, cf. page 53.
$\gamma_1(f)$	The set of $\mu_*(R)$ for all first order right factors R of f.
S_r^*	Maps ∂ to $\partial + r$, cf. page 53.
v	A partially defined valuation from V to E, cf. section 3.3.3.
V_*	The set of $y \in V$ for which the valuation $v(y) \in E$ is defined.
adjoint	$\overline{k}(x)$-anti-automorphism of $\overline{k}(x)[\partial]$ given by $\partial \mapsto -\partial$.
$\mathrm{type}(f)$	Isomorphism class of $V(f)$, cf. section 3.3.5.
LCLM factorization	$f_1, \ldots, f_n$ for which $f = \mathrm{LCLM}(f_1, \ldots, f_n)$.
completely reducible	f allows an LCLM factorization with $f_1, \ldots, f_n$ irreducible.
GCRD	Greatest Common Right Divisor.

Chapter 4 :

L	A differential operator.
C	The field of constants (not necessarily algebraically closed).
k	$\overline{C}(x)$
$L^{Ⓢm}$	The m-th symmetric power of the operator L.
$L_1 Ⓢ L_2$	Symmetric product, cf. page 76.
$S^m(A)$	Symmetric power of a matrix differential equation $AY = Y'$.

$Sym^m(W)$	For a vector space W this is the m-th symmetric power of W.
$Sym^m(U)$	For a matrix U this denotes a matrix of which the columns form a basis of $Sym^m(W)$, where W is the vector space spanned by the columns of U.
$e_1 \leq_r e_2$	$e_1 - e_2 \in \frac{1}{r}\mathbb{Z}$ and $e_1 - e_2 \leq 0$.
$\min_r(L)$	$\leq_r$-minimal generalized exponents of L.
$L^{(i)}$	Monic operator for which $\partial^i(V(L)) = V(L^{(i)})$.

Chapter 5:

RRem	Remainder after a right-hand division.
$\mathcal{E}_{\mathcal{D}}(f,f)$	$\{r \in \overline{k}(x)[\partial] \vert r(V(f)) \subset V(f),\ \mathrm{order}(r) < \mathrm{order}(f)\}$, the eigenring of $V(f)$.
$\mathrm{degl}(y)$	Degree, as a polynomial in $\log(x)$, of the part of $y \in V_*$ with the lowest valuation.

[1]In an older version of this text, [27], this was called *canonical exponential part* (meaning: a canonical choice of a representative in E for an exponential part in $E/\sim$) and the list of generalized exponents was called *canonical list*.

Chapter 2

Formal Solutions and Factorization of Differential Operators with Power Series Coefficients

The topic of this chapter is formal solutions of linear differential equations with formal power series coefficients. The method proposed for computing these solutions is based on factorization of differential operators. The notion of exponential parts is introduced to give a description of factorization properties and to characterize the formal solutions. The algorithms will be described and their implementation is available.

2.1 Introduction

Factorization of differential operators is a powerful computer algebra tool for handling ordinary linear differential equations. It can be applied to compute formal solutions and to study the structure of a differential equation. A differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y = 0$$

corresponds to a differential operator

$$f = \partial^n + a_{n-1}\partial^{n-1} + \ldots + a_0\partial^0$$

acting on y. Here the coefficients a_i are elements of the differential field $k((x))$ and ∂ is the differentiation d/dx. The field k is the field of constants. It is assumed to have characteristic 0. The differential operator f is an element of the non-commutative ring $k((x))[\partial]$. This is an example of an Ore ring [40].

Sections 2.6 and 2.8 contain the main results of this chapter. These results are expressed using the notion of exponential parts. The exponential parts will be studied in section 2.6 from the viewpoint of factorization, and in section 2.8 from the viewpoint of formal solutions. They form the key ingredient for our factorization algorithm for $k(x)[\partial]$ in chapter 3. Another application is found in section 2.9. Here the question is: when is a given vector space a solution space of a certain differential operator. This question can easily be answered using the direct sum splitting in section 2.8.

The algorithms in this chapter are given in sections 2.4, 2.5 and 2.8.4. From an algorithmic point of view the factorization in $k((x))[\partial]$ is the central problem because all other algorithms in this thesis require this tool. We will discuss it in the rest of this section.

Note that in general elements of $k((x))$ consist of infinitely many terms. Only a finite number of them can be computed. This means that a factorization can only be determined up to some finite accuracy. The notion of accuracy will be formalized later. Increasing the accuracy of a factorization will be called *lifting* a factorization.

From [35] we know that an element of $k((x))[\partial]$ which has only 1 slope in the Newton polygon (cf. section 2.3.3) and which has an irreducible Newton polynomial (cf. section 2.3.4) is irreducible in $k((x))[\partial]$. In [35] Malgrange shows that in the following two cases a differential operator $f \in k((x))[\partial]$ is reducible in this ring and how a factorization can be computed:

1. An operator with a broken Newton polygon (i.e. more than 1 slope).

2. An operator with one slope > 0 where the Newton polynomial is reducible and not a power of an irreducible polynomial.

In our method these two cases of factorization and the factorization of regular singular operators are called *coprime index 1 factorizations*. Coprime index 1 means that the factorization can be lifted by the usual Hensel lifting (cf. any book on computer algebra) procedure. For a definition of the coprime index see section 2.2.

Example:

$$f = \partial^4 + \frac{1}{x^2}\partial^3 + \frac{2}{x^4}\partial^2 + \frac{1}{x^6}\partial + \frac{1}{x^8}.$$

The Newton polynomial is $T^4+T^3+2T^2+T+1$. This polynomial can be factored over $\mathbb{Q}$ as $(T^2+1)(T^2+T+1)$. Because T^2+1 and T^2+T+1 in $\mathbb{Q}[T]$ are coprime (i.e. the gcd is 1) we can conclude from [35] that f is reducible in $\mathbb{Q}((x))[\partial]$. A factorization of $f = LR$ is obtained in two steps. The first step is to compute the factorization up to accuracy 1 (definitions follow later, this integer 1 is related to the coprime index). This accuracy is obtained when we have the Newton polynomials T^2+1 and T^2+T+1 of L and R (here T^2+1 and T^2+T+1 can be interchanged to obtain a different factorization). The next step is to lift the factorization up to the desired accuracy. Because T^2+1 and T^2+T+1 are coprime this lifting can be done by the usual Hensel lifting procedure. In each lift step the extended Euclidean algorithm is used. Note that in this example the reducibility of f can be concluded from very few coefficients of f in k; the coefficients which determine the Newton polynomial are sufficient.

Now there remains one hard case of factorization in $k((x))[\partial]$. Here f has one slope $s \neq 0$ and the Newton polynomial is of the form P^d, where P is an irreducible polynomial over k and d is an integer > 1. In this case it is more difficult to decide if f is reducible or not. A factorization of f will have coprime index > 1.

Example:

$$f = \partial^4 + \frac{2+x^4}{x^4}\partial^2 - \frac{8}{x^5}\partial + \frac{1+20x^2}{x^8}.$$

The Newton polynomial of f is $T^4 + 2T^2 + 1 = (T^2+1)(T^2+1)$. Because the two factors T^2+1 and T^2+1 are not coprime we can not apply Hensel lifting to find a factorization over $\overline{\mathbb{Q}((x))}[\partial]$. Malgrange provides a factorization method in $\overline{\mathbb{Q}((x))}[\partial]$ for this case. We want to find a factorization in $\mathbb{Q}((x))[\partial]$. In this example f is reducible in $\mathbb{Q}((x))[\partial]$. However, $f + 1/x^6$ (replace the coefficient 20 by 21) is irreducible in $\mathbb{Q}((x))[\partial]$. In the previous example adding $1/x^6$ would have no influence on the reducibility of f because the reducibility could already be decided from the Newton polynomial. We see that this example is more complicated because more coefficients of f are relevant for deciding reducibility. We shall proceed as follows:

- Compute a first order right-hand factor $\partial - r$ of f where $r \in \overline{k((x))}$. We use a variant on the method in [35] for this.
- Compute an operator $R \in k((x))[\partial]$ of minimal order such that $\partial - r$ is a right-hand factor of R.
- Perform a division to find a factorization $f = LR$.

For some applications, like factorization in $k(x)[\partial]$, we need to compute the factors L and R up to a high accuracy. The method sketched for computing L and R is not very suitable for this because it is slow. We will use this slow method to compute L and R up to a certain accuracy (up to the coprime index) and then use a different method to lift the factorization. Coprime index > 1 means that the usual Hensel lifting does not work because the Newton polynomials of L and R have gcd $\neq 1$. For this case we give a variant on the Hensel lifting method in section 2.4.

The factorization of a differential operator f is done recursively. If f can be factored $f = LR$ then the factorization algorithm is applied to the factors L and R (or only to R when we are only interested in right-hand factors) until f is factored in irreducible factors. This causes a difficulty; if a factorization is required with a given accuracy it is not clear how accurate the intermediate factorizations should be. To solve this problem we use *lazy evaluation* in our implementation. This is a computer algebra trick which makes exact computation in $k((x))$ possible. It does not use truncations of some finite accuracy. Instead, an expression $a \in k((x))$ is denoted as the name and arguments of a procedure that computes coefficients of a. These coefficients are automatically computed and stored when they are needed. This method of computing in $k((x))$ is very efficient because coefficients which are not used will not be computed.

2.2 Valuations and the coprime index

A discrete *valuation* on a ring D is a map $v : D \to \mathbb{Z} \bigcup \{\infty\}$ such that for all a and b in D we have: $v(ab) = v(a) + v(b)$, $v(a+b) \geq \min(v(a), v(b))$ and $v(a+b) = \min(v(a), v(b))$ if $v(a) \neq v(b)$. $v(0) = \infty$. An example: D is the field of p-adic numbers $\mathbb{Q}_p$ or D is a polynomial ring $\mathbb{Q}_p[x]$ over the p-adic numbers. Define the valuation $v(a)$ of $a \in \mathbb{Q}_p[x]$ as the largest integer n such that $a \in p^n \mathbb{Z}_p[x]$. Another example: $s \in \mathbb{Q}$ and $D = k((x))[y]$ where k is a field. Write $s = n/d$ where n and d are integers, $\gcd(n,d) = 1$ and $d > 0$. Now the valuation $v_s(\sum_{i,j} a_{i,j} x^i y^j)$ is defined as the minimum $id - jn$ for which $a_{i,j} \neq 0$.

A third example: k is a field, $s \in \mathbb{Q}$, $s \geq 0$ and $D = k((x))[\delta]$. Here δ is defined as $x\partial \in k((x))[\partial]$, cf. section 2.3.2. Write $s = n/d$ where n and d are integers, $\gcd(n,d) = 1$ and $d > 0$. Now the valuation $v_s(\sum_{i,j} a_{i,j} x^i \delta^j)$ is defined as the minimum $id - jn$ for which $a_{i,j} \neq 0$.

A *filtered ring* is a ring D with a chain of additive subgroups $\cdots \supset D_{-1} \supset D_0 \supset D_1 \cdots$ such that: $1 \in D_0$, $D = \bigcup_{n \in \mathbb{Z}} D_n$ and $D_n D_m \subset D_{n+m}$ for all integers n and m. The chain $(D_n)_{n \in \mathbb{Z}}$ is called a *filtration* of D. The *associated graded ring* $\mathrm{gr}R$ is defined as $\oplus_n D_n / D_{n+1}$. The symbol map $\sigma : D \to \mathrm{gr}D$ is defined as: $\sigma(0) = 0$, $\sigma(f) = f + D_{n+1}$ if $f \in D_n \setminus D_{n+1}$. For more information about filtrations see [10]. A valuation v defines a filtration on a ring D as follows

$$D_n = \{f \in D | v(f) \geq n\}.$$

For positive integers a the set D_0/D_a has the structure of a ring.

For a ring D with a valuation v we can define a *truncation* σ_a with *accuracy* a for non-zero elements f of D and positive integers a as follows

$$\sigma_a(f) = f + D_{v(f)+a} \in D_{v(f)}/D_{v(f)+a}.$$

The symbol map is σ_1.

Suppose $f \in D$ can be written as $f = LR$ where $L, R \in D$. For invertible elements $u \in D$ we have $f = LR = (Lu)(u^{-1}R)$. We will call the ordered pair L, R equivalent with the pair $Lu, u^{-1}R$. Let t be a positive integer. Then the ordered pair L, R is called *coprime* with *index* t if for all $a \geq t$ the pair $\sigma_{a+1}(L), \sigma_{a+1}(R)$ is determined up to the above equivalence by $\sigma_a(L)$, $\sigma_a(R)$ and $\sigma_{a+t}(f)$. Assume t is minimal, then t is called the *coprime index* of L, R. If L, R is not coprime for any integer t then the coprime index is ∞.

For our examples $\mathbb{Q}_p[x]$, $k((x))[y]$ and $k((x))[\delta]$ the notion of equivalence for pairs L, R can be avoided by restricting ourselves to monic elements f, L and R. Then we can define the coprime index of the factorization $f = LR$ as the smallest positive integer t for which the following holds: For all integers $a \geq t$ and monic elements L' and R' of D, if

$$\sigma_a(L') = \sigma_a(L) \;\text{ and }\; \sigma_a(R') = \sigma_a(R) \;\text{ and }\; \sigma_{a+t}(L'R') = \sigma_{a+t}(f)$$

then

$$\sigma_{a+1}(L') = \sigma_{a+1}(L) \;\text{ and }\; \sigma_{a+1}(R') = \sigma_{a+1}(R).$$

Example: Suppose we want to factor $f = x^2 + x + 3 \in D = \mathbb{Q}_3[x]$. First we look at the truncation $\sigma_1(f) = x^2 + x \in D_0/D_1$ which factors as $x(x+1) \in D_0/D_1$. Because x and $x+1$ have gcd 1 in $D_0/D_1 \simeq F_3[x]$ we can apply Hensel lifting to find a factorization $f = LR$ in D. To determine L and R up to some accuracy a we only need to know f up to accuracy a. So the coprime index is 1 in this example.

Example: $f_1 = x^4 - x^2 - 2 = L_1 R_1 = (x^2+1)(x^2-2) \in \mathbb{Q}_3[x]$ and $f_2 = x^4 - x^2 - 20 = L_2 R_2 = (x^2+4)(x^2-5) \in \mathbb{Q}_3[x]$. Now f_1 and f_2 are the same up to accuracy 2 (i.e. modulo 3^2) but the factorizations L_1, R_1 and L_2, R_2 are different up to this accuracy.

It follows that to determine the factorization of f_1 up to some accuracy a it is not sufficient to know $\sigma_a(f_1)$. This means that the coprime index of L_1, R_1 is > 1. We can not apply ordinary Hensel lifting to find a factorization of f_1 because $\sigma_1(L_1)$ and $\sigma_1(R_1)$ have gcd $\neq 1$.

The name coprime index is explained from the case $k((x))[y]$. In this ring L, R have finite coprime index if and only if L and R are coprime in the usual sense (i.e. $\gcd(L, R) = 1$). It follows from proposition 5 in chapter 5 that the coprime index of a factorization $f = LR$ in $k((x))[\delta]$ is always finite. The proof of this is postponed till after proposition 5.

2.3 Preliminaries

This section summarizes the concepts and notations we will use in this chapter. Definitions will be brief; references to more detailed descriptions are given.

2.3.1 The field $k((x))$

k is a field of characteristic 0, $\overline{k}$ is its algebraic closure. $k((x))$ is the field of formal Laurent series in x with finite pole order and coefficients in k. $\overline{k((x))}$ is the algebraic closure of $k((x))$. It is (cf. [11]) contained in the algebraically closed field $\bigcup_{n \in \mathbb{N}} \overline{k}((x^{1/n}))$, the field of Puiseux series with coefficients in $\overline{k}$.

A *ramification* of the field $k((x))$ is a field extension $k((x)) \subset k((r))$ where r is algebraic over $k((x))$ with minimum polynomial $r^n - ax$ for some non-zero $a \in k$ and positive integer n (cf. [52]). If $a = 1$ this is called a *pure ramification*.

For $r \in \overline{k((x))}$ (not necessarily with minimum polynomial $r^n - ax$) we call the smallest integer n for which $r \in \overline{k}((x^{1/n}))$ the *ramification index* $\mathrm{ram}(r)$ of r. If L is a finite algebraic extension of $k((x))$ then the ramification index of L is the smallest n for which $L \subset \overline{k}((x^{1/n}))$.

$k((x))$ is a *differential field* with differentiation d/dx. If $k((x)) \subset L$ is an algebraic extension then d/dx can be extended in a unique way to L. All finite algebraic extensions $k((x)) \subset L$ are of the following form:

$$L = l((r))$$

where $k \subset l$ is a finite extension and $l((x)) \subset l((r))$ is a ramification (cf. [52], proposition 3.1.5).

2.3.2 The ring $k((x))[\delta]$

Define $\delta = x\partial \in k((x))[\partial]$. We have $\delta x = x\delta + x$ in $k((x))[\delta]$. Since $k((x))[\partial] = k((x))[\delta]$ we can represent differential operators in the form $f = a_n\delta^n + \ldots + a_0\delta^0$. This form has several advantages. The multiplication formula

$$\left(\sum_i x^i P_i(\delta)\right)\left(\sum_j x^j Q_j(\delta)\right) = \sum_n x^n \sum_{i+j=n} P_i(\delta + j)Q_j(\delta)$$

and the definition of the Newton polygon (cf. section 2.3.3) are easier for operators with this syntax. The operators we consider are usually *monic*. This means $a_n = 1$. The *order* of a differential operator f is the degree of f as a polynomial in δ.

f is called the *least common left multiple* of a sequence of differential operators $f_1, \ldots, f_r$ if all f_i are right factors of f, the order of f is minimal with this property, and f is monic. Notation: $f = \mathrm{LCLM}(f_1, \ldots, f_r)$ (cf. [47]). The solution space of f is spanned by the solutions of $f_1, \ldots, f_r$. So $V(f) = \sum V(f_i)$ where $V(f)$ stands for the solution space of f. In order to speak about the solutions of differential operators a differential extension of $k((x))$ is required that contains a fundamental system of solutions of $f_1, \ldots, f_r$. For this we can use the so-called *universal extension* that we will denote as V. This V is constructed as follows (this construction is obtained from [24], our V is called R in lemma 2.1.1 in [24]). Define the set

$$E = \bigcup_{n \in \mathbb{N}} \overline{k}[x^{-1/n}].$$

First view $\mathrm{Exp}(e)$ and $\log(x)$ as variables and define the free $\overline{k((x))}$-algebra W in these variables $W = \overline{k((x))}[\{\mathrm{Exp}(e) | e \in E\}, \log(x)]$. Then define the derivatives $\mathrm{Exp}(e)' = \frac{e}{x}\mathrm{Exp}(e)$ and define the derivative of $\log(x)$ as $1/x$. This turns W into a differential ring. We can think of $\mathrm{Exp}(e)$ as

$$\mathrm{Exp}(e) = \exp(\int \frac{e}{x})$$

because $x\frac{d}{dx}$ acts on $\mathrm{Exp}(e)$ as multiplication by e. Now define V as the quotient ring $V = W/I$ where the ideal I is generated by the following relations:

$$\mathrm{Exp}(e_1 + e_2) = \mathrm{Exp}(e_1)\mathrm{Exp}(e_2) \quad \text{for} \quad e_1, e_2 \in E$$

and

$$\mathrm{Exp}(q) = x^q \in \overline{k((x))} \quad \text{for} \quad q \in \mathbb{Q}.$$

Note that this ideal is closed under differentiation. Hence V is a differential ring. It is proven in [24] that V is an integral domain and that $\overline{k}$ is the set of constants of V. We denote the set of solutions of f in V as $V(f)$. This is a $\overline{k}$-vector space. Since every $f \in k((x))[\delta]$ has a fundamental system of solutions in V (cf. [24]) it follows that

$$\dim(V(f)) = \mathrm{order}(f).$$

The *substitution map* $S_e : k((x))[\delta] \to k((x))[\delta]$ is a $k((x))$-homomorphism defined by $S_e(\delta) = \delta + e$ for $e \in k((x))$. S_e is a ring automorphism. The following is a well-known relation between the solution spaces:

$$V(f) = \mathrm{Exp}(e) \cdot V(S_e(f)).$$

The algorithm "Riccati solution" in section 2.5.1 introduces algebraic extensions over $k((x))$. This requires computer code for algebraic extensions of the constants $k \subset l$. But we can avoid writing code for ramifications. Given a field extension $k((x)) \subset k((r))$ where $r^n = ax$ for some $a \in k$ we will use the following ring isomorphism

$$\theta_{a,n} : k((r))[\delta] \to k((x))[\delta]$$

defined by $\theta_{a,n}(r) = x$ and $\theta_{a,n}(\delta) = \frac{1}{n}\delta$. This map enables us to reduce computations in $k((r))[\delta]$ to computations in $k((x))[\delta]$.

2.3.3 The Newton polygon

The *Newton polygon* of a monomial $x^i y^j$ in the commutative polynomial ring $k((x))[y]$ is defined as the set $\{(j,b) \in \mathbb{R}^2 | i \leq b\}$. The Newton polygon $N(f)$ of a non-zero polynomial $f \in k((x))[y]$ is defined as the convex hull of the union of the Newton polygons of the monomials for which f has a non-zero coefficient (cf. [11], p. 36). The main property is $N(fg) = N(f) + N(g)$ for f and g in $k((x))[y]$. A rational number s is called a ***slope*** of f if s is the slope of one of the edges of the polygon $N(f)$. If s is a slope of fg then s is a slope of f or s is a slope of g.

For the non-commutative case $f \in k((x))[\delta]$ definitions of the Newton polygon are given in [35], [54] and [52], p. 48. $N(x^i\delta^j)$ is defined as $\{(a,b) \in \mathbb{R}^2 | 0 \leq a \leq j, i \leq b\}$ and $N(f)$ is again defined as the convex hull of the union of the Newton polygons of the monomials that appear in f. This definition is slightly different from the commutative case. As a consequence all slopes are ≥ 0. This is needed to ensure $N(fg) = N(f) + N(g)$. If f has only one slope $s = 0$ then f is called *regular singular*.

2.3.4 The Newton polynomial

Let $s \geq 0$ be a rational number. We have defined a valuation v_s and a truncation σ_a for non-zero elements of $k((x))[\delta]$ in section 2.2. σ_a depends on s and will from now on be denoted as $\sigma_{a,s}$.

If $s > 0$ then $\sigma_{1,s}(L)\sigma_{1,s}(R) = \sigma_{1,s}(LR) = \sigma_{1,s}(R)\sigma_{1,s}(L)$ for all L and R in $k((x))[\delta]$. If $s = 0$ then $\sigma_{1,s}(L)\sigma_{1,s}(R) = \sigma_{1,s}(LR) = S_{-v_s(L)}(\sigma_{1,s}(R)) \cdot S_{v_s(R)}(\sigma_{1,s}(L))$.

So $\sigma_{1,s}$ is commutative (i.e. is the same for LR and RL) if $s > 0$. If $s = 0$ then $\sigma_{1,s}$ is commutative up to substitutions $S_{-v_s(L)}$ and $S_{v_s(R)}$ which map δ to δ plus some integer.

To $\sigma_{1,s}(f)$ for $f \in k((x))[\delta]$ corresponds a certain polynomial, the so-called *Newton polynomial* $N_s(f)$ (the definition is given after the example) of f for slope s. The Newton polynomial is useful for factorization in $k((x))[\delta]$ because if $f = LR$ then $\sigma_{1,s}(L)\sigma_{1,s}(R) = \sigma_{1,s}(f)$. So a factorization of f induces a factorization of the Newton polynomial.

Example: Consider the following differential operator

$$f = 7x^{-5} + 2x^{-6}\delta + 2x^{-5}\delta + 3x^{-5}\delta^2 - 3x^{-5}\delta^3 + 5x^{-4}\delta^3 + x^{-4}\delta^5 \\ +2x^{-2}\delta^5 + 2x^{-3}\delta^6 + 3x^{-2}\delta^7 + 2x^{-1}\delta^8 + \delta^9$$

In figure 1 we have drawn every monomial $x^i\delta^j$ which appears in f by placing the coefficient of this monomial on the point (j,i). This gives a set of points (j,i). For all points (j,i) for which $x^i\delta^j$ has a non-zero coefficient in f we can draw the rectangle with vertices $(0,i)$, (j,i), (j,∞) and $(0,\infty)$. The Newton polygon is the convex hull of the union of all these rectangles. It is the part of the plane between the points $(0,\infty)$, $(0,-6)$, $(1,-6)$, $(5,-4)$, $(9,0)$ and $(9,\infty)$. In the commutative case (i.e. if we had written y instead of δ in f) the definition of the Newton polygon is slightly different and the point $(0,-6)$ would have been $(0,-5)$ in this example. But for $k((x))[\delta]$ the Newton polygon is defined in such a way that there are no negative slopes.

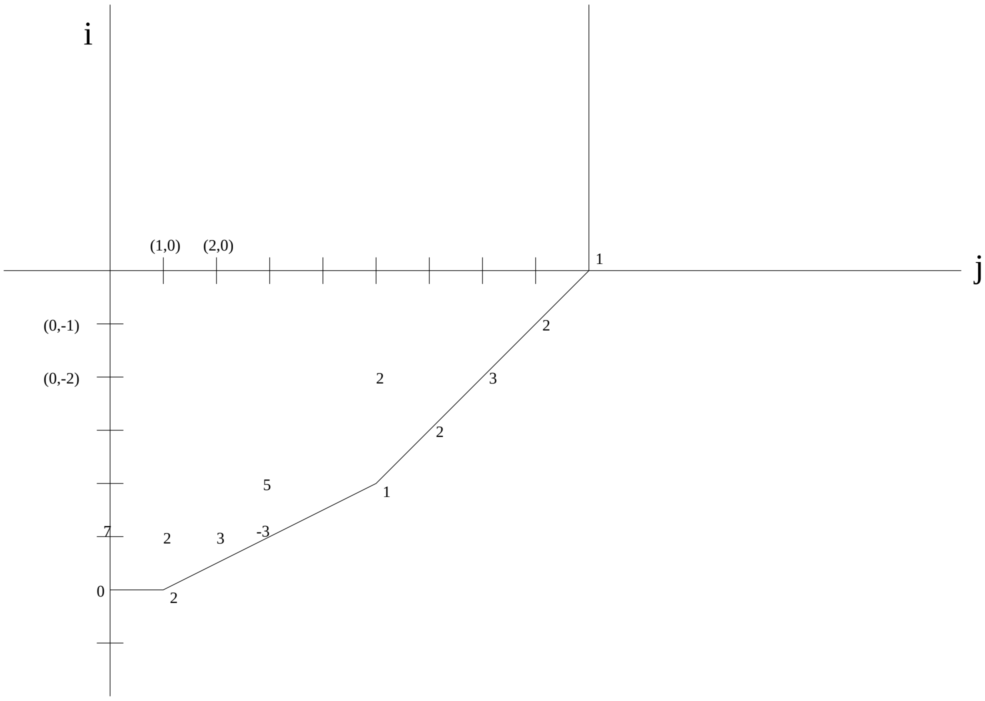

Fig. 1

The slopes of f are 0, 1/2 and 1. The Newton polynomials are $N_0(f) = 2T$, $N_{1/2}(f) = T^2 - 3T + 2$ and $N_1(f) = T^4 + 2T^3 + 3T^2 + 2T + 1$. Here T is used as a variable. $N_s(f)$ will be defined for all non-negative $s \in \mathbb{Q}$. However, we will only use the Newton polynomial for those values s which are a slope in the Newton polygon because for other values the Newton polynomial is trivial (i.e. degree 0).

Write $s = n/d$ where n and d are integers, $\gcd(n, d) = 1$ and $d > 0$. The valuation v_s gives a filtration (D_i), $i \in \mathbb{Z}$. $\sigma_{1,s}(f)$ is an element of $\overline{D} = \bigcup_{i\in\mathbb{Z}} D_i/D_{i+1}$. A multiplication is defined for elements of $\overline{D}$. An addition is only defined for $a, b \in \overline{D}$ which are element of the same D_i/D_{i+1}.

D_0 and $k[x^n\delta^d]$ are equal modulo D_1. There is a k-linear bijection

$$N'_s : D_i/D_{i+1} \to k[T]$$

which is also a ring isomorphism if $i = 0$. If $i = 0$ then N'_s is defined by $N'_s(x^n\delta^d) = T$.

For every $i \in \mathbb{Z}$ there is a unique pair of integers n_i, d_i such that the map ϕ_i : $D_0/D_1 \to D_i/D_{i+1}$ defined by $\phi(a) = x^{n_i}\delta^{d_i}a$ is a bijection. The integers n_i, d_i can be determined from the conditions $0 \le d_i < d$ and $v_s(x^{n_i}\delta^{d_i}) = i$. Now $N'_s(a)$ for $a \in D_i/D_{i+1}$ can be defined as $N'_s(\phi_i^{-1}(a))$. N'_s is also defined for non-zero elements of $f \in k((x))[\delta]$ as $N'_s(\sigma_{1,s}(f))$. In our example $N'_0(f) = 2T$, $N'_{1/2}(f) = T^2 - 3T + 2$ and $N'_1(f) = T^9 + 2T^8 + 3T^7 + 2T^6 + T^5$.

For slope $s = 0$ we define the Newton polynomial $N_0(f)$ as $N'_0(f)$. From the multiplication formula in section 2.3.2 the following property follows for $L, R \in k((x))[\delta]$

$$N_0(LR) = S_{T=T+v_0(R)}(N_0(L))N_0(R).$$

Here $S_{T=T+v_0(R)}(N_0(L))$ means $N_0(L)$ with T replaced by $T+v_0(R)$. For our example f we get $N_0(f \cdot f) = 4(T-6)T$.

For slope $s > 0$ we have the following property for $L, R \in k((x))[\delta]$

$$N'_s(LR) = T^p N'_s(L) N'_s(R).$$

Here p is either 0 or 1, depending on the slope s and the valuations $v_s(L)$ and $v_s(R)$. Let $i = v_s(L)$ and $j = v_s(R)$. Then $\phi_i(1) \cdot \phi_j(1) = x^{n_i+n_j}\delta^{d_i+d_j} \bmod D_{i+j+1}$. This is either equal to $\phi_{i+j}(1)$ or $x^n\delta^d\phi_{i+j}(1) \bmod D_{i+j+1}$, depending on whether $d_i + d_j$ is smaller than d or not. In the first case $p = 0$, in the second case $p = 1$. For our example $N'_{1/2}(f \cdot f) = T \cdot (N'_{1/2}(f))^2$ and $N'_1(f \cdot f) = (N'_1(f))^2$. Now define $N_s(f)$ as $N'_s(f)$ divided by T to the power the multiplicity of the factor T in $N'_s(f)$. Then

$$N_s(LR) = N_s(L) N_s(R)$$

for $s > 0$ and for all $L, R \in k((x))[\delta]$.

Note that our definition does not correspond to the usual definition of the Newton polynomial. It corresponds to the definition of the reduced characteristic polynomial in [3]. The roots of $N_0(f)$ in $\overline{k}$ are called the *exponents* of f. If $f \in k((x))[\delta]$ is regular singular (i.e. f has only one slope $s = 0$, or equivalently degree$(N_0(f)) =$ order(f)) and all exponents of f are integers then f is called *semi-regular*.

Property: If $f = LR$ then the Newton polynomial of the right-hand factor $N_s(R)$ divides $N_s(f)$. However, for a left-hand factor this need not hold. But if $s > 0$ or if $v_0(R) = 0$ (for example if R is regular singular and monic) then $N_s(f) = N_s(L)N_s(R)$ so in such cases $N_s(L)$ divides $N_s(f)$.

2.4 The lift algorithm

Suppose $f \in k((x))[\delta]$ is monic and that $f = LR$ is a non-trivial factorization, where L and R are monic elements of $k((x))[\delta]$. Let $s \geq 0$ be a rational number. Recall that there is a valuation v_s on $D = k((x))[\delta]$, a filtration $(D_{n,s})$, $n \in \mathbb{Z}$ and a truncation map $\sigma_{a,s}$ depending on s. In this section we will assume that L and R have been computed up to some accuracy a. How to compute this $\sigma_{a,s}(L)$ and $\sigma_{a,s}(R)$ will be the topic of the sections 2.5 and 2.7. In this section we deal with the question how to compute $\sigma_{a+1,s}(L)$ and $\sigma_{a+1,s}(R)$ from $\sigma_{a,s}(L)$, $\sigma_{a,s}(R)$ and f in an efficient way. The goal is an algorithm with the following specification:

Lift Algorithm:
Assumption: $f = LR$ where f, L, R are monic elements of $k((x))[\delta]$.
Input: $a \geq 1$, s, $\sigma_{a,s}(L)$, $\sigma_{a,s}(R)$ and f.
Output: Either $\sigma_{a+1,s}(L)$ and $\sigma_{a+1,s}(R)$ or "failed", where "failed" can only occur if $t > a$ where t is the coprime index.

We use this algorithm to lift a factorization. If the output is "failed" then we will use the less efficient method in section 2.7 to lift the factorization. Note that since $a \geq 1$ this can only happen if the coprime index is > 1.

Suppose $t \leq a$. We will use indeterminates for those coefficients of $\sigma_{a+t,s}(L)$ and $\sigma_{a+t,s}(R)$ which are not yet known. Then the equation $\sigma_{a+t,s}(LR) = \sigma_{a+t,s}(f)$ gives a set of equations in these unknowns (more details on how to find these equations are given below). $t \leq a$ is needed to ensure that all these equations are linear. Coprime index t means that $\sigma_{a+1,s}(L)$ and $\sigma_{a+1,s}(R)$ can be uniquely determined from these linear equations.

Except if the coprime index is 1, our algorithm usually does not know the coprime index in concrete situations. Then the lift algorithm will use a guess for the coprime index. If the lift algorithm is called for the first time, it takes $t = 2$. Otherwise it takes the guess for t that was used in the previous lift step. Then it will try, by solving linear equations, if there is a unique solution for $\sigma_{a+1,s}(L)$ and $\sigma_{a+1,s}(R)$ from $\sigma_{a,s}(L)$, $\sigma_{a,s}(R)$ and $\sigma_{a+t,s}(f)$. If so, t remains unchanged and the accuracy of the factorization increases; the output of the lift algorithm is $\sigma_{a+1,s}(L)$ and $\sigma_{a+1,s}(R)$. If the solution for $\sigma_{a+1,s}(L)$ and $\sigma_{a+1,s}(R)$ is not unique (there is at least one solution because of the assumption that the factorization $f = LR$ exists) the number t will be increased by 1. If t is still $\leq a$ then we can use recursion with our increased guess t for the coprime index. Otherwise, if $t > a$, the output of the lift algorithm is "failed", and we will have to use the less efficient method in section 2.7 to lift the factorization. Note that the efficiency of our lift algorithm depends on the coprime index, if this number is very high then it may not provide any speedup over the method from section 2.7.

A truncation $\sigma_{a,s}(R) = R + D_{v_s(R)+a}$ is stored as an element $R' \in k[x, 1/x, \delta]$ with no terms in $D_{v_s(R)+a}$. Now write

$$r = \sum_{i,j} r_{ij} x^i \delta^j$$

where the sum is taken over all i, j such that $v_s(R) + a \leq v_s(x^i\delta^j) < v_s(R) + a + t$ and $j \leq \mathrm{order}(R)$. Here r_{ij} are indeterminates. We set $r_{ij} = 0$ for $j = \mathrm{order}(R)$, $i \neq 0$, and set $r_{ij} = 1$ for $j = \mathrm{order}(R)$, $i = 0$. Similarly write L' and l. Now we look for values for the l_{ij} and r_{ij} such that $R' + r$ and $L' + l$ approximate R and L up to accuracy $a+1$. If the coprime index is t, the accuracy is at least $a+1$ if the following holds: $\sigma_{a+t,s}((L'+l)(R'+r)) = \sigma_{a+t,s}(f)$, or equivalently

$$(L'+l)(R'+r) \equiv f \mod D_{v_s(f)+a+t}.$$

$(L'+l)(R'+r) = L'R' + lR' + L'r + lr$. To determine $lR' \bmod D_{v_s(f)+a+t}$ it suffices to have R' up to accuracy t because $v_s(l) + v_s(R') \geq v_s(f) + a$. Similarly $\sigma_{t,s}(L')$ suffices to compute $L'r \bmod D_{v_s(f)+a+t}$. $v_s(lr) \geq v_s(f) + a + a \geq v_s(f) + a + t$ so lr vanishes modulo $D_{v_s(f)+a+t}$. Hence

$$f \equiv L'R' + l\sigma_{t,s}(R') + \sigma_{t,s}(L')r \mod D_{v_s(f)+a+t}.$$

By equating the coefficients of the left-hand side to the coefficients of the right-hand side (the coefficients of all monomials of valuation $< v_s(f) + a + t$) we find the linear equations in l_{ij} and r_{ij}. To determine these equations we must multiply l by $\sigma_{t,s}(R')$, ($= \sigma_{t,s}(R)$ because R' equals R up to accuracy a and $t \leq a$) which is the lowest block of R with slope s and width t in the Newton polygon of R. Similarly we must compute $\sigma_{t,s}(L')r$.

Usually the most time consuming part is the multiplication $L'R'$ modulo $D_{v_s(f)+a+t}$. One approach is the following. Compute $L'R'$ in $k[x, 1/x, \delta]$ and store the result together with L' and R'. In the next lift step a similar multiplication must be performed, but then L' and R' are slightly changed. Suppose we must compute the product $(L'+e_1)(R'+e_2)$ in the next lift step. Here L' and R' are large expressions and e_1 and e_2 are small. Using the previous multiplication $L'R'$ we can speed up this multiplication by writing $(L'+e_1)(R'+e_2) = L'R' + e_1R' + L'e_2 + e_1e_2$. The result of this multiplication is again stored for use in the next lift step.

In this approach $L'R'$ has been computed exactly. This is not efficient since we only need it up to accuracy $a+t$, i.e. modulo $D_{v_s(f)+a+t}$. Computing modulo $D_{v_s(f)+a+t}$ is not as convenient as computing modulo a power of x when using the multiplication formula in section 2.3.2. We compute $L'R'$ modulo a suitable power of x such that $L'R'$ can still be determined modulo $D_{v_s(f)+a+t}$. Unless the slope s is zero, however, a few more terms of the product $L'R'$ than needed have been computed then. These terms are stored to speed up the multiplication the next time that the lift algorithm is called.

2.5 Coprime index 1 factorizations

The lifting process for coprime factorizations can be done by solving linear equations. However, for coprime index 1 solving linear equations can be avoided. In this case we must solve a system (see section 2.4) of the form $l\sigma_{1,s}(R) + \sigma_{1,s}(L)r = g$ where g is computed by multiplying the so far computed truncations (called L' and R' in section 2.4) of L and R and subtracting this product from f. As in section 2.3.4 this equation can be converted to an equation $lR_0 + rL_0 = g$ for certain $l, r, L_0, R_0, g \in k[T]$ and l, r unknown. Such an equation can be solved by the Euclidean algorithm.

Consider the example f in section 2.3.4. f has slopes 0, 1/2 and 1 in this example. In [35] a method is given to compute a right-hand factor f_1 with only slope 0 and order 1, a right factor f_2 with slope 1/2 and order 4 and a right factor f_3 with slope 1 and order 4. The Newton polynomial of f_2 is the same as the Newton polynomial $N_{1/2}(f)$ of f for slope 1/2. It is $2-3T+T^2 = (T-1)(T-2)$. Because $\gcd(T-1, T-2) = 1$ this f_2 is again reducible in $\mathbb{Q}((x))[\delta]$, cf. [35]. It has a right factor g_1 of order 2 and slope 1/2 with Newton polynomial $T-1$ and a right factor g_2 with Newton polynomial $T-2$. So to obtain g_1 two factorization were needed. In one application, our algorithm for factorization in $\mathbb{Q}(x)[\partial]$, we are mainly interested in one of the irreducible right-hand factors of f in $\mathbb{Q}((x))[\delta]$. That is why we want to be able to compute g_1 directly without using an intermediate factorization to compute f_2. This is done by the following algorithm.

Algorithm Coprime Index 1 Factorizations:
Input: $f \in k((x))[\delta]$, f monic
Output: All monic coprime index 1 factorizations $f = LR$ in $k((x))[\delta]$ such that R does not have a non-trivial coprime index 1 factorization.
Note: the definition of coprime index depends on the valuation that is chosen on $k((x))[\delta]$. Here only the valuations v_s that are defined in section 2.2 are considered.

for all slopes s of f **do**
  $g := N_s(f)$
  Compute a prime factorization of g in $k[T]$, $g = cg_1^{e_1}\cdots g_r^{e_r}$,

where g_i are the different monic irreducible factors and $c \in k$.
if $s = 0$ **then**
$M := \{g_1, \ldots, g_r\}$
$N := M \setminus \{g | g(T) = h(T+i), h \in M, i \in \mathbb{N}, i > 0\}$
else
$N := \{g_1^{e_1}, \ldots, g_r^{e_r}\}$
end if
for h in N **do**
Write $h = T^p + h_{p-1}T^{p-1} + \ldots + h_0 T^0$.
Write $s = n/d$ with $d > 0$ and $\gcd(n,d) = 1$.
$R' := \delta^{pd} + h_{p-1}x^{-n}\delta^{(p-1)d} + h_{p-2}x^{-2n}\delta^{(p-2)d} + \ldots + h_0 x^{-pn}\delta^0$.
Now R' has Newton polynomial h. We want to lift R' to a right factor R such that R' is R modulo $D_{v_s(R')+1}$.
L' := an operator such that $\sigma_{1,s}(f) = \sigma_{1,s}(L'R')$.
L' is uniquely determined by requiring that L' has no monomials of valuation $> v_s(L')$.
f, L', R' with the lift algorithm gives a factorization $f = LR$
end do
end do

We need to prove the following:

1. L' and R' lift to a unique coprime index 1 factorization $f = LR$.
2. The right factors R do not allow a non-trivial coprime index 1 factorization.
3. All such coprime index 1 factorizations $f = LR$ (f, L and R monic) are obtained this way.

Suppose $\sigma_{a,s}(L'R') = \sigma_{a,s}(f)$, meaning that the factorization has been lifted up to accuracy a. If no lift steps were done yet, then $a = 1$. Now we look for $l \in D_{v_s(L')+a}$ and $r \in D_{v_s(R')+a}$ such that $\sigma_{a+1,s}((L'+l)(R'+r)) = \sigma_{a+1,s}(f)$ and $\mathrm{order}(r) < \mathrm{order}(R')$. To prove statement 1 we have to show that l, r exist and that $\sigma_{a+1,s}(L'+l)$ and $\sigma_{a+1,s}(R'+r)$ are uniquely determined. This means that $l \bmod D_{v_s(L)+a+1} \in \overline{D}$ (cf. section 2.3.4) and $r \bmod D_{v_s(R)+a+1} \in \overline{D}$ are uniquely determined. Then L' and R' are replaced by $L'+l$ and $R'+r$ and the accuracy of the approximations L' and R' for L and R has increased by 1. l and r must satisfy the following equation in $\overline{D}$

$$\sigma_{1,s}(L)r + l\sigma_{1,s}(R) = f - L'R' \bmod D_{v_s(f)+a+1}.$$

By applying N'_s we obtain the following equation in $k[T]$ if $s = 0$

$$S_{T=T+a}(L_0)r_0 + l_0 R_0 = g$$

and

$$L_0 r_0 + l_0 R_0 = g \quad \text{or} \quad TL_0 r_0 + l_0 R_0 = g$$

if $s > 0$. Here $L_0 = N'_s(L)$, $R_0 = N'_s(R)$, $l_0 = N'_s(l \bmod D_{v_s(L)+a+1})$, $r_0 = N'_s(r \bmod D_{v_s(R)+a+1})$ and $g = N'_s(f - L'R' \bmod D_{v_s(f)+a+1})$. Note that $v_s(R)$ is 0 if $s = 0$. The requirement $\mathrm{order}(r) < \mathrm{order}(R)$ means $\mathrm{degree}(r_0) < \mathrm{degree}(R_0)$.

To prove statement 1 we now have to show that $l_0, r_0 \in k[T]$ exist and are uniquely determined. For this it is sufficient to show that $\gcd(TL_0, R_0) = 1$ if $s > 0$ and $\gcd(S_{T=T+a}(L_0), R_0) = 1$ if $s = 0$. First the case $s > 0$. R_0 is the factor h of the Newton polynomial in the algorithm. $L_0 R_0 = N'_s(f) = T^i N_s(f)$ for some integer i. The set N of factors h of $N_s(f)$ is chosen in such a way in the algorithm that $\gcd(h, N_s(f)/h) = 1$. Also $\gcd(h, T) = 1$ because $N_s(f)$ does not contain a factor T by definition and h is a factor of $N_s(f)$. So $\gcd(TL_0, R_0) = 1$. Now the case $s = 0$. We have $L_0 R_0 = N_s(f)$ because $v_s(R) = 0$ (see the multiplication formula for N_0 in section 2.3.4). R_0 is the factor h of $N_s(f)$ in the algorithm. We have to show that $\gcd(S_{T=T+a}(L_0), R_0) = 1$. The set N containing these factors h was chosen in such a way that this holds for all $a \geq 1$.

To prove the second statement we distinguish 2 cases. Suppose $s = 0$. Then the Newton polynomial of R is irreducible. Hence R must be irreducible because a factorization of R gives a factorization of the Newton polynomial. Now suppose $s > 0$. Then the Newton polynomial is of the form p^i where p is irreducible and i is an integer. If $i > 1$ then it is not clear whether R is reducible or not. Suppose R can be factored $R = R_1 R_2$. Then the Newton polynomials of R_1 and R_2 are both factors of p^i. So the gcd of these Newton polynomials is not equal to 1. Coprime index 1 would mean that $\sigma_{a+1,s}(R_1)$ and $\sigma_{a+1,s}(R_2)$ can be uniquely determined from $\sigma_{a,s}(R_1)$, $\sigma_{a,s}(R_2)$ and $\sigma_{a+1,s}(f)$. To determine $\sigma_{a+1,s}(R_1)$ and $\sigma_{a+1,s}(R_2)$ requires solving an equation $l_0 N_s(R_1) + r_0 N_s(R_2) = g$ in $k[T]$. Such an equation has a unique solution if and only if the gcd of the Newton polynomials $N_s(R_1)$ and $N_s(R_2)$ is 1. So a possible factorization $R = R_1 R_2$ can not be a coprime index 1 factorization, which proves statement 2.

Suppose $f = LR$ is a monic factorization satisfying statement 2. Now we need to show that the algorithm finds this factorization. R can have only one slope s, otherwise it could be factored by the given algorithm (which contradicts the assumption that statement 2 holds). First consider the case $s = 0$. Then $N_s(R)$ must be an irreducible polynomial, otherwise R can be factored by the algorithm. So $N_s(R)$ must be an element of the set M in the algorithm. It can not be an element of $\{g | g(T) = h(T+i), h \in M, i \in \mathbb{N}, i > 0\}$ because then $\gcd(S_{T=T+a}(L_0), R_0) = 1$ does not hold for all $a \geq 1$ which was shown to be a necessary and sufficient condition for having coprime index 1 if $s = 0$. So $N_s(R) \in N$. This means that $\sigma_{1,s}(R)$ and hence also $\sigma_{1,s}(L)$ are the same as $\sigma_{1,s}(R_1)$ and $\sigma_{1,s}(L_1)$ for a factorization L_1, R_1 of f given by the algorithm. Because the coprime index is 1 this factorization L_1, R_1 is completely determined by $\sigma_{1,s}(R_1)$, $\sigma_{1,s}(L_1)$ and f. Hence these two factorizations $L_1 R_1$ and LR are the same and so the third statement holds. In the same way the case $s > 0$ is proven.

□

Remark: the given method can also be applied for factorization in the ring $L[\delta]$ where L is a finite extension of $k((x))$, because

- The method is not different for algebraic extensions of the constants $k \subset l$.
- Ramifications over $l((x))$ can be handled using the map $\theta_{a,n}$ in section 2.3.2.
- All finite field extensions of $k((x))$ are obtained as an algebraic extension of the constants followed by a ramification, cf. section 2.3.1.

Consider again the example f in section 2.3.4 and let $k = \mathbb{Q}$. The given algorithm produces a right-hand factor R_1 with slope 0, order 1 and Newton polynomial T, a right factor R_2 with slope $1/2$, order 2 and polynomial $T-1$, a right factor R_3 with slope $1/2$, order 2 and polynomial $T-2$ and a right factor R_4 with slope 1, order 4 and Newton polynomial $(T^2+T+1)^2$. Now R_1, R_2 and R_3 are irreducible in $\mathbb{Q}((x))[\delta]$ because their Newton polynomials are irreducible. But it is not yet clear whether R_4 is irreducible or not. The second example in section 2.1 remains unfactored as well. Reducible operators f that remain unfactored by the given factorization algorithm are of the following form: f has one slope $s > 0$ and $N_s(f)$ is a power > 1 of an irreducible polynomial. The given algorithm will compute only a trivial factorization $L = 1$, $R = f$ for this case. If such an operator is reducible then a factorization must have coprime index > 1. In section 2.6 the notion of exponential parts will be introduced. Using exponential parts a description of the irreducible elements of $k((x))[\delta]$ will be given.

If f has one slope $s > 0$, $s \in \mathbb{N}$ and the Newton polynomial is a power of a polynomial of degree 1, then compute $S_{cx^{-s}}(f)$ where c is the root of the Newton polynomial (see also case 4 of the algorithm in section 2.5.1). Then apply the factorization algorithm to $S_{cx^{-s}}(f)$ and find a factorization of f by applying $S_{-cx^{-s}}$ to the factors of $S_{cx^{-s}}(f)$. For all other cases (i.e. $s \notin \mathbb{N}$ or degree$(N_s(f)) > 1$) we apply the method in section 2.7. The factorization obtained that way lifts rather slowly, i.e. it costs much time to compute more terms. The lifting will be speeded up using the lift method of section 2.4 whenever that is possible (when its output is not the message "failed").

A differential operator can have infinitely many different factorizations. For example ∂^2 which equals $1/x^2$ times $\delta^2 - \delta$ has $ax + b$ as solutions, where a and b are constants. Hence it has $\partial - (ax+b)'/(ax+b) = \partial - a/(ax+b)$ as right factors. Note that algorithm coprime index 1 factorizations produces only a finite number of different factorizations. In the semi-regular case (cf. section 2.3.4) it computes only 1 unique factorization, although like the example ∂^2 shows other factorizations could exist as well.

2.5.1 Computing first order factors over $\overline{k((x))}$

An element r of some differential extension of $k((x))$ is by definition a *Riccati solution* of $f \in k((x))[\delta]$ if $\delta - r$ is a right factor of f. The reason this is called Riccati solution is that they are solutions of the so-called *Riccati equation*. This is a non-linear differential equation. The Riccati equation of $f \in k((x))[\delta]$ can be found by computing a right division of f by $\delta - u$, where u is an indeterminate. The remainder of this right division is the Riccati equation. It is a polynomial in u and the derivatives of u. It vanishes precisely when we substitute for u an element r such that $\delta - r$ is a right-hand factor of f. The Riccati solutions are of the form xy'/y where y is a solution of f. In the usual definition the Riccati solutions are the logarithmic derivatives y'/y of solutions of f. The definition in this chapter differs by a factor x because we work with $\delta = x\partial$ instead of ∂. In this chapter only Riccati solutions in $\overline{k((x))}$ are considered. In general there exist more Riccati solutions in larger differential fields. The implementation does not determine the Riccati equation itself because this can be a large expression. Instead we use factorization to find Riccati solutions. Computing first order right-hand factors of f is the same as computing Riccati solutions.

The following algorithm is similar to the Rational Newton algorithm (cf. [3]) which is a version of the Newton algorithm (cf. [54, 19]) that computes formal solutions using a minimal algebraic extension of the constants field k. A difference between the Rational Newton algorithm and the following algorithm Riccati solution is that we use factorization of differential operators. So the order of the differential operator decreases during the computation.

Algorithm Riccati solution:
Input: $f \in k((x))[\delta]$
Output: a first order right-hand factor in $\overline{k((x))}[\delta]$

1. If $\mathrm{order}(f) = 1$ then the problem is trivial.
2. If one of the following holds
   (a) f is regular singular and the $N_0(f)$ is reducible.
   (b) The Newton polygon has more than 1 slope.
   (c) f has one slope $s > 0$ and $N_s(f)$ is not a power ≥ 1 of an irreducible polynomial.

   then compute a coprime index 1 factorization and apply recursion to the right-hand factor.
3. If f has one slope s and the Newton polynomial $N_s(f)$ is of the form p^e with p irreducible, $e \geq 1$ and p is of degree $d > 1$. Then extend k by one root r of p. Now compute a right factor of order $\mathrm{order}(f)/d$ with $(T-r)^e$ as Newton polynomial using a coprime index 1 factorization as in the algorithm in section 2.5. This is a coprime index 1 factorization because the gcd of $(T-r)^e$ and $p^e/(T-r)^e$ (this is the Newton polynomial of the left hand factor) is 1. Now apply recursion to the right-hand factor.
4. If f has one slope $s > 0$, $s \in \mathbb{N}$ and $N_s(f)$ is a power of a polynomial of degree 1, then compute $S_{cx^{-s}}(f)$ where c is the root of $N_s(f)$. Use recursion (this recursion is valid because the slopes of $S_{cx^{-s}}(f)$ are smaller than the slope of f) to find a first order factor of $S_{cx^{-s}}(f)$. Then apply $S_{-cx^{-s}}$.
5. If f has one slope $s > 0$, $s \notin \mathbb{N}$ and the Newton polynomial is a power of a polynomial of degree 1, then write $s = n/d$ with $\gcd(n,d) = 1$, $n > 0$. Now we will apply a ramification of index d. Instead of extending the field $k((x))$ we apply the isomorphism $\theta_{a,d} : k((r))[\delta] \rightarrow k((x))[\delta]$ of section 2.3.2. First we need to compute a suitable value $a \in k$. $\theta_{a,d}(x) = \theta_{a,d}(r^d/a) = x^d/a$. Write the Newton polynomial of f as $(T-c)^e$, where $c \in k$ and $e \in \mathbb{N}$. Then the Newton polynomial of $\theta_{a,d}(f)$ equals a constant times $(T^d - d^d c a^n)^e$. Now choose a equal to c^p, $p \in \mathbb{Z}$, such that $d^d c a^n$ is a d-th power of an element $b \in k$. This is done by choosing p such that $pn + 1$ is a multiple of d. Then the Newton polynomial $(T^d - d^d c a^n)^e$ equals $(T^d - b^d)^e$ and can be factored as $(T-b)^e g^e$ with $\gcd((T-b)^e, g^e) = 1$. Now use a coprime index 1 factorization as in section 2.5

with $(T-b)^e$ as Newton polynomial for the right-hand factor. This provides a right factor R of order $e = \mathrm{order}(f)/d$. Now use recursion on R to find a first order factor and apply $\theta_{a,d}^{-1}$.

Note that there are two cases where a field extension of $k((x))$ is applied. One case was an extension of k of degree d, and the other case was a ramification of index d. Both these cases were extensions of $k((x))$ of degree d. In both cases the algorithm finds a right factor of order $\mathrm{order}(f)/d$ over this algebraic extension. In the three other cases field extensions were not needed. We can conclude

Lemma 1 *Every $f \in k((x))[\delta]$ has a Riccati solution which is algebraic over $k((x))$ of degree $\leq \mathrm{order}(f)$.*

2.6 Exponential parts

A commutative invariant is a map ϕ from $k((x))[\delta]$ to some set such that $\phi(fg) = \phi(gf)$ for all $f, g \in k((x))[\delta]$. An example is the Newton polygon, i.e. $N(fg) = N(gf)$ for all non-zero f and g. However, there are more properties of differential operators that remain invariant under changing the order of multiplication. We want a commutative invariant which contains as much information as possible. In [52] Sommeling defines *normalized eigenvalues* and *characteristic classes* for matrix differential operators. The topic of this section is the analogue of normalized eigenvalues for differential operators in $k((x))[\delta]$. We will call these *exponential parts*. The exponential parts are useful for several topics. They appear as an exponential integral in the formal solutions (this explains the name exponential part). They describe precisely the algebraic extensions over $k((x))$ needed to find the formal solutions. The exponential parts are also used in our method of factorization in the ring $k(x)[\partial]$ in chapter 3. For factorization in $k((x))[\delta]$ the exponential parts will be used to describe the irreducible elements, (cf. theorem 2).

Differential operators (in this chapter that means elements of $k((x))[\delta]$ or $\overline{k((x))}[\delta]$) can be viewed as a special case of matrix differential operators. So our definition of exponential parts could be viewed as a special case of the definition of normalized eigenvalues in [52]. A reason for giving a different definition is that the tools for computing with matrix differential operators are not the same as for differential operators. Important tools for matrix differential operators are the splitting lemma and the Moser algorithm. The tools we use for differential operators are the substitution map and the Newton polynomial. That is why we want to have a definition of exponential parts expressed in these tools. Because then the definition allows the computation of exponential parts using a variant of the "algorithm Riccati solution", namely the "algorithm semi-regular parts" in section 2.8.4. A second reason for our approach is that it allows the definition of semi-regular parts of differential operators.

Let L be a finite extension of $k((x))$. Since $L \subset \overline{k}((x^{1/n}))$ for some integer n we can write every $r \in L$ as $r = e + t$ with $e \in E$ and $t \in x^{1/n}\overline{k}[[x^{1/n}]]$. Now e is called the *principal part* $\mathrm{pp}(r)$ of $r \in L$. Using the following lemma we can conclude $e \in k((x))[r] \subset L$.

Lemma 2 *Let $n \in \mathbb{Q}$ and $r \in \overline{k((x))}$ be equal to $r_n x^n$ plus higher order terms. Then $r_n x^n$ is an element of the field $k((x))[r]$.*

Proof: Write $r = r_n x^n + r_m x^m$ plus higher order terms, where $m \in \mathbb{Q}$, $m > n$. We want to prove that there exists an $s \in k((x))[r]$ of the form $r_n x^n$ plus terms higher than x^m. Then we can conclude $r_n x^n \in k((x))[r]$ by repeating this argument and using the fact that the field $k((x))[r]$ is complete (cf. [12] Chap I, §2, thm. 2). We can find this s as a $\mathbb{Q}$-linear combination of r and $x\frac{dr}{dx}$.

□

Definition 1 *Let $f \in k((x))[\delta]$, $e \in E$ and $n = \mathrm{ram}(e)$. Let $P = N_0(S_e(f))$, the Newton polynomial corresponding to slope 0 in the Newton polygon of $S_e(f) \in \overline{k}((x^{1/n}))[\delta]$. Now $\mu_e(f)$ is defined as the number of roots (counted with multiplicity) of P in $\frac{1}{n}\mathbb{Z}$ and $\overline{\mu}_e(f)$ is defined as the number of roots (counted with multiplicity) of P in $\mathbb{Q}$.*

Recall that $\mathrm{ram}(e)$ denotes the ramification index of e. Note that we have only defined the Newton polynomial for elements of $k((x))[\delta]$, not for ramifications of $\underline{k((x))}$. Define $N_0(f)$ for $f \in \overline{k}((x^{1/n}))[\delta]$ as follows. Write $f = \sum_i x^{i/n} f_i$ with $f_i \in \overline{k}[\delta]$. Then $N_0(f)$ is (written as a polynomial in δ instead of T) defined as f_i where i is minimal such that $f_i \neq 0$.

We define an equivalence $\sim$ on E as follows: $e_1 \sim e_2$ if $e_1 - e_2 \in \frac{1}{n}\mathbb{Z}$ where n is the ramification index of e_1. Note that the ramification indices of e_1 and e_2 are the same if $e_1 - e_2 \in \mathbb{Q}$. If $e_1 \sim e_2$ then $\mu_{e_1}(f) = \mu_{e_2}(f)$ for all $f \in k((x))[\delta]$ so we can define μ_e for $e \in E/\sim$. Similarly $\overline{\mu}_e(f)$ is defined for $e \in E/\mathbb{Q}$.

Definition 2 *The* exponential parts *of an operator $f \in k((x))[\delta]$ are the elements $e \in E/\sim$ for which $\mu_e(f) > 0$. The number $\mu_e(f)$ is the* multiplicity *of e in f.*

Lemma 3 *Let $f = LR$ where f, L and R are elements of $\overline{k}((x^{1/n}))[\delta]$. Let N_f be the number of roots of $N_0(f)$ in $\frac{1}{n}\mathbb{Z}$, counted with multiplicity. Similarly define N_L and N_R. Then $N_f = N_L + N_R$.*

The proof of this lemma is not difficult; we will skip it. Note that if $n = 1$ then $N_f = \mu_0(f)$.

Lemma 4 *If $f = LR$ where f, L and R are elements of $k((x))[\delta]$ and e in E or in $E/\sim$ then $\mu_e(f) = \mu_e(L) + \mu_e(R)$.*

If $f = LR$ where f, L and R are elements of $\overline{k((x))}[\delta]$ and e in E or in $E/\mathbb{Q}$ then $\overline{\mu}_e(f) = \overline{\mu}_e(L) + \overline{\mu}_e(R)$.

Proof: If n is the ramification index of e, then $\mu_e(f)$ is the number of roots in $\frac{1}{n}\mathbb{Z}$ of $N_0(S_e(f))$. Now the first statement follows using the previous lemma and the fact that $S_e(f) = S_e(L)S_e(R)$. The proof for $\overline{\mu}$ is similar.

□

Theorem 1 *Let f be a non-zero element of $k((x))[\delta]$, then the sum of the multiplicities of all exponential parts is:*

$$\sum_{e \in E/\sim} \mu_e(f) = \mathrm{order}(f).$$

Let f be a non-zero element of $\overline{k((x))}[\delta]$, then

$$\sum_{e \in E/\mathbb{Q}} \overline{\mu}_e(f) = \mathrm{order}(f).$$

Proof: If $\mathrm{order}(f) = 1$ then both statements hold. If f is reducible then we can use induction and lemma 4 so then both statements hold. In $\overline{k((x))}[\delta]$ every operator of order > 1 is reducible (see also the algorithm in section 2.5.1 which computes a first order right-hand factor in $\overline{k((x))}[\delta]$) so the second statement holds.

To prove the first statement we need to show that the sum of the multiplicities is the same for μ over all $e \in E/\sim$ and $\overline{\mu}$ over all $e \in E/\mathbb{Q}$. Suppose $\overline{e}$ is an element of $E/\mathbb{Q}$. The sum of $\mu_e(f)$ taken over all $e \in E/\sim$ such that $\overline{e} \equiv e \bmod \mathbb{Q}$ is equal to $\overline{\mu}_{\overline{e}}(f)$ because they are both equal to the number of rational roots of the same Newton polynomial. So we can see that the sum of the multiplicities $\overline{\mu}$ is the same as sum of the multiplicities μ by grouping together those exponential parts of f that are congruent modulo $\mathbb{Q}$.

□

2.6.1 Semi-regular part

An operator $f \in k((x))[\delta]$ is called *semi-regular* over $k((x))$ if f has only one exponential part which is equal to $0 \in E/\sim$. A semi-regular operator is a regular singular operator with only integer roots of the Newton polynomial. In other words $\mu_0(f) = \mathrm{order}(f)$. An operator $f \in k((x))[\delta] = k((x))[\partial]$ is *regular* (or: non-singular) if f can be written as a product of an element of $k((x))$ and a monic element of $k[[x]][\partial]$. A regular operator is regular singular and the roots of the Newton polynomial are $0, 1, \ldots, \mathrm{order}(f)-1$. So a regular operator is semi-regular. We can generalize the notion of semi-regular for algebraic extensions $k((x)) \subset L$.

Definition 3 *$f \in L[\delta]$ is called* semi-regular *over L if it is regular singular and all roots of $N_0(f)$ are integers divided by the ramification index of L.*

For a ramification $r^n = ax$ an isomorphism $\theta_{a,n} : k((r))[\delta] \to k((x))[\delta]$ was given in section 2.3.2. Now $f \in k((r))[\delta]$ is semi-regular over $k((r))$ if and only if $\theta_{a,n}(f) \in k((x))[\delta]$ is semi-regular over $k((x))$.

Definition 4 *Let $f \in k((x))[\delta]$. Then the* semi-regular part *R_e of f for $e \in E$ is the monic right-hand factor in $k((x))[e, \delta]$ of $S_e(f)$ of order $\mu_e(f)$ which is semi-regular over $k((x))[e]$.*

R_e can be computed by a coprime index 1 factorization of $S_e(f)$ as in section 2.5 using slope $s = 0$. The Newton polynomial (called h in the algorithm) is the largest factor of $N_0(S_e(f))$ for which all roots are integers divided by the ramification index. Since such coprime index 1 factorizations for a given Newton polynomial are unique (see the comments after Algorithm Coprime Index 1 Factorizations) it follows that R_e is uniquely defined. Note that if the ramification index n is > 1 then in fact our algorithm does not compute with $S_e(f)$ but with $\theta_{a,n}(S_e(f))$ for some constant a, cf. the remark on page 23. Then we have to compute the highest order factor of $\theta_{a,n}(S_e(f))$ of which the roots of the Newton polynomial are integers, instead of integers divided by n.

$S_{-e}(R_e)$ is a right-hand factor of f. Note that if $e_1 \sim e_2$ then $S_{-e_1}(R_{e_1}) = S_{-e_2}(R_{e_2})$. Hence $S_{-e_1}(R_{e_1}), \ldots, S_{-e_p}(R_{e_p})$ in the following lemma are up to a permutation uniquely determined by f.

Lemma 5 *Let f be an element of $k((x))[\delta]$. Let $e_1, \ldots, e_p \in E$ be a list of representatives of all exponential parts in $E/\sim$ of f. Then*

$$f = \mathrm{LCLM}(S_{-e_1}(R_{e_1}), \ldots, S_{-e_p}(R_{e_p})).$$

Remark: A similar statement (expressed in the terminology of D-modules) is given in corollaire 4.3.1 in [35]. There is, however, a subtle but important difference namely that in our lemma the operators R_i are semi-regular instead of regular singular. To this difference corresponds a different notion of exponential parts as well; in corollaire 4.3.1 in [35] a notion appears which, in our terminology, can be viewed as elements of $E/\overline{k}$ instead of our $E/\sim$. One often distinguishes the two notions irregular singular and regular singular. In this thesis we propose to drop the notion of regular singular as much as possible and only to make a distinction between semi-regular and not semi-regular, and measure the "non-semi-regularity" using the exponential parts in $E/\sim$. The motivation for doing this is to generalize algorithms that work for regular singular operators to the irregular singular case. We will see later (chapters 3, 4 and 5) the benefits of this approach.

Proof: Let $R = \mathrm{LCLM}(S_{-e_1}(R_{e_1}), \ldots, S_{-e_p}(R_{e_p}))$. Conjugation over $k((x))$ only permutes $S_{-e_1}(R_{e_1}), \ldots, S_{-e_p}(R_{e_p})$. Hence R is invariant under conjugation over $k((x))$ and so $R \in k((x))[\delta]$. $S_{-e_i}(R_{e_i})$ is a right factor of R, so R_{e_i} is a right factor of $S_{e_i}(R)$. So $N_0(R_{e_i})$ is a factor of $N_0(S_{e_i}(R))$, hence $\mu_{e_i}(R) \geq \mathrm{degree}(N_0(R_{e_i})) = \mu_{e_i}(f)$ because all roots of $N_0(R_{e_i})$ are integers divided by the ramification index. Then by theorem 1 we can conclude $\mathrm{order}(R) \geq \mathrm{order}(f)$. R is a right-hand factor of f because the $S_{-e_i}(R_{e_i})$ are right factors of f. Hence $f = R$.

□

This provides a method to compute a fundamental system of solutions of f. The solutions of $f = \mathrm{LCLM}(S_{-e_1}(R_{e_1}), \ldots, S_{-e_p}(R_{e_p}))$ are spanned by the solutions of $S_{-e_1}(R_{e_1}), \ldots, S_{-e_p}(R_{e_p})$. The solutions of $S_{-e_1}(R_{e_1})$ are obtained by multiplying the solutions of R_{e_1} by $\mathrm{Exp}(e_1)$ (recall that $\mathrm{Exp}(e_1) = \exp(\int \frac{e_1}{x} dx)$, cf. section 2.3.2). Consequently, when all e_i and R_{e_i} have been computed, then the problem of finding the solutions of f is reduced to solving semi-regular differential operators, which is a much easier problem (cf. section 2.8.1).

Define $\overline{R}_e$ for $e \in E$ and $f \in \overline{k((x))}[\delta]$ as the largest regular singular factor of $S_e(f)$ for which all roots of the Newton polynomial are rational numbers. Now we can show in the same way for $f \in \overline{k((x))}[\delta]$ that

$$f = \mathrm{LCLM}(S_{-e_1}(\overline{R}_{e_1}), \ldots, S_{-e_q}(\overline{R}_{e_q})) \tag{2.1}$$

where $e_1, \ldots, e_q \in E$ is a list of representatives for all $e \in E/\mathbb{Q}$ for which $\overline{\mu}_e(f) > 0$.

2.6.2 Irreducible elements of $k((x))[\delta]$

If $r \in \overline{k((x))}$ is a Riccati solution of $f \in k((x))[\delta]$ then the principal part $e = \mathrm{pp}(r) \in k((x))[r]$ modulo $\sim$ is an exponential part of f. Conversely, if $\mu_e(f) > 0$ then f has Riccati solution $r_e \in k((x))[e]$ of which the principal part is e modulo $\sim$. Though there may be infinitely many such Riccati solutions, we can compute one such r_e in a canonical way. The algorithm in section 2.5 provides (although infinitely many different factorizations could exist) only 1 unique factorization of semi-regular operators (namely the one that has coprime index 1). This way we can compute a unique right factor $\delta - r_e$ of $S_{-e}(R_e)$ by computing a first order factor of R_e and applying S_{-e}. If $e_1 \sim e_2$ then $r_{e_1} = r_{e_2}$. So r_e is defined for exponential parts $e \in E/\sim$ of f.

Suppose $e_1 \in E$ is algebraic over $k((x))$ of degree d and suppose $\mu_{e_1}(f) > 0$. Suppose $e_1, \ldots, e_d \in \overline{k((x))}$ are the conjugates of e_1 over $k((x))$. If L is a Galois extension of $k((x))$ then conjugation over $k((x))$ is an automorphism of $L[\delta]$. So $\mu_{e_i}(f) = \mu_{e_j}(f)$ for all i, j. We can find unique right factors $\delta - r_{e_i} \in k((x))[e_i, \delta] \subset \overline{k((x))}[\delta]$ of f as just described. Then $R = \mathrm{LCLM}(\delta - r_{e_1}, \ldots, \delta - r_{e_d})$ is a right-hand factor of f. Because conjugation is an automorphism the r_{e_i} are all conjugates of r_{e_1} over $k((x))$. So the set $\{\delta - r_{e_1}, \ldots, \delta - r_{e_d}\}$ is invariant under conjugation which implies that R is invariant under conjugation over $k((x))$. Hence $R \in k((x))[\delta]$. In general

$$\mathrm{order}(\mathrm{LCLM}(f_1, \ldots, f_n)) \leq \sum_i \mathrm{order}(f_i)$$

because the order of an operator is equal to the dimension of the solution space, and the solution space of $\mathrm{LCLM}(f_1, \ldots, f_n)$ is spanned by the solutions of $f_1, \ldots, f_n$. So $\mathrm{order}(R) \leq d$. Since $\mu_{e_i}(R) = \mu_{e_1}(R) > 0$ for all $i = 1, \ldots, d$ we can conclude by theorem 1 that $\mathrm{order}(R) \geq d$ if all e_i represent different exponential parts. For this we must prove $e_i - e_j \notin \mathbb{Q}$ if $i \neq j$. Suppose $e_i - e_j \in \mathbb{Q}$. We now have to prove that $e_i = e_j$. The Galois group G of $k((x))[e_1, \ldots, e_d]$ over $k((x))$ acts transitively on $e_1, \ldots, e_d$. Hence $\gamma(e_i) = e_j$ for some $\gamma \in G$. If $\gamma(e_i) = e_i + (e_j - e_i)$ where $(e_j - e_i) \in \mathbb{Q}$ then $\gamma^{\#G}(e_i) = e_i + (\#G)(e_j - e_i)$. Here $\#G$ denotes the number of elements of G. However, for any finite group G and element $\gamma \in G$ the equation $\gamma^{\#G} = 1$ holds so $\gamma^{\#G}(e_i) = e_i$. Hence $(\#G)(e_j - e_i) = 0$ and $e_i = e_j$. Now we can conclude $\mathrm{order}(R) = d$. We have partly proven the following

Theorem 2 *$f \in k((x))[\delta]$ has an exponential part e which is algebraic over $k((x))$ of degree d if and only if f has an irreducible right-hand factor $R \in k((x))[\delta]$ of order d.*

Note: In a different terminology (normalized eigenvalues, characteristic classes and D-modules) this result is found in [52] as well.

Proof: Given an exponential part of degree d over $k((x))$ we have already shown how to construct R as $\mathrm{LCLM}(\delta - r_{e_1}, \ldots, \delta - r_{e_d})$. Now we must show that R is irreducible in $k((x))[\delta]$. Suppose R has a non-trivial right-hand factor R_1 of order $d_1 < d$. By induction we can conclude that R_1 has an exponential part e which is algebraic over $k((x))$ of degree d_1. Lemma 4 shows that e is an exponential part of R. Then $e, e_1, \ldots, e_d$ are $d + 1$ different exponential parts of R contradicting theorem 1. So R is irreducible.

Now suppose f has an irreducible right factor R of order d. The exponential parts of R are exponential parts of f by lemma 4. We will show that all exponential parts of R are conjugated over $k((x))$ and algebraic of degree d over $k((x))$. Let e_1 be an exponential part of R algebraic of degree p over $k((x))$. So the conjugates $e_1, \ldots, e_p$ are exponential parts of R and by our construction we find an irreducible factor R_1 of R of order p. Since R is irreducible we have $R_1 = R$ and hence $p = d$. Now $e_1, \ldots, e_d$ are d different exponential parts of R. Because of theorem 1 there can not be more exponential parts, so all exponential parts of R are conjugated with e_1.

□

2.7 Coprime index > 1 factorization

How can one compute an irreducible factor of a polynomial $f \in \mathbb{Q}[y]$? A method is to compute a root r and the minimum polynomial of r. This is not the usual factorization method for the ring $\mathbb{Q}[y]$. But for the ring $k((x))[\delta]$ this idea supplies a method for the cases we have not yet treated. The role of the root is played by a Riccati solution. The analogue of the minimum polynomial for a Riccati solution r is the least common left multiple of $\delta - r$ and its conjugates. A minimum polynomial is the product of $y - r$ and its conjugates. One does not need to compute the conjugates to determine this product. The same holds for the least common left multiple. To see this write the LCLM as an operator R with undetermined coefficients $R = a_n\delta^n + \cdots + a_0\delta^0$. Now the statement that $\delta - r$ is a right factor of R translates into a linear equation in $a_0, \ldots, a_n$. This is an equation over $k((x))[r]$. We know that all conjugated equations (which we do not compute) hold as well. Then this system of equations can be converted to a system over $k((x))$. We show how this can be done in a slightly more general situation. Suppose α is algebraic of degree d over a field K and we have an equation $b_0\alpha^0 + \cdots b_{d-1}\alpha^{d-1} = 0$ (in our application $K = k((x))$, $\alpha = r$ and the b_i are $k((x))$-linear expressions in a_i). The system formed by this linear equation and all its conjugates is equivalent with $b_0 = b_1 = \cdots = b_{d-1} = 0$. The reason is that the transition matrix (which is a Vandermonde matrix) between these two systems of linear equations is invertible.

This method for computing R is not very efficient for two reasons. The right-hand factor R is computed by solving linear equations over $k((x))$ which is rather complicated. The computation of these linear equations involves an algebraic extension over $k((x))$. So we prefer to lift R with the algorithm in section 2.4 whenever possible.

Example:

$$f = \delta^4 + 2\delta^3 - \frac{2}{x}\delta^2 + \frac{9}{4x} + \frac{1}{x^2} \in k((x))[\delta]$$

The exponential parts are $e_1 = \frac{1}{\sqrt{x}} + \frac{\sqrt{-1}}{2}$ in $E/\sim$ and the conjugates e_2, e_3, e_4 of e_1 over $\mathbb{Q}((x))$. If $\sqrt{-1} \notin k$ then e_1 is algebraic of degree 4 over $k((x))$ and then f is irreducible in $k((x))[\delta]$. Now assume that $\sqrt{-1} \in k$. Then e is algebraic of degree 2 over $k((x))$ and hence f has an irreducible right-hand factor $R \in k((x))[\delta]$ of order 2. To e_1 corresponds the following right-hand factor in $\overline{k((x))}$

$$r = \delta - x^{-1/2} - \frac{\sqrt{-1}}{2}x^0 + (-\frac{27}{80} - \frac{3\sqrt{-1}}{40})x^{1/2} + (\frac{1587}{12800} + \frac{4141\sqrt{-1}}{12800})x^1 + \cdots$$

Write $R = \delta^2 + a_1\delta + a_0$ where $a_0, a_1 \in k((x))$ are to be determined. Dividing R by r results in a remainder of the form $a_0b_{0,0} + a_1b_{0,1} + b_{0,2} + x^{1/2}(a_0b_{1,0} + a_1b_{1,1} + b_{1,2})$ for some $b_{i,j} \in k((x))$. By equating this to zero, the following linear equations are obtained: $a_0b_{i,0} + a_1b_{i,1} + b_{i,2} = 0$, $i = 1, 2$. Solving these equations over $k((x))$ gives

$$\begin{aligned} R &= \delta^2 + \left((\frac{1}{2} - \sqrt{-1})x^0 + (-\frac{573}{6400} + \frac{3661\sqrt{-1}}{6400})x^1 + \cdots \right) \delta^1 + \\ & \left(-x^{-1} + (-\frac{2\sqrt{-1}}{5} - \frac{37}{40})x^0 + (-\frac{12291\sqrt{-1}}{64000} + \frac{48663}{64000})x^1 + \cdots \right) \delta^0. \end{aligned}$$

It is not efficient to compute many coefficients of a_0, a_1 in this way. It suffices to determine R in this way up to accuracy 2 (i.e. to determine the coefficient of x^0 in a_1 and the coefficient of x^{-1} in a_0). Then the higher terms can be computed more efficiently by the lift algorithm in section 2.4.

2.8 Formal solutions of differential equations

2.8.1 Solutions of semi-regular equations

Let $f \in k((x))[\delta]$ be a semi-regular operator of order $n \geq 1$. Then we can apply section 2.5 to factor $f = L(\delta - r)$ where r is an element of $\mathbb{Z} + x \cdot k[[x]]$. $S_r(f) = S_r(L)\delta$. We can recursively compute a fundamental system of solutions $a_1, \ldots, a_{n-1} \in k((x))[\log(x)]$ of $S_r(L)$. Define $s_i = \int \frac{a_i}{x} dx$ for $i = 1, \ldots, n-1$ and $s_n = 1$. Then $s_1, \ldots, s_n$ is a fundamental system of solutions of $S_r(f)$. These s_i are elements of $k((x))[\log(x)]$ because $a_i/x \in k((x))[\log(x)]$ and every element of $k((x))[\log(x)]$ has an anti-derivative in this ring. By requiring that the coefficients of $x^0\log(x)^0$ in $s_1, \ldots, s_{n-1}$ are 0 the s_i are uniquely defined. To obtain the solutions of f we multiply the solutions of $S_r(f)$ by $t = \mathrm{Exp}(r) = \exp(\int \frac{r}{x} dx)$. This $t \in k((x))$ can be computed efficiently as follows. If r is written as $m \in \mathbb{Z}$ plus an element of $x \cdot k[[x]]$ then t can be written as $x^m + t_{m+1}x^{m+1} + t_{m+2}x^{m+2} + \cdots$. The the fact that t is a solution of $\delta - r$ gives a linear equation for t_{m+1}, after solving it we find an equation for t_{m+2}, etcetera.

The same method can also be used for an element f of $L[\delta]$ which is semi-regular over L, where L is an algebraic extension of $k((x))$, for the same reason as in the remark on page 23. This way a uniquely defined basis of solutions $s_1, \ldots, s_n \in L[\log(x)]$ can be computed. By theorem 3 on page 34 (first apply the theorem to $k((x))[\delta]$, then generalize using the remark on page 23) it follows that f is semi-regular over L if and only if f has a fundamental system of solutions in $L[\log(x)]$.

2.8.2 The canonical basis of solutions

Let $e_1, \ldots, e_r \in E$ be representatives for the exponential parts of f. Computing e_i and the corresponding semi-regular parts R_{e_i} can be done by the algorithm in section 2.8.4. Note that the algorithm only computes the e_i up to conjugation over $k((x))$. This means that the formal solutions will also be computed up to conjugation over $k((x))$, i.e. if a number of solutions are conjugated then only one of them will be computed.

The semi-regular $R_{e_i} \in k((x))[e_i, \delta]$ has a basis of solutions $s_{i,j} \in k((x))[e_i, \log(x)]$. So according to section 2.6.1 we get a basis of solutions of the form

$$y = \mathrm{Exp}(e_i)s_{i,j} \quad \text{where} \quad e_i \in E \quad \text{and} \quad s_{i,j} \in k((x))[e_i, \log(x)] \tag{2.2}$$

(recall that $\mathrm{Exp}(e_i) \in V$ stands for $\exp(\int \frac{e_i}{x})$). In the LCLM factorization in lemma 5 the $S_{-e_i}(R_{e_i})$ are uniquely determined. Furthermore a unique basis of solutions for semi-regular operators was defined in the previous section. As a consequence, the basis of solutions obtained in this way is uniquely defined. We will call this basis the *canonical basis of solutions*.

For a solution in the form (2.2) $s_{i,j}$ is called the *semi-regular part* of (2.2) and e_i is called the *exponential part* of (2.2). The exponential part of (2.2) is an exponential part of the operator as well. The semi-regular part $s_{i,j}$ is a solution of the semi-regular part R_{e_i}. Note that from a given y in the form (2.2), e_i can be determined modulo $\sim$ (without further restrictions on $s_{i,j}$ one can not determine $e_i \in E$ from y because when replacing for example e_i by $e_i - 1$ and $s_{i,j}$ by $x \cdot s_{i,j}$ in y we obtain an equivalent expression).

A few introductory comments on the next section: Every $f \in \overline{k((x))}[\delta]$ is an element of some $L[\delta]$ where L is a finite extension of $k((x))$. By a suitable transformation $\theta_{a,d}$ as in the remark on page 23 the problem of finding solutions of f can be reduced to finding solutions of an operator $\theta_{a,d}(f) \in l((x))[\delta]$. The solutions of f can be obtained from the solutions of $\theta_{a,d}(f)$. But the elements of the basis of solutions that we find for f are not necessarily in the form (2.2) (in other words: are not necessarily an element of some V_e) but are element of some $\overline{V}_e$, definitions follow in the next section.

Example: $\delta - \sqrt{x}/(2 + 2\sqrt{x})$. Apply $\theta_{1,2}$ to obtain $\frac{1}{2}\delta - \frac{1}{2}x/(1+x)$. A basis for the solutions is $1 + x$. This is of the form (2.2) with $e = 0$. Now apply an inverse transformation to find the solution $1 + \sqrt{x}$ of f. This is not of the form (2.2) but it is a sum of two terms of the form (2.2), one with $e = 0$ and one with $e = 1/2$. This example shows that the direct sum decomposition $V(f) = \bigoplus V_e(f)$ in theorem 3 in the next section which holds for $f \in k((x))[\delta]$ need not hold for $f \in \overline{k((x))}[\delta]$. For $f \in \overline{k((x))}[\delta]$ a less precise statement is given in theorem 3, corresponding to the less precise version $\overline{\mu}$ of exponential parts.

2.8.3 The solution space and exponential parts

Definition 5 *Define for $e \in E$ the set*

$$\overline{V}_e = \mathrm{Exp}(e) \cdot \overline{k((x))}[\log(x)] \subset V$$

and

$$V_e = \mathrm{Exp}(e) \cdot \big((\overline{k} \cdot k((x))[e])[\log(x)]\big) \subset \overline{V}_e$$

If $e_1 \sim e_2$ then $V_{e_1} = V_{e_2}$ so V_e is also defined for $e \in E/\sim$. Similarly $\overline{V}_e$ is defined for $e \in E/\mathbb{Q}$. Define

$$V_e(f) = V_e \bigcap V(f) \quad \text{and} \quad \overline{V}_e(f) = \overline{V}_e \bigcap V(f).$$

Note that $\overline{k} \cdot k((x))[e] = \overline{k} \cdot k((x^{1/n}))$ where $n = \mathrm{ram}(e)$. The reason for writing $\overline{k} \cdot k((x^{1/n}))$ instead of $\overline{k}((x^{1/n}))$ is that in general (namely if $k \neq \overline{k}$) the field $\overline{k}((x^{1/n}))$ is not a subfield of $\overline{k((x))}$.

Theorem 3 *For non-zero $f \in k((x))[\delta]$*

$$V(f) = \bigoplus_e V_e(f) \quad \text{and} \quad \dim(V_e(f)) = \mu_e(f)$$

where the sum is taken over all $e \in E/\sim$. For non-zero $f \in \overline{k((x))}[\delta]$

$$V(f) = \bigoplus_e \overline{V}_e(f) \quad \text{and} \quad \dim(\overline{V}_e(f)) = \overline{\mu}_e(f)$$

where the sum is taken over all $e \in E/\mathbb{Q}$.

This theorem enables us to give an alternative definition of exponential parts and their multiplicities $\mu_e(f)$ in terms of the solution space of f.

Proof: Let $f \in k((x))[\delta]$. Each element of the basis of solutions in the previous section is an element of some V_e where e is an exponential part of f. So the sum of the $V_e \bigcap V(f)$ contains a complete basis of solutions of f. In this basis of solutions, $\mu_e(f)$ elements are in the form (2.2), i.e. $\mu_e(f)$ elements are in $V_e(f)$. Hence

$$V(f) = \sum_e V_e(f) \quad \text{and} \quad \dim(V_e(f)) \geq \mu_e(f)$$

where the sum is taken over all exponential parts of f. It follows from the following lemma 6 that this is a direct sum. Then $\mathrm{order}(f) = \dim(V(f)) = \sum_e \dim(V_e(f)) \geq \sum_e \mu_e(f) = \mathrm{order}(f)$ hence the $\geq$ must be an equality. The second statement follows in the same way.

□

Lemma 6

$$V = \bigoplus_{e \in E/\sim} V_e \qquad \text{and} \qquad V = \bigoplus_{\overline{e} \in E/\mathbb{Q}} \overline{V}_{\overline{e}}$$

Proof: Let $n \in \mathbb{N}$. Then $\overline{k((x))} = \bigoplus_q \mathrm{Exp}(q) \cdot (\overline{k} \cdot k((x^{1/n})))$ where the sum is taken over all $q \in \mathbb{Q}$ with $0 \leq q < 1/n$. So for $\overline{e} \in E/\mathbb{Q}$

$$\overline{V}_{\overline{e}} = \bigoplus_e V_e$$

where the sum is taken over all $e \in E/\sim$ such that $\overline{e} = e \bmod \mathbb{Q}$. This reduces the first direct sum to the second one. Because of the relations $\mathrm{Exp}(e_1)\mathrm{Exp}(e_2) = \mathrm{Exp}(e_1 + e_2)$ every element of V can be written as a polynomial in the $\mathrm{Exp}(e)$ of degree 1. So $V = \sum_{\overline{e}} \overline{V}_{\overline{e}}$. We will show that this is a direct sum which finishes the proof of this lemma.

Let $e_1, \ldots, e_d \in E$ be different modulo $\mathbb{Q}$. Let $s_i \in \overline{k((x))}[\log(x)]$ and $s = \sum_i \mathrm{Exp}(e_i)s_i = 0$. To prove that the sum is direct we need to show that all s_i

are zero. Assume that not all $s_i = 0$ and that $d > 1$ is minimal with this property. Then all $s_i \neq 0$. Now $x\frac{ds}{dx} = \sum_i \mathrm{Exp}(e_i)(e_i s_i + xs_i')$. Suppose the vectors $(s_1, \ldots, s_d)$ and $(e_1 s_1 + xs_1', \ldots, e_d s_d + xs_d')$ are linearly independent over $\overline{k((x))}(\log(x))$. Then we can find a linear combination in which at least one (but not all) of the components vanishes. This contradicts the fact that d is minimal (multiply with a suitable element of $\overline{k((x))}[\log(x)]$ to eliminate $\log(x)$ from the denominator). So these two vectors must be linearly dependent over $\overline{k((x))}(\log(x))$. It follows that

$$\frac{e_1 s_1 + xs_1'}{s_1} = \frac{e_2 s_2 + xs_2'}{s_2} \in \overline{k((x))}(\log(x))$$

so

$$e_2 - e_1 = xs_1'/s_1 - xs_2'/s_2 = xb'/b$$

where $b = s_1/s_2 \in \overline{k((x))}(\log(x))$. But $e_2 - e_1 \in E$ and $e_2 - e_1 \notin \mathbb{Q}$ which contradicts lemma 7.

$\square$

Lemma 7 *Let $b \in k((x^{1/n}))(\log(x))$. Suppose that the logarithmic derivative $c = xb'/b$ is an element of $\overline{k((x))}$. Then $c \in \frac{1}{n}\mathbb{Z} + x^{1/n} \cdot k[[x^{1/n}]]$.*

Proof: Write $b = p/q$ with $p, q \in k((x^{1/n}))[\log(x)]$. Write $p = p_l \log(x)^l + \cdots$ and $q = q_m \log(x)^m + \cdots$ where $p_l, q_m \in k((x^{1/n}))$. The dots stands for an element of $k((x^{1/n}))[\log(x)]$ of lower degree as a polynomial in $\log(x)$.

$$c = \frac{xb'}{b} = \frac{xp'}{p} - \frac{xq'}{q} = \frac{xp_l' \log(x)^l + \cdots}{p_l \log(x)^l + \cdots} - \frac{xq_m' \log(x)^m + \cdots}{q_m \log(x)^m + \cdots}$$

$$= \frac{x(p_l' q_m - q_m' p_l)\log(x)^{l+m} + \cdots}{p_l q_m \log(x)^{l+m} + \cdots} \in \overline{k((x))}.$$

Then $x(p_l' q_m - q_m' p_l)/(p_l q_m)$ must be the same element c of $\overline{k((x))}$. Write $r = p_l/q_m \in k((x^{1/n}))$. Then $c = x(p_l' q_m - q_m' p_l)/(p_l q_m) = xr'/r \in \frac{1}{n}\mathbb{Z} + x^{1/n} \cdot \overline{k}[[x^{1/n}]]$.

$\square$

2.8.4 Coprime index 1 LCLM factorization

Lemma 8 *Let $f_1, \ldots, f_d \in k((x))[\delta]$, $e \in E/\sim$ and $f = \mathrm{LCLM}(f_1, \ldots, f_d)$. Then*

$$\max_i \mu_e(f_i) \leq \mu_e(f) \leq \sum_i \mu_e(f_i).$$

In particular every exponential part e of f is an exponential part of at least one of the f_i.

Proof: These inequalities follow from the dimensions of $V_e(f)$ and $V_e(f_i)$ in the following equation: $V_e(f) = V_e \bigcap (\sum_i V(f_i)) = \sum_i V_e(f_i)$. The second equality holds because the $V(f_i)$ are direct sums of $V(f_i) \bigcap V_{e_1}$ taken over all $e_1 \in E/\sim$.

□

Lemma 9 *Let $f \in k((x))[\delta]$ be monic and let $f_1, \ldots, f_d \in k((x))[\delta]$ be right hand factors of f. Suppose that $\sum_i \mathrm{order}(f_i) = \mathrm{order}(f)$ and that the f_i have no exponential parts in common. Then*

- $f = \mathrm{LCLM}(f_1, \ldots, f_d)$
- *If $e \in E/\sim$ and $\mu_e(f) > 0$ then here is precisely one f_i such that $V_e(f) \subset V(f_i)$.*
- *For this e and f_i the semi-regular part R_e of f is the semi-regular part of f_i as well.*

Proof: Using the previous lemma, the fact that the f_i have no exponential part in common and theorem 1 we can conclude that $\mathrm{order}(\mathrm{LCLM}(f_1, \ldots, f_d)) = \sum \mathrm{order}(f_i)$, and this equals $\mathrm{order}(f)$ by the assumption in this lemma. Since all f_i, and hence this LCLM, are right-hand factors of f the first statement follows. If e is an exponential part of f then for precisely one i we have $\mu_e(f_i) > 0$. Then $\mu_e(f_i) = \mu_e(f)$ because of the previous lemma and because the μ_e of the other f_j are zero. For the second statement note that $V_e(f_i) \subset V_e(f)$, because f_i is a right-hand factor of f. Since $\mu_e(f_i) = \mu_e(f)$ the dimensions are the same. Hence $V_e(f) = V_e(f_i) \subset V(f_i)$. The third statement follows because $V(S_{-e}(R_e)) = V_e(f) \subset V(f_i)$, hence $S_{-e}(R_e)$ is a right-hand factor of f_i and so R_e is a right-hand factor of $S_e(f_i)$.

□

Lemma 10 *Let $f, g \in k((x))[\delta]$ and suppose $\gcd(N_s(f), N_s(g)) = 1$ holds for all $s \in \mathbb{Q}$, $s > 0$. Suppose $\gcd(N_s(f), S_{T=T+n}(N_s(g))) = 1$ holds for $s = 0$ and all $n \in \mathbb{Z}$. Then f and g have no exponential parts in common.*

Proof: For every exponential part e of f there exists a Riccati solution r_e of f such that e is the principal part of r_e modulo $\sim$, cf. section 2.6.2. Now the proof follows from the next lemma.

□

Lemma 11 *Let $r \in \overline{k((x))}$ be a Riccati solution of $f \in k((x))[\delta]$. Suppose r, viewed as an element of $\bigcup_n \overline{k}((x^{1/n}))$, can be written as $r_s x^s$ plus higher order terms, where $s \in \mathbb{Q}$, $s \leq 0$ and $r_s \neq 0$ if $s < 0$. Write $s = n/d$ with $n, d \in \mathbb{Z}$, $\gcd(n, d) = 1$ and $d > 0$. Then $-s$ is a slope of f and r_s^d is a root of the Newton polynomial $N_{-s}(f)$.*

Proof: $\delta - r$ is a right-hand factor of f. If the ramification index of r is 1 the lemma can easily be proved using the fact that the slopes of factors of f are slopes of f and the Newton polynomials of right factors of f are factors of the Newton polynomials of f, cf. section 2.3.4. However, we have not defined the Newton polygon and Newton polynomial over ramifications of $k((x))$. Choose $d' \in \mathbb{N}$ such that $\theta_{1,d'}(\delta - r) \in \overline{k}((x))[\delta]$. Then d must divide d'. Now $\theta_{1,d'}(\delta - r)$ is a right-hand factor of $\theta_{1,d'}(f)$. The slope of $\theta_{1,d'}(\delta - r)$ is $-sd'$ so $\theta_{1,d'}(f)$ has this slope as well. Hence f has a slope $-s$. The Newton polynomial of $\theta_{1,d'}(\delta - r)$ is $\frac{1}{d'}T - r_s$. If $N_{-s}(f) = c(T^p + a_{p-1}T^{p-1} + \cdots + a_0 T^0)$ where c is a constant then $N_{-sd'}(\theta_{1,d'}(f))$ is a constant times $T^{pd} + d'^d a_{p-1} T^{(p-1)d} + \cdots + d'^{pd} a_0 T^0$. So $\frac{1}{d'}T - r_s$ is a factor of this Newton polynomial hence r_s^d is a root of $T^p + a_{p-1}T^{p-1} + \cdots + a_0 T^0$.

□

Now we can write *algorithm LCLM factorization* as follows. Take algorithm Coprime Index 1 Factorizations in section 2.5. Replace the lines

if $s = 0$ **then**
$M := \{g_1, \ldots, g_r\}$
$N := M \setminus \{g | g(T) = h(T+i), h \in M, i \in \mathbb{N}, i > 0\}$
else

by the lines

if $s = 0$ **then**
$M := \{g_1, \ldots, g_r\}$
$M' := M \setminus \{g | g(T) = h(T+i), h \in M, i \in \mathbb{N}, i > 0\}$
$M'' := \{\{n | \exists_{i \in \mathbb{Z}} g_n(T+i) = h\} | h \in M'\}$
$N := \{\prod_{i \in h} g_i^{e_i} | h \in M''\}$
else

The resulting algorithm produces a number of factorizations. The sum of the orders of the right factors is equal to the order of f. The different right factors $f_1, \ldots, f_d$ have no exponential parts in common because of lemma 10. Hence $f = \mathrm{LCLM}(f_1, \ldots, f_d)$. This variant on the algorithm in section 2.5 produces an *LCLM factorization*, i.e. it produces a number of right-hand factors $f_1, \ldots, f_d$ such that $f = \mathrm{LCLM}(f_1, \ldots, f_d)$. The orders of the f_i need not be minimal because we only apply the "easy" (i.e. coprime index 1) factorization method.

Algorithm semi-regular parts:
Input: $f \in k((x))[\delta]$
Output: representatives $e_1, \ldots, e_d \in E$ for all exponential parts up to conjugation over $k((x))$ and the corresponding semi-regular parts $R_{e_i} \in k((x))[e_i, \delta]$.

1. Same as case 1 in Algorithm Riccati solution. This is also a special case of case 6 below after a suitable substitution map S_e.

2. If algorithm LCLM factorization produces a non-trivial (i.e. $d > 1$) LCLM factorization $f = \mathrm{LCLM}(f_1, \ldots, f_d)$ then apply recursion to the right factors $f_1, \ldots, f_d$.

3. If the condition of case 3 in Algorithm Riccati solution holds, and furthermore the slope of f is non-zero, then proceed as in case 3 in Algorithm Riccati solution; apply recursion to the right-hand factor.

4. Same as case 4 in Algorithm Riccati solution, apply recursion to $S_{cx^{-s}}(f)$.

5. Same as case 5 in Algorithm Riccati solution, apply recursion on R.

6. If f has one slope $s = 0$ and the Newton polynomial has the following form $N_s(f) = g \cdot S_{T=T+i_1}(g) \cdots S_{T=T+i_n}(g)$ where $n \geq 0$ and i_j are integers, and g is an irreducible polynomial. Let $r \in \overline{k}$ be a root of g. Extend the field

k with r (note that g can have degree 1 in which case $r \in k$). Define $h = T \cdot (T + i_1) \cdots (T + i_n)$. This is the largest factor of $N_0(S_r(f))$ which has only integer roots. Now use a coprime index 1 factorization (cf. Algorithm Coprime Index 1 Factorizations in section 2.5) to compute a right factor R of $S_r(f)$ that has Newton polynomial h.

The right-hand factors R that this algorithm produces in case 6 are the semi-regular parts of f (actually such R is an image of a semi-regular part under certain maps $\theta_{a,d}$ that were used in case 5). The corresponding exponential parts are obtained by keeping track of the substitution maps S_e and ramification maps $\theta_{a,d}$ that were performed. The recursion in case 2 of the algorithm is valid because of lemma 9.

In the cases 3 and 5 of the algorithm a field extension over $k((x))$ is applied (also in case 6 if degree$(g) > 1$ but the argument is almost the same for this case). Suppose the degree of the of this field extension is d. Then the algorithm computes a right factor f_1 of f and uses recursion on this right factor. Let $f_1, \ldots, f_d \in L[\delta]$ be the conjugates of f_1 over $k((x))$ where L is some finite extension of $k((x))$. Lemma 10 and lemma 9 were formulated for $k((x))[\delta]$ instead of $L[\delta]$, but they are still applicable when using the less precise notion of exponential parts $\overline{\mu}$. We must replace the condition "for all $n \in \mathbb{Z}$" by "for all $n \in \mathbb{Q}$" in lemma 10 in order for this lemma to hold for the case of $\overline{\mu}$ instead of μ. So our algorithm would produce all exponential parts and semi-regular parts if we would use recursion on not only f_1 but also on $f_2, \ldots, f_d$. However, this could introduce very large algebraic field extensions (worst case d factorial) which could make the algorithm too slow to be useful. If we would use recursion on $f_2, \ldots, f_d$ we will only find conjugates of the exponential parts and semi-regular parts that are obtained from f_1. So there is no need to do the recursion on $f_2, \ldots, f_d$ because the result of that computation can also be obtained as the conjugates (which are not computed, however) of the output of the recursion on f_1.

Algorithm formal solutions:
Input: $f \in k((x))[\delta]$
Output: a basis of solutions, up to conjugation over $k((x))$
Step 1: this is the main step: apply algorithm semi-regular parts.
Step 2: compute the solutions $s_{i,j}$ of R_{e_i} as in section 2.8.1.
Step 3: Return the set of $\mathrm{Exp}(e_i)s_{i,j}$.

Our method for computing formal solutions can not avoid the use of field extensions over $k((x))$ because these field extensions appear in the output. It does, however, delay the use of algebraic extensions as long as possible. The use of algorithm LCLM factorization reduces the problem of finding solutions to subproblems for operators of smaller order. This way the order of the operator is as small as possible at the moment that an algebraic extension is introduced, and so the amount of computation in algebraic extensions is minimized. Lazy evaluation is used to minimize the number of operations in the constants field.

2.9 A characterization of the solution spaces

The symbol $\log(x)$ is viewed as an element of a differential extension of $k((x))$ which satisfies the equation $y' = 1/x$. The corresponding linear differential equation is $y'' + \frac{1}{x}y' = 0$. We do not view $\log(x)$ as a function on an open subset of the complex plane, but as a formal expression which is defined by the property that the derivative is $1/x$. From this viewpoint it is clear that the $\overline{k((x))}$-homomorphism

$$S_{\log} : \overline{k((x))}[\log(x)] \to \overline{k((x))}[\log(x)]$$

defined by $S_{\log}(\log(x)) = \log(x)+1$ is a differential automorphism, because the derivative of $\log(x) + 1$ is also $1/x$, and hence all differential properties of $\log(x) + 1$ and $\log(x)$ are the same. This automorphism can be extended to the ring V by defining $S_{\log}(\mathrm{Exp}(e)) = \mathrm{Exp}(e)$. If $f \in V[\delta]$ and $y \in V$ is a solution of f then $S_{\log}(y)$ is a solution of $S_{\log}(f)$. Note that the differential Galois group G of the Picard-Vessiot extension $\overline{k((x))} \subset \overline{k((x))}(\log(x))$ contains more elements than just $S_{\log}$. However, we will see that it is sufficient to consider only $S_{\log}$. This is explained from the fact that G is equal to the Zariski closure of the group generated by $S_{\log}$.

Let $f \in k((x))[\delta]$. The questions of this section are: what are the possible right-hand factors of f in $k((x))[\delta]$, or in $\overline{k((x))}[\delta]$, what are the semi-regular and regular right factors. Every right factor R corresponds to a subspace of solutions $V(R) \subset V(f)$. But not every linear subspace $W \subset V(f)$ corresponds to a right factor of f because we do not look for right factors in $V[\delta]$ but only in smaller rings like $k((x))[\delta]$. So the question now is the following. Given a finite dimensional $\overline{k}$ vector space $W \subset V$, when is W the solution space of either

1. a semi-regular operator in $k((x))[\delta]$
2. a regular operator in $k((x))[\delta]$
3. any operator in $\overline{k((x))}[\delta]$
4. any operator in $k((x))[\delta]$.

Example: Let $\log(x)$ be a basis of W. Now there can not be any $f \in \overline{k((x))}[\delta]$ such that $W = V(f)$. Because then $S_{\log}(\log(x))$ would be a solution of $S_{\log}(f) = f$. So f has $\log(x)$ and $S_{\log}(\log(x)) - \log(x) = 1$ as solutions. Hence the dimension of $V(f)$ is at least 2.

Lemma 12 *Let W be a n dimensional $\overline{k}$ subspace of V. Then $W = V(f)$ for some semi-regular $f \in k((x))[\delta]$ if and only W has a basis $b_1, \ldots, b_n \in k((x))[\log(x)]$ and $S_{\log}(W) = W$.*

Proof: Let $f \in k((x))[\delta]$ be semi-regular. Then it follows from section 2.8.1 that $V(f)$ has a basis of solutions in $k((x))[\log(x)]$. Furthermore $S_{\log}(V(f)) = V(S_{\log}(f)) = V(f)$.

Now suppose $S_{\log}(W) = W$ and suppose $b_1, \ldots, b_n \in k((x))[\log(x)]$ is a basis of W as a $\overline{k}$ vector space. We want to construct a semi-regular operator f such that $V(f) = W$. Let b be an element of W of minimal degree d as a polynomial in $\log(x)$. Suppose $d > 0$. Then $S_{\log}(b) - b \in W$ has degree $d-1$ which contradicts the minimality of d. Hence $d = 0$, so b is an element of $\overline{k} \cdot k((x))$. Then $b \in l \cdot k((x))$ where l is some finite extension of k. After multiplication by a constant we may assume that one of the coefficients of b is 1. Then, by taking the trace over the field extension $k \subset l$, we may assume $b \in k((x))$ and $b \in W$ (use here that W has a basis of elements in $k((x))[\log(x)]$, hence the trace over k of an element $b \in W$ is an element of W). Now $b \neq 0$ because the trace of the coefficient 1 is not 0. Because $b \in V(f)$ for the operator f that we want to construct it follows that $R = \delta - xb'/b$ must be a right factor of f. This operator R is a $\overline{k}$ linear map from V to V. The kernel is the solution space of R. It has dimension 1. Because the kernel is a subspace of W it follows that $\dim(R(W)) = n - 1$. It is easy to check that $R(W)$ satisfies the conditions of this lemma, hence by induction there is a semi-regular operator $L \in k((x))[\delta]$ such that $V(L) = R(W)$. Now define $f = LR$. This is a semi-regular operator in $k((x))[\delta]$ because $L, R \in k((x))[\delta]$ are semi-regular. $f(W) = L(R(W)) = \{0\}$ and $\dim(W) = \mathrm{order}(f)$ so $V(f) = W$.

□

From the remark on page 23 it follows that the lemma is also valid when $k((x))$ is replaced by a finite extension L of $k((x))$.

Lemma 13 *Let W be a n dimensional $\overline{k}$ subspace of V. Then $W = V(f)$ for some regular $f \in k((x))[\delta]$ if and only W has a basis $b_1, \ldots, b_n \in k[[x]]$ and all non-zero elements of W have valuation $< n$.*

Proof: If $f \in k((x))[\delta]$ is regular it is known by the Cauchy theorem that there exists a basis $b_1, \ldots, b_n \in k[[x]]$ of solutions such that b_i is x^{i-1} modulo x^n. It is easy to compute these b_i as follows. The equation $f(b_i) = 0$ (writing f as an element of $k[[x]][\partial]$ is more convenient for this) gives a linear equation in the coefficient of x^n in b_i, a linear equation for the coefficient of x^{n+1}, etcetera. From these equations the coefficients of b_i can be computed.

To prove the reverse statement let $b_1, \ldots, b_n \in k[[x]]$ be a basis of W and suppose that all non-zero elements of W have valuation (i.e. the smallest exponent of x which has a non-zero coefficient) smaller than n. Then, after a basis transformation, we may assume that b_i is x^{i-1} modulo x^n. Now define $R_1 \in k[[x]][\partial]$ as $R_1 = \partial - b_1'/b_1$. Define for $1 \leq d < n$ the operator $R_{d+1} \in k[[x]][\partial]$ as follows: define $y_{d+1} = R_d(b_{d+1})$. Note that $v(R_i(b_{d+1})) = d - i$ for $1 \leq i \leq d$. So $v(y_{d+1}) = 0$ and hence $\partial - y_{d+1}'/y_{d+1} \in k[[x]][\partial]$. Now define $R_{d+1} = (\partial - y_{d+1}'/y_{d+1})R_d$. Now $f = R_n$ is a monic element of $k[[x]][\partial]$, hence regular, with $V(f) = W$.

□

From the lemma we see that right factors of regular operators need not be regular. Suppose for example that $1, x, x^2$ is a basis of solutions of f. Then the right-hand factor given by the basis of solutions $1, x^2$ is not regular. But the right factor with the basis $1, x + x^2$ is regular. An LCLM of regular operators is not necessarily regular either. For certain purposes (not for all) semi-regular is a more convenient notion than regular because factors, products, LCLM's and symmetric products of semi-regular operators are semi-regular.

If $W \subset V$ is a solution space of a differential operator $f \in \overline{k((x))}[\delta]$ then $W = \bigoplus_{\overline{e}} (W \bigcap V_{\overline{e}})$ because of theorem 3. Furthermore $S_{\log}(W)$ must equal W because f is invariant under $S_{\log}$. This proves one part of the following lemma.

Lemma 14 *Let W be a finite dimensional $\overline{k}$ subspace of V. Then $W = V(f)$ for some $f \in \overline{k((x))}[\delta]$ if and only $W = \bigoplus_{\overline{e}}(W \bigcap \overline{V}_{\overline{e}}) = S_{\log}(W)$ where the sum is taken over all $\overline{e} \in E/\mathbb{Q}$.*

Proof: Assume $W \neq \{0\}$ is finite dimensional and $W = \bigoplus_{\overline{e}}(W \bigcap \overline{V}_{\overline{e}}) = S_{\log}(W)$. Let $e \in E$ such that $W_e = W \bigcap \overline{V}_e \neq \{0\}$. Note that $S_{\log}(\overline{V}_e) = \overline{V}_e$ hence W_e is invariant under $S_{\log}$. W_e has a basis of the form $\mathrm{Exp}(e) \cdot s_i$, $i = 1, \ldots, t$ where $s_i \in \overline{k((x))}[\log(x)]$ so $s_i \in L[\log(x)]$ for some finite extension L of $k((x))$. Using lemma 12 it follows that there exists an operator $R_e \in L[\delta]$ which has s_i, $i = 1, \ldots, t$ as a basis of solutions. So $S_{-e}(R_e)$ has $\mathrm{Exp}(e)s_i$, $i = 1, \ldots, t$ as a basis of solutions and so $S_{-e}(R_e)$ must be a right-hand factor of the operator f that we want to construct. Choose a representative $e \in E$ for every $\overline{e} \in E/\mathbb{Q}$ for which $W \bigcap \overline{V}_{\overline{e}} \neq \{0\}$. Construct the corresponding $S_{-e}(R_e)$ and define f as the LCLM of these $S_{-e}(R_e)$. Then $V(f) = W$.

□

Lemma 15 *Let W be a finite dimensional $\overline{k}$ subspace of V. Then $W = V(f)$ for some $f \in k((x))[\delta]$ if and only the conditions of the previous lemma hold, and furthermore W is invariant under the action of the Galois group of the algebraic extension $k((x)) \subset \overline{k((x))}$.*

Proof: if τ is a $k((x))$ automorphism of $\overline{k((x))}$ then τ can be extended to V by setting $\tau(\log(x)) = \log(x)$ and $\tau(\mathrm{Exp}(e)) = \mathrm{Exp}(\tau(e))$. Now for any $f \in \overline{k((x))}[\delta]$ we have $V(\tau(f)) = \tau(V(f))$ because conjugation commutes with differentiation. So if $f \in k((x))[\delta]$ then $V(f) = \tau(V(f))$ which proves one part of the lemma. Now suppose $W = V(f)$ for some monic $f \in \overline{k((x))}[\delta]$ and suppose that $W = \tau(W)$. Now $\mathrm{order}(f - \tau(f)) < \mathrm{order}(f)$ and $W \subset V(f - \tau(f))$ so $\dim(V(f - \tau(f))) > \mathrm{order}(f - \tau(f))$ and hence $f - \tau(f)$ must be 0. So if W is invariant under the Galois group of the algebraic extension $k((x)) \subset \overline{k((x))}$ then f is invariant as well, hence $f \in k((x))[\delta]$.

□

Every $y \in V$ is a finite sum $y = \sum_e b_e$ with $b_e \in V_e$. Define W as the closure under Galois actions and under $S_{\log}$ of the set $\sum_e \overline{k} \cdot b_e$. Now W satisfies the conditions of the previous lemma, hence for every $y \in V$ there is a $g \in k((x))[\delta] \setminus \{0\}$ such that $y \in V(g)$. From this it follows that for any non-zero $f \in k((x))[\delta]$ the map $f : V \to V$ is surjective. This is seen as follows. If the kernel of g is not contained in the image of f then the dimension of the kernel of gf would be smaller than the sum of the dimensions of the kernels of g and f. In other words, $\mathrm{order}(gf) < \mathrm{order}(g) + \mathrm{order}(f)$ which is a contradiction. Hence $V(g) \subset f(V)$ for every g and so f is surjective, $f(V) = V$.

Chapter 3

Factorization of Differential Operators with Rational Functions Coefficients

In this chapter we will give a new efficient method for factorizing differential operators with rational functions coefficients. This method solves the main problem in Beke's factorization method, which is the use of splitting fields and/or Gröbner basis.

3.1 Introduction

A differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$$

corresponds to a differential operator

$$f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$$

acting on y. In this chapter the coefficients a_i are elements of the differential field $k(x)$ and ∂ is the differentiation d/dx. The field k is the field of constants. It is assumed to have characteristic 0. $\overline{k}$ is the algebraic closure of k. The differential operator f is an element of the non-commutative ring $k(x)[\partial]$. This is an example of an Ore ring [40]. A factorization $f = LR$ where $L, R \in \overline{k}(x)[\partial]$ is useful for computing solutions of f because solutions of the right-hand factor R are solutions of f as well.

The topic in this chapter is factorization in the ring $\overline{k}(x)[\partial]$. Multiplication in $\overline{k}(x)[\partial]$ is not commutative. However, some properties of are independent of the order of the multiplication, for example the Newton polygons of fg and gf at a point p are the same. The non-commutativity is one of the reasons that factorization in $\overline{k}(x)[\partial]$ is difficult. To handle this difficulty we will extract the *commutative part* $\mu_*(f)$ of an operator f. We will first try to find properties of differential operators which do not depend on the order of multiplication and then we will define the commutative part of f as the collection of these properties that we found. For this purpose we will first define *exponential parts* and their multiplicities for local differential operators in section 3.3. Then $\mu_*(f)$ will be defined as the collection of all exponential parts and their multiplicities at all singularities of f.

Let $f = LR$ where $f \in k(x)[\partial]$ is given and where $L, R \in \overline{k}(x)[\partial]$ is a factorization that we want to compute. The commutative part μ_* has the following property

$$\mu_*(f) = \mu_*(L) + \mu_*(R).$$

This equation leaves only a finite number of possibilities for $\mu_*(R)$. Beke's method (cf. [6] and also section 3.4) for computing first order right-hand factors R of f can be explained in terms of μ_* as follows. Try all possible $\mu_*(R)$ and for each $\mu_*(R)$ the problem of finding R is reduced to computing the rational solutions of a certain differential operator. Computing rational solutions of a differential operator can be done quickly (cf. [1]) but the number of possible $\mu_*(R)$ one needs to check depends exponentially (worst case) on the number of singularities. So Beke's method performs well on examples with few singularities, but for operators with many singularities "try all possibilities" is not a good answer to the question which $\mu_*(R)$ need to be considered. Furthermore this method involves computing in algebraic extensions over k which can be of exponentially large degree. Most previous factorization algorithms (except [47]) are based on Beke's algorithm for computing first order factors, and use the exterior power method for computing higher order factors.

This chapter is organized as follows:

- Sections 3.5 and 3.6 contain the main result of this chapter: An algorithm, that does not use computations with exponentially large algebraic extensions nor Gröbner bases, for factorizing differential operators. This algorithm can produce (first order or higher order) factors, or irreducibility proofs, for a certain class (specified in section 3.5) of differential operators. However, not every operator is in this class, so not every operator can be handled. It even need not compute all first order factors.

- Section 3.7. A supplemental algorithm, that makes our algorithm complete for first order right-hand factors.

- Section 3.8. The exterior power method. This is another supplemental algorithm, obtained from the literature, to make the algorithm complete for higher order factors. The exterior power method is not efficient; only small operators (low order and small coefficients) can be handled this way. So we want to avoid it whenever possible.

- Section 3.4. Beke's algorithm for computing factors of order 1, reformulated in our terminology.

In section 3.7 we use the algorithm of sections 3.5 and 3.6 to compute a set S with at most order(f) elements such that $\mu_*(R) \in S$ for all first order right-hand factors R. When such an S is computed, the problem of computing all first order right-hand factors is practically solved because the number of possibilities that need to be checked is now linear instead of exponential like in Beke's algorithm, and the algebraic extensions that we need to work with are of much lower degree than in Beke's algorithm. As already mentioned, Beke's algorithm, section 3.4, sometimes performs well but it can also be extremely slow if there are many singularities. For such cases the algorithm obtained by combining sections 3.5, 3.6 and 3.7 is an good alternative.

Computing left-hand factors and computing right-hand factors are equivalent problems. They can be reduced to each other by applying the adjoint. The adjoint is a $\overline{k}(x)$-anti-automorphism of $\overline{k}(x)[\partial]$ given by $\partial \mapsto -\partial$. It interchanges the role of left and right. Using the adjoint and the algorithm in sections 3.5, 3.6 and 3.7 we can compute all first order left and right-hand factors so every operator of order ≤ 3 can either be factored or proven to be irreducible. The method given sections 3.5 and 3.6 can also compute higher order factors (or to produce irreducibility proofs) for many (see section 3.5 for a more precise description) operators of order > 3. Tests show that this method can handle large examples; operators in $\mathbb{Q}(x)[\partial]$ of order > 10 with > 10 singularities are often still feasible if the bound that is computed in section 3.9.1 is not too high. This would be impossible with previous factorization algorithms that use the exterior power method for computing higher order factors; computing exterior powers of such large operators will cause the computer to run out of memory. Note that in a few cases, namely the operators which do not belong in the class specified in section 3.5, we have to use the exterior power method as well, in which case factorizing operators of order 10 is impossible as well.

If the bound in section 3.9.1 is very high then even small operators are hard to factor. We can not hope to solve this problem; for example the factorization of $\partial^2 - \frac{1}{n}\partial + \frac{n}{x}$ with $n = 10^{10}$ is not feasible no matter which method we use because the result will not fit in any existing computer.

3.2 Preliminaries

The reader is assumed to be familiar with sections 3, 6 and 8 (except for the algorithm) of chapter 2. From section 3 the preliminaries (note that these are found elsewhere as well, references are given in chapter 2): Newton polygon/polynomial, differential field, Ore ring, the ring $k((x))[\delta]$ where $\delta = x\partial$, LCLM (Least Common Left Multiple), algebraic extensions of $k((x))$ and the universal extension. From section 6: exponential parts and from section 8 the relation between exponential parts and formal solutions. In the next section we will give a different introduction to exponential parts which is hopefully easier to understand than section 6 in chapter 2.

We assume that the characteristic of the constants field k is 0. If $f \in k(x)[\partial]$ then f has finitely many coefficients in $k(x)$ and each of these coefficients has finitely many coefficients in k. So without loss of generality we can restrict ourselves to a coefficients field k and a differential operator $f \in k(x)[\partial]$ where k is finitely generated over $\mathbb{Q}$.

3.3 Exponential parts of local differential operators

This section gives a short introduction of exponential parts. For proofs of the statements in this section see chapter 2. The notations are the same as in chapter 2.

3.3.1 A description in terms of the solution space

Let V be the universal extension (called R in lemma 2.1.1 in [24]) of $\overline{k((x))}$. This is a differential ring extension of $\overline{k((x))}$ consisting of all solutions of all $f \in k((x))[\delta]$.

Let $f \in k((x))[\delta] \setminus \{0\}$ be a differential operator. The action of f defines a $\overline{k}$-linear surjective (cf. page 41) map

$$f : V \to V.$$

The kernel of this map, denoted as $V(f)$, is the solution space of f. V contains all solutions of f. Hence the dimension of the kernel of f on V is maximal

$$\mathrm{order}(f) = \dim(V(f)).$$

This number $\dim(V(f))$ is useful for factorization because it is independent of the order of the multiplication, i.e. $\dim(V(fg)) = \dim(V(gf))$. To obtain more of such useful numbers we will split $V(f)$ in a direct sum and look at the dimensions of the components (V_e, E and $\sim$ are defined in chapter 2, and are described below as well)

$$V = \bigoplus_{e \in E/\sim} V_e.$$

The V_e are $\overline{k}$-vector spaces and also $k((x))[\delta]$-modules. So $f(V_e) \subset V_e$ for all $f \in k((x))[\delta] \setminus \{0\}$. Then $f(V_e) = V_e$ because f is surjective on V. The kernel of f on V_e is denoted by $V_e(f) = V(f) \bigcap V_e$. Denote

$$\mu_e(f) = \dim(V_e(f)).$$

This is consistent with the definition of $\mu_e(f)$ in chapter 2 because of theorem 3 on page 34. These μ_e are useful for factorization because they are independent of the order of the multiplication, i.e. if $f, g \in k((x))[\delta] \setminus \{0\}$ then

$$\mu_e(gf) = \mu_e(fg) = \mu_e(f) + \mu_e(g).$$

This equation is lemma 4 in chapter 2. It also follows from the fact that the dimension of the kernel of the composition of two surjective linear maps equals the sum of the dimensions of the kernels.

Recall the following definitions from chapter 2. These definitions were done in such a way that the subspaces V_e of V are as small as possible (more precisely: V_e is an indecomposable $\overline{k} \cdot k((x))[\delta]$-module) because then the integers $\mu_e(f)$ give as much as possible information about f. Denote the set

$$E = \bigcup_n \overline{k}[x^{-1/n}]$$

and the map

$$\mathrm{Exp} : E \to V$$

as $\mathrm{Exp}(e) = \exp(\int \frac{e}{x} dx)$. To define $\mathrm{Exp}(e)$ without ambiguity one can use the construction of the universal extension (briefly described in section 2.3.2, the proof of this construction is found in [24]). Then $\mathrm{Exp}(e_1 + e_2) = \mathrm{Exp}(e_1)\mathrm{Exp}(e_2)$ so Exp behaves like an exponential function. For rational numbers q we have $\mathrm{Exp}(q) = x^q \in \overline{k((x))}$. Denote (see also page 33)

$$V_e = \mathrm{Exp}(e) \cdot (\overline{k} \cdot k((x))[e])[\log(x)] \subset V.$$

Note that $\overline{k} \cdot k((x))[e] = \overline{k} \cdot k((x^{1/n}))$ where n is the ramification index of e. Define $\sim$ on E as follows: $e_1 \sim e_2$ if and only if $e_1 - e_2$ is an integer divided by the ramification index of e_1. $V_{e_1} = V_{e_2}$ if and only if $e_1 \sim e_2$ so V_e is defined for $e \in E/\sim$. Hence $\mu_e(f)$ is defined for $e \in E/\sim$ as well.

$$V(f) = \bigoplus_{e \in E/\sim} V_e(f)$$

An element $e \in E/\sim$ is called an *exponential part* of f if $\mu_e(f) > 0$. The number $\mu_e(f) = \dim(V_e(f))$ is called the *multiplicity* of e in f. The sum of the multiplicities of all exponential parts of f equals the order of f.

3.3.2 Exponential parts and semi-regular parts

We now give the definition of $\mu_e(f)$ as it appears in chapter 2. Let $e \in \overline{k((x))}$. Then the *substitution map*

$$S_e : \overline{k((x))}[\delta] \to \overline{k((x))}[\delta]$$

is the $\overline{k((x))}$-automorphism given by

$$S_e(\delta) = \delta + e.$$

The following gives the relation between the solution spaces

$$\mathrm{Exp}(e) \cdot V(S_e(f)) = V(f).$$

Let $f \in k((x))[\delta] \setminus \{0\}$ and $e \in E$. Let n be the ramification index of e. Let $P = N_0(S_e(f))$ be the Newton polynomial corresponding to slope 0 in the Newton polygon of $S_e(f) \in \overline{k}((x^{1/n}))[\delta]$. Now $\mu_e(f)$ is defined as the number of roots (counted with multiplicity) of P in $\frac{1}{n}\mathbb{Z}$. If $e_1 \sim e_2$ then $\mu_{e_1}(f) = \mu_{e_2}(f)$ for all $f \in k((x))[\delta] \backslash \{0\}$ hence $\mu_e(f)$ is defined for $e \in E/\sim$ as well.

Let L be a finite algebraic extension of $k((x))$ and let $f \in L[\delta]$. Then f is called *semi-regular* over L if f has a fundamental system of solutions in $L[\log(x)]$. According to chapter 2 this is equivalent with the following two conditions

- f is regular singular
- The roots of the Newton polynomial $N_0(f)$ are integers divided by the ramification index of L over $k((x))$.

Note that the definition of semi-regular depends on the field L. For $f \in k((x))[\delta]$ we have $\mu_0(f) = \mathrm{order}(f)$ if and only if all solutions of f are elements of $V_0 = \overline{k} \cdot k((x))[\log(x)]$ if and only if f is semi-regular over $k((x))$. A regular operator is semi-regular as well.

Semi-regular operators are "easy" differential operators. It is easy to compute the formal solutions (cf. chapter 2) for such operators. One of the benefits of exponential parts and semi-regular parts is that we can use them to split up a "difficult" differential operator f as an LCLM of "easier" parts. More precisely: an operator f can be written as an LCLM of operators which are of the form $S_{-e}(R_e)$ for some $e \in E$ and semi-regular $R_e \in k((x))[e, \delta]$.

Let $e \in E$, $f \in k((x))[\delta]$ and $\mu_e(f) > 0$. Then the *semi-regular part* R_e of f for $e \in E$ is defined in chapter 2 as the highest order monic right-hand factor of $S_e(f)$ in $k((x))[e, \delta]$ which is semi-regular over $k((x))[e]$. The order of R_e is $\mu_e(f)$. $S_{-e}(R_e)$ is a right-hand factor of f. If f is monic and $e_1, \ldots, e_d \in E$ is a list of representatives of all exponential parts of f, then (cf. section 2.6.1)

$$f = \mathrm{LCLM}(S_{-e_1}(R_{e_1}), \ldots, S_{-e_d}(R_{e_d})). \tag{3.1}$$

This LCLM factorization of f corresponds to the direct sum splitting (cf. sections 2.8.2 and 2.8.3)

$$V(f) = V_{e_1}(f) \bigoplus \cdots \bigoplus V_{e_d}(f). \tag{3.2}$$

The solution space of $S_{-e_i}(R_{e_i})$ is $V_{e_i}(f)$.

3.3.3 Generalized exponents

In some applications (section 3.9.1, chapter 4 and chapter 5) the use of the equivalence $\sim$ erases useful information about the differential operator. We would like to make a canonical choice of representatives in E for the exponential parts (which are in $E/\sim$), and call these the generalized exponents[1].

In chapter 2 we first defined exponential parts using the map S_e and the Newton polynomial N_0 (because such a definition is convenient for computing the exponential parts) and afterwards related the exponential parts to the formal solutions (because that makes exponential parts easier to understand). We will do the same for the generalized exponents, first define them using N_0 and S_e, and then relate them to the formal solutions by introducing the notion of the *valuation* of a formal solution.

Definition 6 *Let $e \in E$ and $f \in \overline{k((x))}[\delta] \setminus \{0\}$. Define the number $\nu_e(f)$ as the multiplicity of the root 0 in $N_0(S_e(f))$.*

$e \in E$ is called a generalized exponent of f if $\nu_e(f) > 0$. The number $\nu_e(f)$ is called the multiplicity of this generalized exponent.

For a given $\overline{e} \in E/\mathbb{Q}$ the sum of $\nu_e(f)$ taken over all $e \in E$ for which $\overline{e}$ is e mod $\mathbb{Q}$ equals $\overline{\mu}_{\overline{e}}(f)$. Hence by theorem 1 on page 27 it follows that

$$\sum_{e \in E} \nu_e(f) = \mathrm{order}(f). \tag{3.3}$$

Definition 7 *Let $f \in \overline{k((x))}[\delta]$ be of order n. The list $e_1, \ldots, e_n \in E$ is called a* list of generalized exponents *of f if for all $e \in E$ the number of e_i which equal e is $\nu_e(f)$.*

[1]In an earlier version of this text a generalized exponent was called *canonical exponential part* (meaning: a canonical choice of a representative in E for an exponential part in $E/\sim$) and the list of generalized exponents was called *canonical list*.

Two lists of generalized exponents are equivalent if they are a permutation of each other. Up to this equivalence a list of generalized exponents is uniquely defined for every $f \in \overline{k((x))}[\delta]$. If f is regular singular then the list of generalized exponents is the list of roots of the Newton polynomial $N_0(f)$ of f.

Lemma 16 *If $e \in E$, $f \in \overline{k((x))}[\delta]$ and $e_1, \ldots, e_n \in E$ is the list of generalized exponents of f then $e_1 - e, \ldots, e_n - e$ is the list of generalized exponents of $S_e(f)$.*

Proof: This follows from the fact that $S_{e_i - e}(S_e(f)) = S_{e_i}(f)$.

□

Lemma 17 *If R is a right-hand factor of f then the list of generalized exponents of R is a sublist of the list of generalized exponents of f. In other words: $\nu_e(R) \leq \nu_e(f)$ for all $e \in E$.*

Proof: If R is a right-hand factor of f then $S_e(R)$ is a right hand factor of $S_e(f)$. So the Newton polynomial $N_0(S_e(R))$ is a factor of $N_0(S_e(f))$, cf. section 2.3.4.

□

The lemma does not hold for left-hand factors of f. Take for example $f = \delta \cdot (\delta - 3/x^5)$. The list of generalized exponents is $5, 3/x^5$ and the list of generalized exponents of δ is 0.

Lemma 18 *If $f_1, \ldots, f_d \in \overline{k((x))}[\delta]$ have no generalized exponents in common then the list of generalized exponents of $f = \mathrm{LCLM}(f_1, \ldots, f_d)$ is the concatenation of the lists of generalized exponents of the f_i.*

Proof: Denote l as the list of generalized exponents of f and m as the concatenation of the lists of generalized exponents of the f_i. The lists of generalized exponents of the f_i are sublists of l and since they have no elements in common it follows that m is a sublist of l. The number of elements of m is the sum of the orders of the f_i. Hence this number is $\geq \mathrm{order}(f)$, and this equals the number of elements of l. Hence l is m (up to a permutation).

□

Note that if the f_i do have generalized exponents in common then not every generalized exponent of f needs to be a generalized exponent of one of the f_i. Take for example f_1 such x is a basis of $V(f_1)$ and take f_2 such that $x + x^{10}$ is a basis of $V(f_2)$. Then the lists of generalized exponents of f_1 and f_2 are both 1, but the list of generalized exponents of $\mathrm{LCLM}(f_1, f_2)$ is $1, 10$.

Consider the set

$$\overline{V}_0 = \overline{k((x))}[\log(x)]$$

cf. page 34 in chapter 2. We can define a valuation

$$v : \overline{V}_0 \longrightarrow \mathbb{Q} \bigcup \{\infty\}$$

where $v(0) = \infty$ and $v(a)$ with $a \neq 0$ is the smallest exponent of x in a with a non-zero coefficient. So $x^{-v(a)}a \in \overline{k}[[x^{1/n}]][\log(x)]$ for some n and $v(a)$ is maximal with this property.

$\overline{V}_e \subset V$ is defined as $\mathrm{Exp}(e) \cdot \overline{V}_0$, cf. chapter 2. Define the set

$$V_* = (\bigcup_e \overline{V}_e) \setminus \{0\}$$

where the union is taken over all $e \in E$. Notice that V_* is closed under multiplication. We can extend the valuation v to V_*

$$v : V_* \longrightarrow E$$

as follows: let $y \in V_*$. Then $y = \mathrm{Exp}(e)r$ for some $e \in E$ (which is determined modulo $\mathbb{Q}$ by y) and $r \in \overline{V}_0$. Now define $v(y) = e + v(r)$. This $v(y)$ does not depend on the choice of e and r. For all $e \in E$ we have $v(\mathrm{Exp}(e)) = e$. If $v(y_1)$ and $v(y_2)$ are both defined (i.e. $y_1, y_2 \in V_*$) then $v(y_1 y_2) = v(y_1) + v(y_2)$.

Theorem 4 *Let $f \in \overline{k((x))}[\delta]$ be an operator of order m. There exists a basis $y_1, \ldots, y_m \in V_*$ of $V(f)$ such that $v(y_1), \ldots, v(y_m)$ is the list of generalized exponents of f. Conversely, for any solution y of f in V_* the valuation $v(y)$ is a generalized exponent.*

Proof: We will first prove the theorem for operators $f \in \overline{k}((x^{1/n}))[\delta]$ which are semi-regular over $\overline{k}((x^{1/n}))$. Note that $v(\int \frac{a_i}{x} dx) = v(a_i)$ (take the coefficient of the term $x^0 \log(x)^0$ in the integral equal to 0). From this it follows by induction that the algorithm in section 2.8.1 produces a basis of solutions for which the valuations are the roots of the Newton polynomial (and hence these valuations form the list of generalized exponents). Now suppose $y \in \overline{k}((x^{1/n}))[\log(x)]$ is a solution of this semi-regular f. Factor f (cf. section 2.5 and 2.8.1) as $f = L \cdot (\delta - q + a)$ where $q \in \frac{1}{n}\mathbb{Z}$, $a \in x^{1/n} \cdot \overline{k}[[x^{1/n}]]$ and $L \in \overline{k}((x^{1/n}))[\delta]$ is semi-regular. If $v(y) = q$ then $v(y)$ is a generalized exponent of $\delta - q + a$ and hence of f as well. If $v(y) \neq q$ then write $y = \sum_{i,j} c_{i,j} x^i \log(x)^j$. Here the sum is taken over $i \in \frac{1}{n}\mathbb{Z}$ and $j \in \mathbb{N}$. Take j maximal such that $c_{v(y),j} \neq 0$. Then the coefficient of $x^{v(y)} \log(x)^j$ in $(\delta - q + a)(y) = xy' - qy + ay$ is $c_{v(y),j}(v(y) - q) \neq 0$. So $v((\delta - q + a)(y)) \leq v(y)$. Furthermore all terms in $xy' - qy + ay$ have valuation $\geq v(y)$ hence $v((\delta - q + a)(y)) = v(y)$. Now $(\delta - q + a)(y)$ is a solution of the semi-regular operator L and hence by induction $v(y)$ is a root of the Newton polynomial of L. Because f is regular singular the Newton polynomial of L is a factor of the Newton polynomial of f and hence $v(y)$ is a root of the Newton polynomial of f. So the theorem holds for any semi-regular $f \in \overline{k}((x^{1/n}))[\delta]$.

To prove the theorem for any $f \in \overline{k((x))}[\delta]$ write f as

$$f = \mathrm{LCLM}(S_{-e_1}(\overline{R}_{e_1}), \ldots, S_{-e_q}(\overline{R}_{e_q})) \tag{3.4}$$

as in section 2.6.1. For a definition of $\overline{R}_e$ for $e \in E$ and $f \in \overline{k((x))}[\delta]$ see section 2.6.1. It follows from the definition that the order of $\overline{R}_e$ is $\overline{\mu}_e(f)$. The solutions of $S_{-e}(\overline{R}_e)$ are in $\overline{V}_e(f)$, cf. section 2.8.2. The dimension of the solution space of $S_{-e}(\overline{R}_e)$ is $\mathrm{order}(\overline{R}_e) = \overline{\mu}_e(f)$ which equals the dimension of $\overline{V}_e(f)$ by theorem 3 on page 34.

Hence $V(S_{-e}(\overline{R}_e)) = \overline{V}_e(f)$ and equation (3.4) corresponds to the following direct sum

$$V(f) = \overline{V}_{e_1}(f) \bigoplus \cdots \bigoplus \overline{V}_{e_q}(f).$$

Theorem 4 holds for the $\overline{R}_{e_i}$ because these are semi-regular over $\overline{k}((x^{1/n}))$ for some n. So we have a basis of solutions (computed by the method of section 2.8.1) $y_{i,j}$, $j = 1, \ldots, \overline{\mu}_{e_i}(f)$ of $\overline{R}_{e_i}$ such that the valuations of this basis form the list of generalized exponents of $\overline{R}_{e_i}$. So $\mathrm{Exp}(e_i)y_{i,j}$, $j = 1, \ldots, \overline{\mu}_{e_i}(f)$ is a basis of solutions of $S_{-e_i}(\overline{R}_{e_i})$ and according to lemma 16 the valuations of these $\mathrm{Exp}(e_i)y_{i,j}$ form the list of generalized exponents of $S_{-e_i}(\overline{R}_{e_i})$. Then from equation (3.4) it follows that $\mathrm{Exp}(e_i)y_{i,j}$, $j = 1, \ldots, \overline{\mu}_{e_i}(f)$, $i = 1, \ldots, q$ is a basis of solutions of f and according to lemma 18 the valuations of this basis is the list of generalized exponents.

To prove the second statement take $y \in V(f)$ with $y \in V_*$. Then y is a non-zero element of $\overline{V}_e(f)$ for some $e \in E$. So y is a solution of $S_{-e}(\overline{R}_e)$, and hence $\mathrm{Exp}(-e)y$ is a solution of $\overline{R}_e$. Theorem 4 is true for $\overline{R}_e$ because it is semi-regular over $\overline{k}((x^{1/n}))$ for some n. So $v(\mathrm{Exp}(-e)y) = v(y) - e$ is a generalized exponent of $\overline{R}_e$. Then by lemma 16 it follows that $v(y)$ is a generalized exponent of $S_{-e}(\overline{R}_e)$ and hence by lemma 17 $v(y)$ is a generalized exponent of f.

□

The following lemma gives a relation between factorizations in $\overline{k((x))}[\delta]$ and generalized exponents.

Lemma 19 *Let $r_1, \ldots, r_n \in \overline{k((x))}$ and $f = \delta^n + a_{n-1}\delta^{n-1} + \cdots + a_0\delta^0 \in \overline{k((x))}[\delta]$ such that $f = (\delta - r_1)\cdots(\delta - r_n)$. Define $v'(r) \in \mathbb{Q}$ for $r \in \overline{k((x))}$ as the minimum of 0 and $v(r)$. Let*

$$e_i = \mathrm{pp}(r_i) - \sum_{j>i} v'(r_i - r_j).$$

Then $e_1, \ldots, e_n$ is the list of generalized exponents of f. Furthermore

$$\mathrm{pp}(a_{n-1}) = -\sum_i (e_i + \sum_{j>i} v'(e_i - e_j)). \tag{3.5}$$

Recall that for $r \in \overline{k((x))}$ the *principal part* $\mathrm{pp}(r) \in E$ is defined in section 2.6 by the condition that $v(r - \mathrm{pp}(r)) > 0$.

Proof: Let $v_0(a)$ for non-zero $a \in \overline{k((x))}[\delta]$ be the smallest exponent of x in a with a non-zero coefficient in $\overline{k}[\delta]$, and $v_0(0) = \infty$, which generalizes the definition of v_0 in section 2.2. Then v_0 is a valuation on $\overline{k((x))}[\delta]$ and $v'(r) = v_0(\delta - r)$ for $r \in \overline{k((x))}$. Now the following relation for the Newton polynomials holds for all non-zero $L, R \in \overline{k((x))}[\delta]$

$$N_0(LR) = N_0(S_{v_0(R)}(L)) \cdot N_0(R)$$

which is a generalization of the formula in section 2.3.4 to $\overline{k((x))}[\delta]$. Let $L = \delta - r_1$ and $R = (\delta - r_2)\cdots(\delta - r_n)$ so $f = LR$. By induction we know that $e_2, \ldots, e_n$ is the list of generalized exponents of R. The list of generalized exponents of f is the list of generalized exponents of R plus one more element. To show that this element is e_1 we must show that the multiplicity of the root 0 in the polynomial $N_0(S_{e_1}(f))$ equals the multiplicity of the root 0 in $N_0(S_{e_1}(R))$ plus one, in other words $N_0(S_{e_1}(f))/N_0(S_{e_1}(R)) = T$ (here T is the variable used to denote the Newton polynomial, as in chapter 2). $S_{e_1}(f) = S_{e_1}(L) \cdot S_{e_1}(R)$ and $v_0(S_{e_1}(R)) = v_0(S_{e_1}(\delta - r_2)) + \cdots + v_0(S_{e_1}(\delta - r_n)) = v_0(\delta - r_2 + e_1) + \cdots + v_0(\delta - r_n + e_1) = v_0(\delta - r_2 + r_1) + \cdots + v_0(\delta - r_n + r_1) = \mathrm{pp}(r_1) - e_1$. Hence

$$\frac{N_0(S_{e_1}(f))}{N_0(S_{e_1}(R))} = N_0(S_{v_0(S_{e_1}(R))}(S_{e_1}(L))) = N_0(S_{\mathrm{pp}(r_1)}(L)) = T.$$

Equation (3.5) follows from the fact that $r_1 + \cdots + r_n = -a_{n-1}$ (note that $v'(r_i - r_j) = v'(e_i - e_j)$).

□

Summary: The generalized exponents are the valuations of the solutions (of those solutions for which the valuation is defined, i.e. which are in V_*). The exponential parts are the generalized exponents modulo the equivalence $\sim$. Generalized exponents of right-hand factors of f (but not of left-hand factors) are generalized exponents of f as well. For exponential parts we have this property for all factors.

3.3.4 Localization and exponential parts

For a point $p \in P^1(\overline{k}) = \overline{k} \bigcup \{\infty\}$ we can define a $\overline{k}$-automorphism $l_p : \overline{k}(x) \to \overline{k}(x)$ as follows. If $p = \infty$ then $l_p(x)$ is defined as $1/x$ and if $p \in \overline{k}$ then $l_p(x) = x + p$. We can extend l_p to a ring automorphism of $\overline{k}(x)[\partial]$ by defining $l_p(\partial) = \partial$ if p is finite (i.e. $p \in \overline{k}$) and $l_p(\partial) = -x^2\partial$ if p is infinity. For a differential operator $f \in \overline{k}(x)[\partial]$ we call $l_p(f)$ the *localization* of f at the point $x = p$. The operator $l_p(f)$ is viewed as an element of $\overline{k}((x))[\delta]$ instead of $\overline{k}(x)[\partial]$.

Definition 8 *Let $e \in E/\sim$, $f \in k(x)[\partial]$ and $p \in P^1(\overline{k})$. Define*

$$\mu_{e,p}(f) = \mu_e(l_p(f)).$$

Now e is called an exponential part *of f at the point p if $\mu_{e,p}(f) > 0$. The number $\mu_{e,p}(f)$ is called the* multiplicity *of e in f at the point p.*

If p is a semi-regular point of f then f has only a trivial (i.e. zero modulo $\sim$) exponential part at p.

The following notation $\mu_*(f) \in \mathbb{N}^{(E/\sim) \times P^1(\overline{k})}$ formalizes all exponential parts and their multiplicities at all points in $P^1(\overline{k})$

$$\mu_*(f) : (E/\sim) \times P^1(\overline{k}) \to \mathbb{N}$$

which maps (e, p) to $\mu_{e,p}(f)$. For $f, g \in \overline{k}(x)[\partial]$ we have

$$\mu_*(fg) = \mu_*(gf) = \mu_*(f) + \mu_*(g).$$

A remark on the implementation: Localizing a rational function at the point $x = 0$ is a mathematically trivial operation because $\overline{k}(x) \subset \overline{k}((x))$. On a computer this is not a trivial operation, it is a conversion of data types. Computations with infinite power series are done by *lazy evaluation*.

3.3.5 The type of an operator

In this section we will examine the relation between μ_* and the so-called type of a differential operator.

Definition 9 *Let $f, g \in \overline{k}(x)[\partial]$. Now f and g are said to be of the same* type *if there exist $r_1, r_2 \in \overline{k}(x)[\partial]$ such that*

$$r_1(V(f)) = V(g) \quad \text{and} \quad r_2(V(g)) = V(f)$$

This notion is called *Art-begriff* in [39]. Four different characterizations of this notion are given in [47], corollary 2.6. Verifying if f and g are of the same type can be done by computing the set $\mathcal{E}_{\mathcal{D}}(g, f)$ (cf. chapter 5 and [47]) and checking if it contains an r_1 for which $r_1 : V(f) \to V(g)$ is bijective. If such r_1 exists then an operator $r_2 \in \overline{k}(x)[\partial]$ with $r_2(V(g)) = V(f)$ exists as well (for properties like these and for a quick introduction to this topic see also [56]). r_2 can be found by solving the equation $r_2 r_1 + lf = 1$ via the extended Euclidean algorithm (cf. [40]). This equation has a solution $r_2, l \in \overline{k}(x)[\partial]$ because r_1 is injective on $V(f)$ and hence $\mathrm{GCRD}(f, r_1) = 1$ (GCRD stands for greatest common right divisor).

Define the following equivalence $\sim_*$ on $\overline{k}(x)$.

$$r_1 \sim_* r_2 \Longleftrightarrow \exists_{y \in \overline{k}(x)} \ \ r_1 - r_2 = y'/y.$$

Define for $r \in \overline{k}(x)$ the $\overline{k}(x)$-automorphism

$$S_r^* : \overline{k}(x)[\partial] \to \overline{k}(x)[\partial]$$

by $S_r^*(\partial) = \partial + r$. Note that this is not the same (∂ instead of δ) as the previously defined S_r. For $f, g \in \overline{k}(x)[\partial]$ if $\mu_*(f) = \mu_*(g)$ then $\mu_*(S_r^*(f)) = \mu_*(S_r^*(g))$. Similarly if $\mathrm{type}(f) = \mathrm{type}(g)$ then $\mathrm{type}(S_r^*(f)) = \mathrm{type}(S_r^*(g))$.

Lemma 20 *Let $a, b \in \overline{k}(x)$. Then $\mu_*(\partial) = \mu_*(\partial - a)$ if and only if $\partial - a$ has a non-zero solution y in $\overline{k}(x)$. Furthermore $\mu_*(\partial - a) = \mu_*(\partial - b)$ if and only if $a \sim_* b$.*

Note that $\mu_*(\partial) = \mu_*(\partial - a)$ means $\partial - a$ is semi-regular at all points $p \in P^1(\overline{k})$.

Proof: If $\partial - a$ has a rational solution y then $l_p(\partial - a)$ has a solution $l_p(y) \in V_0$. Hence $\mu_0(l_p(\partial - a)) > 0$ for all p. Since the order is 1 there are no other exponential parts hence $l_p(\partial - a)$ is semi-regular. Conversely if $\partial - a$ is semi-regular at all points p then one can verify that

$$y = \prod_{p \in \overline{k}} (x - p)^{a_p} \in \overline{k}(x)$$

is a non-zero rational solution of $\partial - a$, where $a_p \in \mathbb{Z}$ is the exponent of $\partial - a$ at p. Hence the first statement follows. The second statement is reduced to the first statement by applying S_a^*.

□

Lemma 21 *Let $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^n$ and $g = \partial^n + b_{n-1}\partial^{n-1} + \cdots + b_0\partial^n$ be in $\overline{k}(x)[\partial]$. Let $a_{i,p}, b_{i,p} \in \overline{k}((x))$ for $i = 0, \ldots, n-1$ and $p \in P^1(\overline{k})$ such that $l_p(f) = \delta^n + a_{n-1,p}\delta^{n-1} + \cdots + a_{0,p}\delta^n$ and $l_p(g) = \delta^n + b_{n-1,p}\delta^{n-1} + \cdots + b_{0,p}\delta^n$. Then $a_{n-1} \sim_* b_{n-1}$ if and only if $\mathrm{pp}(a_{n-1,p} - b_{n-1,p})$ is an integer for all $p \in P^1(\overline{k})$.*

Note: For convenience of notation $l_p(f) \in \overline{k}((x))[\delta]$ has been multiplied on the left by an element of $\overline{k}((x))$ so that it can be represented as a monic element of $\overline{k}((x))[\delta]$.

Proof: Denote $f_1 = \partial + a_{n-1}$ and $g_1 = \partial + b_{n-1}$. One can verify (for a similar, but more detailed computation see also lemma 25 in section 3.9.1) that $l_p(f_1) = \delta + a_{n-1,p} + m_p$ for some $m_p \in \mathbb{Z}$. Now $a_{n-1,p} - b_{n-1,p} \in \mathbb{Z} + x \cdot \overline{k}[[x]]$ if and only if $\delta + a_{n-1,p}$ and $\delta + b_{n-1,p}$ in $\overline{k}((x))[\delta]$ have the same exponential part $e \in E/\sim$. So $a_{n-1,p} - b_{n-1,p} \in \mathbb{Z} + x \cdot \overline{k}[[x]]$ for all $p \in P^1(\overline{k})$ if and only if $\mu_*(f_1) = \mu_*(g_1)$. Now the lemma follows from the previous lemma.

□

Proposition 1 *Let $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^n$ and $g = \partial^n + b_{n-1}\partial^{n-1} + \cdots + b_0\partial^n$ be in $\overline{k}(x)[\partial]$. Then*

$$\text{type(f)} = \text{type}(g) \Longrightarrow \mu_*(f) = \mu_*(g). \tag{3.6}$$

Furthermore

$$\mu_*(f) = \mu_*(g) \Longrightarrow a_{n-1} \sim_* b_{n-1}. \tag{3.7}$$

If $n = 1$ then the two implication arrows can be reversed.

For $n > 1$ these arrows can not be reversed. Take for example $\partial^2 + x^5$ and $\partial^2 + x^5 + x$. These two operators have the same μ_* but not the same type. The second arrow can not be reversed either if $n > 1$, as almost any random example will show: $\mu_*(\partial^2) \neq \mu_*(\partial^2 - x)$; the exponential parts are different at $x = \infty$.

Proof: Suppose $\text{type}(f) = \text{type}(g)$. By definition $r(V(f)) = V(g)$ for some operator r. We need to show that $\mu_{e,p}(f) = \mu_{e,p}(g)$ for all e and p. We may assume (after having applied the map l_p) that $p = 0$. Recall from section 3.3 that $r(V_e) = V_e$, $V_e(f) = V_e \bigcap V(f)$ and $\mu_e(f) = \dim(V_e(f))$. From $r(V_e(f)) = r(V_e \bigcap V(f)) \subset r(V(f)) \bigcap r(V_e) = V(g) \bigcap V_e = V_e(g)$ it follows that $\mu_e(f) \leq \mu_e(g)$. In the same way one shows that $\mu_e(f) \geq \mu_e(g)$ and so (3.6) is proven.

If $n = 1$ then (3.7) follows from lemma 20. The fact that $a_{n-1} \sim_* b_{n-1}$ implies $\text{type}(f) = \text{type}(g)$ if $n = 1$ follows directly from the definitions. What remains to be shown is (3.7) for the case $n > 1$.

Consider two lists $e_1, \ldots, e_n$ and $e'_1, \ldots, e'_n$ of elements of $\overline{k}[x^{-1/r}] \subset E$, such that $e_i \sim e'_i$ for all i. Denote $d = (e_1 + \cdots + e_n) - (e'_1 + \cdots + e'_n)$. Then $d \in \frac{1}{r}\mathbb{Z}$ but not necessarily $d \in \mathbb{Z}$. However, if both lists are invariant (up to permutations) under the Galois action of the field extension $\overline{k}(x) \subset \overline{k}(x^{1/r})$ then one can conclude $d \in \mathbb{Z}$.

Let $p \in P^1(\overline{k})$. Let $a_{i,p}, b_{i,p}$ be elements of $\overline{k}((x))$ such that $l_p(f) = \delta^n + a_{n-1,p}\delta^{n-1} + \cdots + a_{0,p}\delta^n$ and $l_p(g) = \delta^n + b_{n-1,p}\delta^{n-1} + \cdots + b_{0,p}\delta^n$ (note: here $l_p(f)$ and $l_p(g)$ have been multiplied on the left by an element of $\overline{k}((x))$ to make them monic). Let $e_1, \ldots, e_n$ resp. $e'_1, \ldots, e'_n$ be the lists of generalized exponents of $l_p(f)$ and $l_p(g)$. Assume that $\mu_*(f) = \mu_*(g)$. Then, after a permutation, we have $e_i \sim e'_i$

for $i = 1, \ldots, n$. Then $v'(e_i - e_j) = v'(e'_i - e'_j)$ where v' is defined in lemma 19. Because the lists of generalized exponents are invariant under the Galois action of $\overline{k}(x) \subset \overline{k}(x^{1/r})$ it follows that $\sum_i (e_i - e'_i)$ is an integer. Then by equation (3.5) it follows that $\mathrm{pp}(a_{n-1,p} - b_{n-1,p})$ is an integer. This holds for all $p \in P^1(\overline{k})$ hence (3.7) follows from lemma 21.

□

Definition 10 *Let $f \in \overline{k}(x)[\partial]$ then $\gamma_1(f)$ is the set of all $\mu_*(R)$ for all first order right-hand factors $R \in \overline{k}(x)[\partial]$ of f.*

Because of lemma 20 the set $\gamma_1(f)$ can be identified with a subset of $\overline{k}(x)[\partial]/\sim_*$. We can also view it as the set of types of all first order right-hand factors. In the next section we will see that once $\gamma_1(f)$ is known, then computing all first order right-hand factors is not difficult anymore. This is in fact more general: Given an operator f and an irreducible operator R, one can compute all right-hand factors of f that are of the same type as R by solving a mixed equation. This follows from work of Loewy and Ore, see [56] for an introduction to this topic. Solving the mixed equation is the topic of chapter 5. So one can find all irreducible right-hand factors of f if one can find the set of types (this set is finite) of all irreducible right-hand factors of f.

The fact that for order $n = 1$ the type of an operator corresponds to μ_* (which is a collection of local data, i.e. data that we can compute) is the reason that computing factors of order 1 is theoretically easier than computing higher order factors. For higher order factors R the type is not determined by $\mu_*(R)$ which makes the situation more complicated. However, the coefficient a_{n-1} of $R = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ is determined modulo $\sim_*$ by $\mu_*(R)$, in other words $\mathrm{type}(\partial + a_{n-1})$ is determined by $\mu_*(R)$. Hence it is not surprising that in Beke's method for higher order factors of f one first computes a differential equation $\wedge^n f$, such that for any right-hand factor $R = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ of f the operator $\partial + a_{n-1}$ is as a right-hand factor of $\wedge^n f$ (see also section 3.8 on this).

3.4 Beke's method for finding first order factors

In this section we will describe Beke's factorization method in [6]. His method is a good illustration how to use exponential parts. Previous implementations for factorization in $\overline{k}(x)[\partial]$ are based on his method. For example, the factorizer in the Kovacic algorithm (cf. Section 3.1 in [30]) is based on Beke's method. Note that Beke only uses this method for regular singular operators, for the more general case he uses polynomial equations. However, equipped with the terminology of chapter 2, the regular singular case is not harder nor easier than the general case. We only need to replace the word exponent in Beke's text by exponential part. Though the method in this section is not precisely the same as in [6], the difference is small enough to call it Beke's method.

Let $f \in k(x)[\partial]$. Assume f has a first order right-hand factor factor $\partial - r$ where $r \in \overline{k}(x)$ and we want to compute such a factor. This is done in 2 steps

1. Determine $\mu_*(\partial - r)$, i.e. determine the exponential part of $\partial - r$ at all singularities.

2. Compute r.

When $\mu_*(\partial - r)$ is known then r is determined up to the equivalence $\sim_*$. So we can take a representative $r_0 \in \overline{k}(x)$ such that $r_0 \sim_* r$, in other words $r - r_0 = y'/y$ for some $y \in \overline{k}(x)$. Now r is easily found as follows. y is a rational solution of $S^*_{r_0}(\partial - r)$ and hence a rational solution of $S^*_{r_0}(f)$. Any rational solution of $S^*_{r_0}(f)$ gives a right factor $\partial - r = \partial - r_0 - y'/y$ of f.

Beke's method does not give a real answer to how to do the first step, except by trying all possibilities. Suppose order$(f) = N$ and f has M singularities. In every singularity there are at most N different exponential parts so the number of possibilities to check is $\leq N^M$. Another reason that checking all possibilities is very costly is because it can introduce large algebraic extensions. Localizing at all singularities costs at most an algebraic extension of degree $M!$ over k. Computing an exponential part in one singularity costs at most an extension of degree N so Beke's method uses an algebraic extension of degree $\leq M! \cdot N^M$. If the set $\gamma_1(f)$ were known then the algebraic extensions one needs to compute with would be much smaller. *Computing all first order right-hand factors of f and computing $\gamma_1(f)$ are equivalent problems.*

Note that Beke's method implies a method for computing the radical solutions (i.e. solutions y for which $y^n \in \overline{k}(x)$ for some integer n). For this we need to adapt the algorithm such that it only tries exponential parts in $\mathbb{Q}$ modulo $\mathbb{Z}$ instead of all exponential parts.

3.5 The main idea of the algorithm

Let $f \in k(x)[\partial]$ and suppose a non-trivial factorization $f = LR$ exists with $L, R \in \overline{k}(x)[\partial]$. We want to determine a right-hand factor of f. This could be done if we knew a non-zero subspace $W \subset V(R)$, cf. section 3.6. However, a priori we only know that $V(R) \subset V(f)$ but this does not give any non-zero element of $V(R)$.

For any exponential part e of f at a point $p \in P^1(\overline{k})$ we have (after replacing f, L, R by $l_p(f), l_p(L), l_p(R)$ we may assume that $p = 0$) $V_e(R) \subset V_e(f)$ and $\mu_e(L) + \mu_e(R) = \mu_e(f)$. Suppose that we are in a situation where $\mu_e(L) = 0$. Then the dimensions of $V_e(R)$ and $V_e(f)$ are the same and hence we have found a subspace $V_e(f) = V_e(R)$ of $V(R)$. Then we can factor f (cf. section 3.6). Note that we do not necessarily find the factorization LR, it is possible that instead of R a right-hand factor of R is found.

So now we search for situations where we may assume $\mu_e(L) = 0$. There are several instances of this:

1. Suppose that order$(L) = 1$ and that f has more than 1 exponential part at the point p. Let $e_1 \not\sim e_2$ be two different exponential parts of f. Then $\mu_{e_1}(L) = 0$ or $\mu_{e_2}(L) = 0$ because the sum of the multiplicities $\mu_e(L)$ for all exponential parts $e \in E/\sim$ is the order of L which is 1. So we need to distinguish two separate cases and in at least one of these cases we will find a non-trivial factorization of f.

2. More generally suppose order$(L) = d$ and that at a point p the operator f has at least $d + 1$ different exponential parts $e_1, \ldots, e_{d+1}$. Then for at least one of

these e_i we have $\mu_{e_i}(L) = 0$. Hence by distinguishing $d+1$ cases $i = 1, \ldots, d+1$ we will find a non-trivial factorization of f.

So we can factor any reducible operator which has:

1. A first order left-hand factor and a singularity with more than 1 exponential part.
2. Or more generally: an operator with a left-hand factor of order d and a singularity at which there are more than d different exponential parts.
3. By using the adjoint we can also factor operators which have a right-hand factor of order d and a point p with more than d different exponential parts.
4. An operator which has a singularity with an exponential part e of multiplicity 1. Then we can distinguish two cases $\mu_e(L) = 0$ or $\mu_e(R) = 0$. The latter case is reduced to the former case using the adjoint. We call the minimum of the multiplicities taken over all exponential parts of all singularities the *minimum multiplicity*. By checking both cases $\mu_e(L) = 0$ or $\mu_e(R) = 0$ any operator f with minimum multiplicity 1 is either irreducible or it is factored by our method.

Note on computing first order factors: If a first order left or right-hand factor exists, then our approach can compute a factorization whenever there is a singularity with at least two different exponential parts. This reduces the problem of finding all first order factors, cf. section 3.7. The only case that remains is when each singularity has only 1 exponential part. However, this special case is a trivial case for Beke's method because we need to check only one possibility in Beke's method. We can proceed as follows: Compute an $r \in k(x)$ such that $\partial - r$ has the same exponential part as f at all singularities. Then $S_r^*(f)$ is semi-regular at all singularities. For computing the first order right-hand factors of such an operator the only thing one needs to do in Beke's method is to compute the rational solutions.

Note on computing higher order factors: An operator with minimum multiplicity 1 is either irreducible or factored by our algorithm. If the minimum multiplicity is > 1 we can often still factor f by constructing irreducible local factors for the different exponential parts and trying to construct right-hand factors $R \in \overline{k}(x)[\partial]$ from these local factors in the same way as in section 3.6. However, in this case our algorithm is a incomplete because we can not guarantee irreducibility if no factorization is obtained. Currently our implementation will print a warning message in such cases. To make the algorithm complete for these cases we will have to use the rather inefficient exterior power method, cf. section 3.8.

Note that it is possible that a factor of a minimum multiplicity 1 operator has minimum multiplicity > 1.

3.6 Computing a right-hand factor R

After having applied the map l_p of section 3.3.4 (and a field extension of k if $p \in \overline{k} \setminus k$) we may assume that the singularity p in the previous section is the point $p = 0$.

The assumption from section 3.5 was that an $e \in E$ is known for which $\mu_e(f) > 0$ and $\mu_e(L) = 0$. From this we concluded that $V_e(f) \subset V(R)$. In other words

$S_{-e}(R_e) \in k((x))[e, \delta]$ is a right-hand factor of R, where R_e is the semi-regular part of f, cf. section 2.6.1. R_e and hence $S_{-e}(R_e)$ can be computed by local factorization (cf. section 2.8.4). We want to have a local right-hand factor r of R. There are several strategies: We can take $r = S_{-e}(R_e)$, or we can take a first order right-hand factor in $k((x))[e, \delta]$ of $S_{-e}(R_e)$. Another strategy, to speed up the algorithm, is first to try to factor f in $k(x)[\partial]$ instead of $\overline{k}(x)[\partial]$. If no factorization in $k(x)[\partial]$ is obtained, then we can redo the computation afterwards to search a factorization in $\overline{k}(x)[\partial]$. If we want to factor f in $k(x)[\partial]$ then we can take $r \in k((x))[\delta]$ of minimal order such that $S_{-e}(R_e)$ is a right-hand factor of r. So, depending on whether we want to factor f in $k(x)[\partial]$ or in $\overline{k}(x)[\partial]$, we have a right-hand factor $r \in k((x))[\delta]$ or $r \in k((x))[e, \delta]$ of R. Note that to find r we do not need to compute formal solutions, we only need the factorization algorithm in chapter 2. From now on we will assume that $r \in k((x))[\delta]$, the other case works precisely the same (just replace k by $\overline{k}$).

Let $n = \text{order}(f)$. The goal is to compute an operator $R = a_d\partial^d + \cdots + a_0\partial^0 \in k[x, \partial]$ that has r as a right-hand factor. Here d should be minimal. Because r divides both f and R on the right it also divides $\text{GCRD}(f, R)$. Then $\text{GCRD}(f, R) = R$ because d is minimal. We conclude that R is a right-hand factor of f. If $d < n$ a non-trivial factorization is obtained this way.

There are two ways of choosing the number d. The first is to try all values $d = 1, 2, \ldots, n-1$. Suppose that for a certain d we find an R that has r as a right-hand factor and for numbers smaller than d such R could not be found. Then d is minimal and hence R is a right-hand factor of f. The second approach to take $d = n - 1$. If we find $R = a_d\partial^d + \cdots + a_0\partial^0$ that has r as a right-hand factor we can compute $\text{GCRD}(R, f)$. This way we also find a right-hand factor of f. Sometimes it is possible to conclude a priori that there is no right-hand factor of order $n - 1$. If for instance all irreducible local factors have order ≥ 3 then the order of a right-hand factor is $\leq n - 3$ and so we can take $d = n - 3$ instead of $d = n - 1$.

We can compute a bound N (cf. section 3.9) for the degrees of the a_i. So the problem now is

- Are there polynomials $a_i \in k[x]$ of degree $\leq N$, not all equal to 0, such that r is a right-hand factor of $R = a_d\partial^d + \cdots + a_0\partial^0$?

Let m be the order of r. Write $D = k((x))[\partial]$. The D module D/Dr is a $k((x))$-vector space of dimension m with a basis $\partial^0, \partial^1, \ldots, \partial^{m-1}$. Write $\partial^0, \partial^1, \ldots, \partial^d$ on this basis as vectors $v_0, \ldots, v_d$ in $k((x))^m$. Now multiply $v_0, \ldots, v_d$ with a suitable power of x such that the v_i become elements of $k[[x]]^m$. r is a right factor of R if and only if

$$a_0v_0 + \cdots + a_dv_d = 0$$

in $k[[x]]^m$. This is a system of linear equations with coefficients in $k[[x]]$ which should be solved over $k[x]$. One way of solving this is to convert it to a system of linear equations over k using the bound N. A much faster way is the Beckermann-Labahn algorithm which was found first by Labahn and Beckermann, and later independently by Derksen [17, 5]. Their method is as follows

Sketch of the Beckermann-Labahn algorithm

- Let $M_i \subset k[x]^{d+1}$ be the $k[x]$-module of all sequences $(a_0, a_1, \ldots, a_d)$ for which $v(a_0v_0 + \cdots + a_dv_d) \geq i$. The "valuation" v of a vector is defined as the minimum of the valuations of its entries. The valuation of 0 is infinity.

- Choose a basis (as $k[x]$-module) of M_0.
- For $i = 1, 2, 3, \ldots$ compute a basis for M_i using the basis for M_{i-1}.

This sketch looks easy and the algorithm is short (Derksen's implementation is only a few kilobytes) but it is absolutely non-trivial. The difficult part is how to construct a basis for M_i from a basis for M_{i-1} in an efficient way. Labahn, Beckermann and Derksen give an elegant solution for this problem by computing a basis with a certain extra property. Given a basis for M_{i-1} with this property they are able to compute a basis for M_i in a very efficient way. Again this basis has this special property which allows the computation of M_{i+1} so one can continue this way.

Define the degree of a vector of polynomials as the maximum of the degrees of these polynomials. From the basis for M_i we can find a non-zero $A_i \in M_i$ with minimal degree. Suppose there exists a non-zero $R = a_d\partial^d + \cdots + a_0\partial^0 \in k[x, \partial]$ having r as a right-hand factor. Then there exists such R with all $\deg(a_i) \leq N$ where N is a bound we can compute, cf. section 3.9. So then there is a non-zero $(a_0, \ldots, a_d)$ of degree $\leq N$ which is an element of every M_i. Because of the minimality of $\deg(A_i)$ it follows that then $\deg(A_i) \leq N$ for all i. So whenever $\deg(A_i) > N$ for any i we know that there is no $R \in k(x)[\partial]$ of order d which has r as a right-hand factor.

Algorithm Construct R
For $i = 0, 1, 2, \ldots$ do

- Compute M_i and $A_i \in M_i$ of minimal degree.
- If $\deg(A_i) > N$ then RETURN "R does not exist".
- If $\deg(A_i) = \deg(A_{i-3})$ then
  Comment: the degree did not increase 3 steps in a row so it is likely that a right-hand factor is found.
  If $A_i = (a_0, \ldots, a_d)$ then write $R = a_d\partial^d + \cdots + a_0\partial^0$. Divide by a_d to make R monic. Test if R and f have a non-trivial right-hand factor in common. If so, return this right-hand factor, otherwise continue with the next i.

Suppose the algorithm does not terminate. Then $\deg(A_i) = B_1$ for all $i \geq B_2$ for some integers B_1 and B_2. Define $D_i \subset M_i$ as the k-vector space generated by A_j with $j \geq i$. These D_i are finite dimensional k-vector spaces and $D_{i+1} \subset D_i$ for each i. Then there must be an integer i such that D_i is the intersection of all D_j. Let $(a_0, \ldots, a_d) = A_i$. This A_i is an element of every $D_j \subset M_j$ so the valuation of $a_0v_0 + \cdots + a_dv_d$ is $\geq j$ for any j. Then $a_0v_0 + \cdots + a_dv_d = 0$ so r is a right-hand factor of $a_d\partial^d + \cdots + a_0\partial^0$. Then we have a contradiction because this means that the algorithm will find a right-hand factor in step i. So the algorithm terminates.

In our implementation we use modular arithmetic to replace the computations in $\mathbb{Q}$ by computations modulo some prime power p^n. This works for sufficiently large p. If it appears during the computation that p is not high enough the computation will be re-done with a larger prime number. Rational numbers can be reconstructed from their modular images if we have taken sufficiently many and sufficiently large prime powers (the algorithm is called iratrecon in Maple, unfortunately no reference is given in the help page). If k is an algebraic extension of $\mathbb{Q}$ then elements of k are represented as polynomials over $\mathbb{Q}$ in one or more variables with a bounded degree.

Then this modular arithmetic avoids the so-called "intermediate expression swell". If the transcendence degree of k over $\mathbb{Q}$ is more than 0 then modular arithmetic does not avoid intermediate expression swell. If we then still want to avoid expression swell we would need to substitute values in $\mathbb{Q}$ for transcendental elements of k to reduce the transcendence degree. For factors of order > 1 it is not clear if this will work, for the case of order 1 factors see the comments at the end of the next section.

3.7 Computing all first order right-hand factors

Our algorithm in sections 3.5 and 3.6 can find a non-trivial factorization for any operator which has a first order right-hand factor. However, it may not compute all first order right-hand factors. In this section we show how to combine Beke's method with our factorization method. With this combination we can:

1. Like Beke's algorithm compute all first order right-hand factors R.
2. Avoid checking an exponential number of different $\mu_*(R)$. In fact we will need to check at most order(f) different $\mu_*(R)$.

Lemma 22 *If $f, L, R \in \overline{k}(x)[\partial]$ and $f = LR$ then $\gamma_1(f) \subset \gamma_1(L) \bigcup \gamma_1(R)$.*

Proof: Let $\partial - r$ be a right factor of f and let $y \neq 0$ be a solution of $\partial - r$. Then y is a solution of f. We must prove that $\mu_*(\partial - r)$ is in $\gamma_1(L)$ or $\gamma_1(R)$. If y is a solution of R then $\partial - r$ is a factor of R so $\mu_*(\partial - r) \in \gamma_1(R)$. If y is not a solution of R then $R(y)$ is a non-zero solution of L. Using the fact $y' = ry$ we can write derivatives of y as multiples of y and hence $R(y) = ty$ for some $t \in \overline{k}(x)$. Now ty is a solution of L so $\partial - (ty)'/(ty) = \partial - t'/t - y'/y = \partial - t'/t - r$ is a right-hand factor of L. So $\mu_*(\partial - t'/t - r) \in \gamma_1(L)$ and $\mu_*(\partial - t'/t - r) = \mu_*(\partial - r)$ (cf. section 3.3.5).

□

Lemma 23 *If $f = \mathrm{LCLM}(f_1, \ldots, f_d)$ with $f, f_1, \ldots, f_d \in \overline{k}(x)[\partial]$ and* $\mathrm{order}(f) = \sum_i \mathrm{order}(f_i)$ *then $\gamma_1(f) = \bigcup_i \gamma_1(f_i)$.*

Without the condition $\mathrm{order}(f) = \sum_i \mathrm{order}(f_i)$ the lemma need not hold. For example $f_1 = \partial \cdot (\partial - x)$ and $f_2 = (\partial - 1/(x-1)) \cdot (\partial - x)$.

Proof: $\bigcup_i \gamma_1(f_i) \subset \gamma_1(f)$ because every right-hand factor of every f_i is a right-hand factor of f. So we only need to show that $\gamma_1(f) \subset \bigcup_i \gamma_1(f_i)$.

First suppose $d = 2$. Suppose $\partial - r$ is a right-hand factor of f. We must show that $\mu_*(\partial - r)$ is in $\gamma_1(f_1)$ or in $\gamma_1(f_2)$. From the condition $\mathrm{order}(\mathrm{LCLM}(f_1, f_2)) = \mathrm{order}(f_1) + \mathrm{order}(f_2)$ it follows that f_1 and f_2 have no common right-hand factor. Then we can write $1 = g_1 f_1 + g_2 f_2$ for some $g_1, g_2 \in \overline{k}(x)[\partial]$ using the extended Euclidean algorithm. The solution space of f is a direct sum $V(f) = V(f_1) \bigoplus V(f_2)$. $g_1 f_1 + g_2 f_2$ is the identity and $g_2 f_2$ acts like the zero map on $V(f_2)$ hence $g_1 f_1$ acts like the projection map of $V(f)$ to $V(f_2)$. Similarly, if $y \in V(f)$ then $g_2 f_2(y) \in V(f_1)$ is the projection of y on the component $V(f_1)$. Let $y \in V(f)$ be a non-zero solution of the right-hand factor $\partial - r$ of f. $(g_1 f_1 + g_2 f_2)(y) = y$ so $g_1 f_1(y) \neq 0$ or $g_2 f_2(y) \neq 0$. Assume $g_1 f_1(y) \neq 0$, in the other case the proof works in the same way. Like in the proof of the previous lemma we can write $g_1 f_1(y) = ty$ for some rational function t. Then ty is a solution of f_2 and so $\partial - r - t'/t$ is a right-hand factor of f_2. $\mu_*(\partial - r) = \mu_*(\partial - r - t'/t) \in \gamma_1(f_2)$.

If $d > 2$ write $f = \mathrm{LCLM}(f_1, \mathrm{LCLM}(f_2, \ldots, f_d))$ and apply induction.

□

Algorithm compute the possible $\mu_*(R)$
Input: An operator $f \in k(x)[\partial]$.
Output: A set S with at most order(f) elements such that $\gamma_1(f) \subset S$.

1. If order$(f) = 1$ then the problem is trivial.

2. If order$(f) > 1$ then apply the factorization algorithm of section 3.5.

   (a) If no non-trivial factorization is found then f has no first order right factors so return the empty set.

   (b) If a factorization $f = LR$ is found then apply recursion on L and R and use lemma 22.

   (c) If a factorization of the form $f = L \cdot \mathrm{LCLM}(R_1, \ldots, R_d)$ is found then apply recursion on L and apply step 2d on $\mathrm{LCLM}(R_1, \ldots, R_d)$.

   (d) If an LCLM factorization $f = \mathrm{LCLM}(R_1, \ldots, R_d)$ is found then

      i. If order$(f) = \sum_i$ order(R_i) then apply lemma 23. Note that if the $R_i \in \overline{k}(x)[\partial]$ are conjugated over k then it suffices to apply recursion on only R_1 because γ_1 of the other factors $R_2, \ldots, R_d$ can be obtained from $\gamma_1(R_1)$ by conjugation.

      ii. If order$(f) < \sum_i$ order(R_i) then compute the greatest common right divisor G_1 of R_1 and $\mathrm{LCLM}(R_2, \ldots, R_d)$. If G_1 is a non-trivial factor of R_1 then let $G_1, \ldots, G_n$ be the conjugates of G_1 over k. Then $f = L \cdot \mathrm{LCLM}(G_1, \ldots, G_n)$ for some L and so we can proceed as in case 2c. This recursion terminates because order$(G_1) <$ order(R_1). If G_1 is not a non-trivial factor then compute operators $\tilde{R}_i$, $i = 2, \ldots, d$ such that $V(\tilde{R}_i) = R_1(V(R_i))$. Then $f = \mathrm{LCLM}(\tilde{R}_2, \ldots, \tilde{R}_d) \cdot R_1$ and we can apply recursion.

Algorithm first order factors
Input: An operator $f \in k(x)[\partial]$.
Output: All first order right-hand factors $R \in \overline{k}(x)[\partial]$ of f.

1. Compute the set S from "algorithm compute the possible $\mu_*(R)$"

2. For each element of $s \in S$ do

   (a) Construct an $r \in \overline{k}(x)$ such that $\mu_*(\partial - r) = s$. Note that this requires no computation because a factor $\partial - r$ with $\mu_*(\partial - r) = s$ has already been computed in a factorization that was done in "algorithm compute the possible $\mu_*(R)$".

(b) Compute a basis $y_1, \ldots, y_d$ of rational solutions of $S_r^*(f)$ and write the general rational solution as $c_1 y_1 + \cdots + c_d y_d$ where the c_i are undetermined constants.

(c) If $d \neq 0$ then $\partial - r - (c_1 y_1 + \cdots + c_d y_d)'/(c_1 y_1 + \cdots + c_d y_d)$ are right-hand factors of f parametrized by $(c_1, \ldots, c_d) \in P^{d-1}(\overline{k})$.

It follows that the set of $r \in \overline{k}(x)$ for which $\partial - r$ is a right-hand factor of f is a disjoint union of at most order(f) projective spaces.

The algorithm in sections 3.5, 3.6 only avoids intermediate expression swell if $k \subset \overline{\mathbb{Q}}$. If the transcendence degree of k is > 0 then the algorithm still works, but then it is much less efficient. We will explain below that finding first order factors of operators in $k(x)[\partial]$ can be reduced to finding first order factors of operators in $\overline{\mathbb{Q}}(x)[\partial]$. This is important for the efficiency because in this way intermediate expression swell can be avoided.

Suppose k is a field, finitely generated over $\mathbb{Q}$, of transcendence degree $d > 0$. We will briefly describe in the rest of this section how computing all first order right-hand factors over k can be reduced to the same problem over a field of transcendence degree $d-1$. We will only give the idea and skip the details. Suppose k is an algebraic function field $k = l(s,t)$, where l is of transcendence degree $d-1$, s is transcendental over l and t is algebraic over $l(s)$. Then there exists a regular point $(s,t) = (s_0, t_0) \in (\overline{l})^2$ on the corresponding curve such that the coefficients of f are in the local ring at this point. A regular point corresponds to a valuation v on k. For elements $c \in k$ we have $v(c) \geq 0$ if and only if c is in the local ring at this point. Such elements can be evaluated at the point (s_0, t_0). Denote this evaluation map by τ. If $c \in k$ with $v(c) \geq 0$ then $\tau(c) \in l(s_0, t_0) \subset \overline{l}$.

This valuation v can be extended to a (non-discrete) valuation on $\overline{k}$. It can be further extended to a valuation on $\overline{k}[x]$ by defining the valuation of an element of $\overline{k}[x]$ as the minimum of the valuations of its coefficients in $\overline{k}$. Then v can be extended to $\overline{k}(x)$ because this is the field of fractions of $\overline{k}[x]$. Now v can be extended to $\overline{k}(x)[\partial]$ by defining the valuation of an operator in $\overline{k}(x)[\partial]$ as the minimum of the valuations of its coefficients in $\overline{k}(x)$. One can verify that this is indeed a valuation, i.e. that for operators $f, g \in \overline{k}(x)[\partial]$ we have $v(f \cdot g) = v(f) + v(g)$. The evaluation map τ can be extended as well, if $g \in \overline{k}(x)[\partial]$ and $v(g) \geq 0$ then $\tau(g) \in \overline{l}(x)[\partial]$ can be defined (first extend τ to $\overline{k}[x]$, then to $\overline{k}(x)$ and then to $\overline{k}(x)[\partial]$).

Without loss of generality we may assume that f is monic (i.e. the coefficient of the highest power of ∂ in f is 1) and we only consider monic factors of f. We can choose the point (s_0, t_0) in such a way that the valuation of f is 0. A monic operator has valuation ≤ 0 because the valuation of the leading coefficient is $v(1) = 0$. If $f = LR$ with $L, R \in \overline{k}(x)[\partial]$ and L, R are monic then $v(f) = v(L) + v(R)$ and since the valuations of L and R are ≤ 0 we have $v(R) = 0$. So any monic right-hand factor R of f can be evaluated at the point $(s,t) = (s_0, t_0)$. In other words: if $f = LR$ with L, R monic then this factorization can be evaluated at the point (s_0, t_0) which gives the factorization $\tau(f) = \tau(L)\tau(R)$. Now we can reduce the problem of computing all first order right factors of f as follows: compute the right factors of $\tau(f)$, this gives $\gamma_1(\tau(f))$ (cf. section 3.3.5 for a definition). Now for any first order right-hand factor R of f we have a right-hand factor $\tau(R)$ of $\tau(f)$ so $\tau(\gamma_1(f)) \subset \gamma_1(\tau(f))$. Choose the point (s_0, t_0) in such a way that for any two different exponential parts of f the images under τ do not coincide. Then we can reconstruct $\gamma_1(f)$ from $\tau(\gamma_1(f))$. We do not know $\tau(\gamma_1(f))$, however. But we know that $\tau(\gamma_1(f))$ is a subset of $\gamma_1(\tau(f))$ so we can check each element of $\gamma_1(\tau(f))$ to see if it yields a factor of f. This way we find all first order right factors of f.

3.8 Several strategies for completing the algorithm

Suppose $f \in k(x)[\partial]$ and our factorization algorithm in sections 3.5, 3.6 and 3.7 produces no non-trivial factorization. Can we then stop the computation and conclude that f is irreducible? If $\text{order}(f) < 4$ or if there exist e, p such that $\mu_{e,p}(f) = 1$ (the algorithm computes all $\mu_{e,p}(f)$ so it knows when this case occurs) then the answer is yes. In the remaining cases we can apply the following approach that we will call the *exterior power method*. It is obtained from [6] combined with significant improvements (namely steps 3 and 4) given in [55, 14].

1. Compute an operator $\wedge^d f \in k(x)[\partial]$ with the property that if $y_1, \ldots, y_d \in V(f)$ then the Wronskian of $y_1, \ldots, y_d$ is in $V(\wedge^d f)$. We will call $\wedge^d f$ the d-th exterior power of f (called Differentialresolvente in [6]. These equations are often also called associated equations). The important property is that if
$$\partial^d + a_{d-1}\partial^{d-1} + \cdots + a_0\partial^0$$
is a right-hand factor of f then $\partial + a_{d-1}$ is a right-hand factor of $\wedge^d f$.

2. Compute all first order right-hand factors in $\overline{k}(x)[\partial]$ of $\wedge^d f$.

3. In [55] a method (based on Plücker relations) is given for deciding which order 1 factors of $\wedge^d f$ correspond to order d right-hand factors of f.

4. Use these first order factors to compute the factors of f of order d. An efficient way to do this step is given in [14].

For operators of order 4 this approach works quite well, for order 5 it is already quite costly, and for higher order it is usually infeasible unless the coefficients are very small. Step 2 can be done by section 3.7, or by Beke's method (cf. section 3.4 and [6], see [13, 23, 42] for variations on Beke's method). We will give a number of strategies to speed up step 2.

First we apply the factorization method from chapter 5 on f. If this produces a non-trivial factorization then we have gained something, we can apply recursion on the factors. But if no factorization is found we gain something as well, because then we can conclude by lemma 24 below that if f is reducible in $\overline{k}(x)[\partial]$ then it is reducible in $k(x)[\partial]$ as well. Hence we only need to compute first order factors of $\wedge^d$ in $k(x)[\partial]$ instead of $\overline{k}(x)[\partial]$. This information removes the main bottleneck (which is splitting field computations) of Beke's method for computing factors of order 1. But we can gain even more as follows. We first try our algorithm in section 3.6 on all singularities p and all exponential parts e. Note that such computations are usually cheaper than computations with $\wedge^d f$ because $\wedge^d f$ is a much larger expression than f. If we are lucky and find a factorization, then we can apply recursion. But if no factorization was found, then we gain something as well, namely then we know that for all e, p if

$\mu_{e,p}(f) > 0$ then $\mu_{e,p}(L) > 0$ (otherwise a factorization would have been found) and in the same way $\mu_{e,p}(R) > 0$ (by applying the adjoint). Hence for every e, p we have $\mu_{e,p}(L) > 0$ if and only if $\mu_{e,p}(R) > 0$. The number of possible μ_* in section 3.4 that need to be considered in Beke's algorithm can be very large. However, with our information on the exponential parts of L and R we can skip a lot of different μ_*. The best case is if order$(f) = 4$. In this case L and R must be irreducible and have order 2 and furthermore $\mu_*(L) = \mu_*(R)$ (otherwise f would already have been factored). Then $\mu_*(R)$ is known, and hence by proposition 1 the type of $\partial + a_{d-1}$ is known (we had $R = \partial^d + a_{d-1}\partial^{d-1} + \cdots + a_0\partial^0$ and $d = 2$). We want to find $\partial + a_{d-1}$ as a right-hand factor of $\wedge^d f$, and since we know the only possible value of $\mu_*(\partial + a_{d-1})$ we can find $\partial + a_{d-1}$ by checking only 1 possibility in Beke's algorithm. So computing $\partial + a_{d-1}$ has been reduced to finding rational solutions. If order$(f) > 4$ then we can still significantly reduce the number of cases in Beke's algorithm in this way, but we can not reduce this number to 1 anymore.

Lemma 24 *If $f \in k(x)[\partial]$ is irreducible in $k(x)[\partial]$ then it is completely reducible in $\overline{k}(x)[\partial]$.*

An operator is called *completely reducible* if it is an LCLM of irreducible (in $\overline{k}(x)[\partial]$) operators. So any irreducible (in $\overline{k}(x)[\partial]$) operator is completely reducible as well.

Proof: Let f_1 be an irreducible right factor of f in $\overline{k}(x)[\partial]$. Let $f_1, \ldots, f_r$ be the conjugates (over the field extension $k \subset \overline{k}$) of f_1. Because conjugation commutes with differentiation we see that $f_1, \ldots, f_r$ are irreducible right factors of f. The Galois group of the extension $k \subset \overline{k}$ permutes the f_i hence LCLM$(f_1, \ldots, f_r)$ is invariant under this group. Then this LCLM is a factor of f in $k(x)[\partial]$ and hence equal to f because f is irreducible in this ring.

□

3.9 A bound for the degrees

Let $f \in k(x)[\partial]$ be given. Let $R = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0 \in \overline{k}(x)[\partial]$ be a right-hand factor of f. The topic of this section is to compute bounds for the degrees of the numerators and denominators of the a_i. These bounds are known when

- For every a_i and for every singularity p of f and the point $p = \infty$ we have a lower bound for the valuation of $l_p(a_i) \in \overline{k}((x))$.
- We have an upper bound for the number of *extra singularities.* A point $p \in \overline{k}$ is called an extra singularity of the factorization $f = LR$ if f is regular at p and R is singular at p.

The bounds in the first item are obtained from the relation $N(f) = N(L) + N(R)$ (cf. section 2.3.3). The valuation of the a_i at the extra singularities is also bounded by this relation. So all that is still needed is an upper bound for the number of extra singularities.

3.9.1 The number of extra singularities

It is known that the number of extra singularities can be bounded using *Fuchs' relation*. This relation says that the sum of the residues is zero (cf. lemma 26). In this section we will relate these residues to the list of generalized exponents. The list of generalized exponents of a right-hand factor R of f is a sublist of the list of generalized exponents of f. This gives us a method to bound the residues of R in the singular points of f. The residues at the extra singularities are negative integers. Hence, since the sum of the residues is zero, the number of extra singularities is bounded by the sum of the residues of R at the singularities of f. Note that the result in this section is similar to [7]. A difference is that we have a precise equation instead of a bound for $\mathrm{lres}(f)$ in lemma 27, resulting in a sharper bound for the number of extra singularities.

Definition 11 *Let $f = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0 \in k(x)[\partial]$ with $a_n \neq 0$. Let $p \in \overline{k}$. Then the* residue $\mathrm{res}_p(f)$ *of f at the point p is defined as the residue of a_{n-1}/a_n at the point p. The residue* $\mathrm{res}_\infty(f)$ *of f at ∞ is defined as the residue of $-x^2a_{n-1}/a_n$ at the point ∞.*

Let $f = a_n\delta^n + a_{n-1}\delta^{n-1} + \cdots + a_0\delta^0 \in k((x))[\delta]$ with $a_n \neq 0$. Define the local residue $\mathrm{lres}(f)$ *as the constant coefficient of $a_{n-1}/a_n \in k((x))$.*

Lemma 25 *Let $f \in k(x)[\partial]$. Let n be the order of f. If $p \in \overline{k}$ then $\mathrm{res}_p(f) = \mathrm{lres}(l_p(f)) + 1 + 2 + \cdots + (n-1)$ and if $p = \infty$ then $\mathrm{res}_p(f) = \mathrm{lres}(l_p(f)) - (1 + 2 + \cdots + (n-1))$.*

Proof: Without loss of generality we may assume that f is monic. Write $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$. Suppose $p \in \overline{k}$. Then $l_p(f) = \partial^n + l_p(a_{n-1})\partial^{n-1} + \cdots + l_p(a_0)\partial^0 = (\frac{1}{x}\delta)^n + l_p(a_{n-1})(\frac{1}{x}\delta)^{n-1} + \cdots + l_p(a_0)$. The coefficient of δ^n in this expression is $1/x^n$ and the coefficient of δ^{n-1} is $l_p(a_{n-1})/x^{n-1} - (1 + 2 + \cdots + (n-1))/x^n$. So $\mathrm{lres}(l_p(f))$ is the residue at $x = 0$ of $l_p(a_{n-1})$ (which is the same as the residue at $x = p$ of a_{n-1}) minus $1 + 2 + \cdots + (n-1)$ and hence the lemma holds for $p \in \overline{k}$.

Now suppose $p = \infty$. $l_p(f) = (-x\delta)^n + l_p(a_{n-1})(-x\delta)^{n-1} + \cdots$. The coefficient of δ^n in this expression is $(-x)^n$ and the coefficient of δ^{n-1} is $(-x)^{n-1}l_p(a_{n-1}) + (-x)^n(1 + 2 + \cdots + (n-1))$. So the local residue is -1 times the coefficient of x^1 in $l_p(a_{n-1}) \in k((x))$ (this coefficient equals the residue of $l_p(a_{n-1})/x^2$ at $x = 0$ and this equals the residue of x^2a_{n-1} at $x = \infty$) plus $1 + 2 + \cdots + (n-1)$.

□

Lemma 26 *Let $f, g \in k(x)[\partial]$ be monic and $p \in P^1(\overline{k})$. Then $\mathrm{res}_p(fg) = \mathrm{res}_p(f) + \mathrm{res}_p(g)$. If $p \in \overline{k}$ and f is regular at the point p then $\mathrm{res}_p(f) = 0$. Furthermore*

$$\sum_{p \in P^1(\overline{k})} \mathrm{res}_p(f) = 0$$

Proof: The proof of the first two statements is easy, we will skip it. Let $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$. The third statement is easy to prove if a_{n-1} is of the form $(x-p)^m$ for some $p \in \overline{k}$ and $m \in \mathbb{Z}$. Now the statement follows because every $a_{n-1} \in \overline{k}(x)$ is a $\overline{k}$-linear combination of such expressions $(x-p)^m$.

□

Note that the relation $\mathrm{res}_p(fg) = \mathrm{res}_p(f) + \mathrm{res}_p(g)$ need not hold without the restriction that g is monic (take for example $f = \partial$, $g = x^5\partial$ and $p = 0$).

Let $e_1, \ldots, e_n \in E$. Define $B(e_1, \ldots, e_n)$ as the constant term in the expression $\sum_i e_i + \sum_{j>i} v'(e_i - e_j)$, where v' is defined in lemma 19.

Lemma 27 *Let $f \in k((x))[\delta]$ and $e_1, \ldots, e_n$ the list of generalized exponents of f. Then* $\mathrm{lres}(f) = -B(e_1, \ldots, e_n)$.

Proof: $\mathrm{pp}(a_{n-1}) = -\sum_i \left(e_i + \sum_{j>i} v'(e_i - e_j)\right)$, cf. lemma 19. The local residue is the constant term of a_{n-1}. This equals the constant term of $\mathrm{pp}(a_{n-1})$, which is $-B(e_1, \ldots, e_n)$.

□

Lemma 28 *Suppose $f, L, R \in \overline{k}(x)[\partial]$ are monic, $f = LR$ and f is regular at the point $p \in \overline{k}$. Then R is singular at p if and only if $\mathrm{res}_p(R)$ is a negative integer.*

Proof: We may assume $p = 0$. Let v be the usual valuation on $\overline{k}((x))$. Let n be the order of R and $b_1, \ldots, b_n \in \overline{k}[[x]]$ be a basis of formal solutions of R such that the valuations $v(b_1), \ldots, v(b_n)$ is the list of generalized exponents of R. Because f is regular the list of generalized exponents of f is $0, 1, \ldots, \mathrm{order}(f) - 1$. The list of generalized exponents $v(b_1), \ldots, v(b_n)$ of R is a sublist of this. Hence $B(v(b_1), \ldots, v(b_n))$ is an integer $\geq 0+1+\cdots+(n-1)$. If R is regular then $B(v(b_1), \ldots, v(b_n)) = 0+1+\cdots+(n-1)$. Conversely, if $B(v(b_1), \ldots, v(b_n)) = 0+1+\cdots+(n-1)$ then (after a permutation) we have $v(b_i) = i-1$, $i = 1, \ldots, n$. Furthermore $b_i \in V(f) \subset \overline{k}((x))$. Hence by lemma 13 in chapter 2 it follows that R is regular.

So R is singular if and only if $B(v(b_1), \ldots, v(b_n)) > 0+1+\cdots+(n-1)$. $\mathrm{res}_0(R) = 1+\cdots+(n-1) - B(v(b_1), \ldots, v(b_n))$ hence this is a negative integer if and only if R is singular.

□

Let $f \in k(x)[\partial]$ and R a right-hand factor of order d. Let S be the set of singularities of f and the point ∞. Let T be the set of extra singularities of R. So R is regular outside $S \bigcup T$ and hence the residue of R is 0 outside $S \bigcup T$. We want to find an upper bound for the number $\#T$ of extra singularities. Since the sum of the residues of R is zero we have

$$\sum_{p \in S} (\mathrm{res}_p(R)) = -\sum_{p \in T} (\mathrm{res}_p(R)) \geq \#T.$$

$\mathrm{res}_p(R)$ is determined by the list of generalized exponents of R at p which is a sublist of the list of generalized exponents of f at the point p. So for every p we have finitely many possibilities for $\mathrm{res}_p(R)$.

We search for a bound for the integer values that $\sum_{p \in S} (\mathrm{res}_p(R))$ can have. This is a rather difficult problem if k is a complicated field. To simplify the problem we will substitute values for the parameters appearing in k to reduce the transcendence degree of k to 0. Then the problem is the following: for each point p we have lists of generalized exponents of f in $\overline{\mathbb{Q}}[x^{-1/n}]$ for some n. Each sublist determines one of the residues that R can have in the point p. Every combination of the possible residues at all $p \in S$ must be added to see if the result happens to be an integer and we must find a bound that integer. This can require computing in algebraic field extensions over $\mathbb{Q}$ of an enormous degree. So we must further simplify the problem (note that this simplification can lead to a possibly higher bound, so the step we will make is not always the best thing to do). This simplification can be done in several ways. One way to eliminate these algebraic numbers is to replace each algebraic number by its image under the following $\mathbb{Q}$-linear map:

$$\Psi : \overline{\mathbb{Q}} \to \mathbb{Q}.$$

$\Psi(a)$ is defined as the trace of a over the field extension $\mathbb{Q} \subset \mathbb{Q}(a)$ divided by the degree of this extension (one should take into account the fact that this may alter the $v'(e_i - e_j)$). Another way is to compute with floating point approximations.

Now we need not compute in complicated constants fields anymore, but one problem remains, namely we must check a large number of different possibilities. To reduce this number we can bound each residue (which is a rational number after having applied Ψ) separately, add all these rational numbers and take the largest integer which is $\leq$ this sum. Similarly one can compute a bound for the image of the residue under Ψ without checking all sublists of the list of generalized exponents.

3.10 Factorization in other rings

The Labahn-Beckermann algorithm can be used to factor in other rings as well. For example the commutative ring $\overline{k}(x)[y]$. An element f in this ring can be factored by computing an irreducible local factor $l \in \overline{k}((x))[y]$ of f and constructing an $R \in \overline{k}(x)[y]$ of minimal degree such that l is a factor of R, in the same way as in section 3.6.

Another example is the ring of difference operators $\overline{k}(x)[\tau]$ where $\tau \cdot x = (x+1) \cdot \tau$. The only place on $P^1(\overline{k})$ where we can study the difference operators locally is $x = \infty$ because all other places on $P^1(\overline{k})$ (a place on $P^1(\overline{k})$ is a valuation on $\overline{k}(x)$) are not invariant under τ. One can compute local factorizations and define exponential parts and generalized exponents for difference operators in a very similar way as for differential operators. So we can apply the method from section 3.6 to the ring $\overline{k}(x)[\tau]$ as well. In the differential case the completeness of our algorithm in section 3.7 depends on the fact that we can choose a suitable singularity to apply our method from section 3.5 to. However, for the ring $\overline{k}(x)[\tau]$ we can not always choose a suitable singularity because $x = \infty$ is the only point we can take. As a consequence, our factorization algorithm for $\overline{k}(x)[\tau]$ is incomplete, even for factors of order 1.

Chapter 4

An algorithm for computing invariants of differential Galois groups

The topic of this chapter is an algorithm for computing the invariants, of a given degree, for differential Galois groups of linear differential equations. This chapter is joint work with Jacques-Arthur Weil. It has been presented at the MEGA'96 conference. An extended version of this text has been submitted for publication.

4.1 Introduction

Let C be a field of characteristic 0 and denote $\overline{C}$ as the algebraic closure of C. Denote $k = \overline{C}(x)$ with the derivation $\partial = \frac{d}{dx}$. Let

$$L(y) = \sum_{i=0}^{n} a_i y^{(i)} = 0 \qquad a_n \neq 0$$

(where the a_i are polynomials in $C[x]$) denote a homogeneous linear differential equation. For such differential equations there is a differential Galois theory analogous to that for polynomial equations. By adjoining the solutions $V(L) \subset V$ and all their derivatives to k we get a differential field (recall that the universal extension V has no zero-divisors) extension $k \subset K$. Then the differential Galois group G of L is defined as the automorphism group of this differential field extension. G acts faithfully on the vector space $V(L)$, and so G can be viewed as a subgroup of $GL(V(L))$. G is an algebraic group, which means that it is a Zariski-closed subset of $GL(V(L))$. The group G contains all the information about the differential relations satisfied by the solutions of $L(y) = 0$ over k. One way to obtain information on G is to compute invariants. An invariant is an element of a symmetric power $Sym^m(V(L))$ that is left fixed by G.

Once a basis $y_1, \ldots, y_n$ of $V(L)$ is fixed, an element of $Sym^m(V(L))$ can be viewed as a homogeneous polynomial P of degree m in n variables $Y_1, \ldots, Y_n$ with coefficients in $\overline{C}$. The *value* of this $P \in \overline{C}[Y_1, \ldots, Y_n]$ is $P(y_1, \ldots, y_n)$. If P is left invariant by G then its value is in k, cf. section 4.2.1 below for more details. Given L and an integer m, the standard method for computing invariants of degree m is to construct an operator denoted as $L^{\circledS m}$ (which is called the m-th symmetric power of L) whose solution space is the set of values of all homogeneous $P \in \overline{C}[Y_1, \ldots, Y_n]$ of degree m, and then to search the rational (i.e. in $k = \overline{C}(x)$) solutions of this equation. Though there exists a good algorithm to compute rational solutions (cf. [1]), the coefficients of $L^{\circledS m}$ rapidly become dramatically big (see [60]). For order$(L) = 2$ this approach works fairly well ([58]). But for larger examples, the computation of these symmetric powers is often too complicated for our computers. To avoid this problem several authors have developed good necessary conditions (see [50] and references therein) by studying the local solutions at singularities of the equation.

In a similar spirit the first main ingredient of this chapter is that, at a singularity $x = 0$, L has a basis of formal solutions where each basis element has the form $\exp\left(\int e/x\right) s$. Here $e \in \overline{C}[x^{-1/r}]$ for some positive integer r and s is an element of $C((x))[e, \log(x)]$. By posing an extra condition on s (namely that the valuation of s is 0, cf. section 4.3) these e's are uniquely determined and are called the *generalized exponents* of L at $x = 0$. A study of these generalized exponents will provide the bounds needed for computing the invariants.

The second main ingredient of this chapter is the so-called Tannakian correspondence. This will allow us to view an invariant either as a polynomial in the solutions whose coefficients are a vector $\mathcal{C}$ of elements of $\overline{C}$ (which we will call a *vector invariant* of degree m), or as a differential polynomial whose coefficients are a vector F of rational functions (which we will call a *dual first integral*[1] of degree m).

From the first ingredient we derive in section 4.4.1 a heuristic that computes a $\overline{C}$-vector space that contains all vector invariants (plus perhaps some additional rubbish)[2]. Using the heuristic we can compute candidates for the invariants. Then we need to check if these candidates are indeed invariants. The main goal of this chapter is to be able to compute invariants even for cases where the computation of $L^{\circledS m}$ is too complicated for our computer. So we need to have a method to check correctness of our candidate invariants without computing this symmetric power. In section 4.4.2 we show that, by using the dual approach (i.e compute first integrals), we can check at a reasonable computational cost if a candidate provided by our heuristic is indeed an invariant. Combining the heuristic with this checking criterion gives an algorithm for computing invariants.

The first advantage of this algorithm is that it avoids the main bottleneck of the standard method (the computation of $L^{\circledS m}$). A second advantage is that, depending on the application, it is more convenient to have the invariant as a value, as a vector invariant, or as a dual first integral, and our checking algorithm provides these different forms (whereas the standard method provides only the rational value).

We would like to thank Elie Compoint, Marius van der Put and Felix Ulmer for stimulating conversations concerning the content of this chapter. We also thank Elie for swamping us with lots of complicated examples that helped us with the

[1]This is because such differential polynomials are first integrals of the dual system, cf. [59, 16].

[2]It is possible that the authors of [50] had such a heuristic in mind as well; most of the ideas that we use in the case of irregular singularities seem to be "known to specialists", though we never saw all of them written down completely.

implementation.

4.2 Invariants of differential Galois groups

In this section, we recall some basic facts about differential Galois groups and their invariants. The unfamiliar reader can consult [44, 33, 36, 9] for a more detailed introduction to differential Galois theory.

4.2.1 The classical theory

Using the universal extension (but also via other methods) one can show that for every linear homogeneous differential equation $L(y) = 0$ there exists a minimal extension $k \subset K$ of differential fields such that K contains a fundamental system of solutions of L. Such a field K is called a Picard-Vessiot extension of k. This extension plays the role of a splitting field for L. Using the fact that the field of constants $\overline{C}$ of k is algebraically closed, one can show that this extension is unique up to isomorphism (see [44, 33] and references therein). The group G of k-automorphisms of K that commute with the derivation is called the differential Galois group of L over k.

One can establish a Galois correspondence between the algebraic subgroups of G and the differential subfields of K ([44, 9]). In particular, an element of K is in k if and only if it is left fixed by G. The group acts naturally on all constructions on $V(L)$ obtained from the standard tools of linear algebra (tensor products, symmetric powers, direct sums, etc. see [36, 9, 46]) and can be characterized as the stabilizer of a line in some construction (Chevalley, [53]).

Definition 12 *An element v of $Sym^m(V(L))$ that is fixed by G is called an* invariant *of G.*
An element v in $Sym^m(V(L))$ that is sent to a constant multiple of itself by any element of G is called a semi-invariant *of G; this means that the one-dimensional vector space spanned by v is invariant under G.*

Suppose order$(L) = n$. Having chosen a basis $y_1, \ldots, y_n$ of $V(L)$, we may identify an invariant with a homogeneous polynomial in $\overline{C}[Y_1, \ldots, Y_n]$ (where $Y_1, \ldots, Y_n$ are variables on which G acts the same as on $y_1, \ldots, y_n$, see [31] for definition and properties of symmetric powers). An invariant given in this presentation will be called a *polynomial invariant*. The invariants of G form a $\overline{C}$-algebra.

Let P be an invariant of G, and $f = P(y_1, \ldots, y_n) \in K$. As P is an invariant, f is fixed by G. The differential Galois correspondence then implies that $f \in k$, so f is a rational function. We will call f the *value of the invariant P*. The expression of P depends on the choice of the basis of $V(L)$, but its value f is independent of this choice. For some applications, one just needs this value (for example to compute closed form solutions of the equation, see [49, 58]) and there, 'to compute an invariant' means 'to compute its value'.

The number of monomials of degree m is $\binom{n+m-1}{n-1}$. $L^{\circledS m}$ is the operator whose solution space is spanned by all monomials of degree m in the y_i. The order of $L^{\circledS m}$ is $\leq \binom{n+m-1}{n-1}$. It is $< \binom{n+m-1}{n-1}$ if and only if there is a non-zero $P \in \overline{C}[Y_1, \ldots, Y_n]$, homogeneous of degree m, having value 0. In this case it can happen that the value of a homogeneous polynomial P of degree m is in k even though P is not an invariant. If order$(L^{\circledS m}) = \binom{n+m-1}{n-1}$ then P is invariant if and only if its value is in k. See [48] for the construction and properties of $L^{\circledS m}$.

4.2.2 The invariants viewed as first integrals

This section we recall some results from [59, 60, 16]. Let Y_j denote the vectors $(y_j, y_j', \ldots, y_j^{(n-1)})$; they satisfy an n-dimensional first order system $Y' = AY$, where A is the companion matrix of L. The matrix U whose columns are the Y_j is a fundamental solution matrix for the system $Y' = AY$.

To simplify the writing, we denote by $y_{i,j}$ the entries of U (i.e. $y_{i,j} = y_j^{(i-1)}$). The solution space V_A of $Y' = AY$ is G-isomorphic with $V(L)$.

For a fixed j, let $Y = (y_{1,j}, \ldots, y_{n,j})$ be a solution of $Y' = AY$. If we consider a monomial μ of degree m in the $y_{i,j}$, then its derivative is a k-linear combination of monomials of degree m in the $y_{i,j}$. As there are $N = \binom{n+m-1}{n-1}$ such monomials, the vectors $w = (y_{1,j}^m, \ldots, y_{n-1,j}y_{n,j}^{m-1}, y_{n,j}^m)$ of all such monomials satisfy an $N \times N$ system which we denote by $Y' = S^m(A)Y$. It follows from the construction that the solution space of the system $Y' = S^m(A)Y$ is G-isomorphic with $Sym^m(V_A)$, the m-th symmetric power of V_A.

Remark: Note that the matrix $S^m(A)$ is easy to construct from a computational point of view (its entries are entries of A multiplied by integers), and that it is sparse. In fact, to construct $L^{\circledS m}$ means to build $S^m(A)$ and then convert it to an equation by a cyclic vector process. It is this conversion that makes the construction of $L^{\circledS m}$ costly.

To have a fundamental solution matrix of $Y' = S^m(A)Y$, we build the *m-th symmetric power matrix* $Sym^m(U)$ the following way. Let $v_i = \sum_{j=1}^n c_j y_{i,j}$ for $i = 1, \ldots, n$ where c_j are arbitrary constants (note that they are the same for all v_i). For r ranging from 1 to N, construct the r-th monomial μ_r in the v_i (for the lexicographic order with $v_1 > \ldots > v_n$). Then, for s ranging from 1 to N, $Sym^m(U)_{r,s}$ is found from μ_r by taking the coefficient of the s-th monomial in the c_j (for the lexicographic order with $c_1 > \ldots > c_n$).

Lemma 29 *The symmetric power matrix $Sym^m(U)$ is is a fundamental solution matrix for $Y' = S^m(A)Y$ and its columns can be identified with a basis of $Sym^m(V_A)$.*

Proof: Follows from the construction.

□

Remark: In the sequel, the notation $Sym^m(U)$ denotes the symmetric power of a matrix, whereas $S^m(A)$ denotes the differential system whose solution space is the symmetric power of the solution space of $Y' = AY$; this is not the same construction and this is why we must use a different notation.

As the solution space of $Y' = S^m(A)Y$ is isomorphic with $Sym^m(V_A)$, the system $Y' = S^m(A)Y$ has a non-zero solution of which all entries are rational if and only if

G has an invariant of degree m. This yields the following two ways of representing the invariants:

Definition 13 *Let $Y' = AY$ be a first order system (with $A \in \mathcal{M}_n(k)$), and let U denote a fundamental solution matrix. For $m \in \mathbb{N}$ put $N = \binom{n+m-1}{n-1}$.*
For any $\mathcal{C} \in \overline{C}^N \setminus \{0\}$ we form the vector $F := Sym^m(U)\mathcal{C} \in K^N$.
We say that $\mathcal{C} \in \overline{C}^N$ is a vector invariant *and that $F := Sym^m(U)\mathcal{C}$ is a* dual first integral *if $F \in k^N$.*

Remark: This correspondence may seem a little bit miraculous. However, one can see from the construction that, as the elements of the Galois group commute with the derivation, they act the same on all rows of $Sym^m(U)$.

Any rational solution of $Y' = S^m(A)Y$ is a dual first integral. To connect this with the polynomial invariants, let $Sym^m(U)_i$ denote the i-th row of $Sym^m(U)$. As the entries of the first row of $Sym^m(U)$ are the monomials of degree m in the solutions y_i of L (with an integer coefficient), we see that $Sym^m(U)_1\mathcal{C}$ is a homogeneous polynomial in the y_i that takes a rational value. The next lemma (cf. e.g. [16, 9]) shows that the corresponding polynomial in the indeterminates Y_i is an invariant of G.

Lemma 30 *A polynomial $P \in \overline{C}[Y_1, \ldots, Y_n]$ is a polynomial invariant of degree m of G if and only if for some $n\times n$ matrix $\mathcal{V}$ whose first row is formed by the indeterminates Y_i, there exists $\mathcal{C} \in \overline{C}^N$ such that $P = Sym^m(\mathcal{V})_1\mathcal{C}$ and that $F := Sym^m(U)\mathcal{C}$ is a dual first integral (i.e $F \in k^N$).*

Proof: see [16].

□

It is equivalent to determine invariants, vector invariants, or dual first integrals from a theoretical point of view. However, it is not equivalent from a computational point of view. We will design below a good heuristic for computing candidate vector invariants. From these vector invariants we will obtain the candidate dual first integral and then it will be simple to check if a candidate is indeed a dual first integral.

One advantage of working with systems is that the construction of symmetric powers is easy to perform (and thus it is easy to check if some given vector is a solution of such a system). Another advantage is that the dual first integrals are independent of the choice of basis of $V(L)$ (whereas vector invariants depend on this choice).

For any point $x_0 \in P^1(\overline{C})$, the system has a local formal fundamental solution matrix $\hat{U}$. The system has a dual first integral F if and only if there exists $\mathcal{C} \in \overline{C}^N$ such that $Sym^m(\hat{U})\mathcal{C} = F$. We will use this in section 4.4 to compute F.

4.3 Bounds on exponents using generalized exponents

When computing rational solutions of a differential operator L one first computes a lower bound for the integer exponents of L at each point $x_0 \in P^1(\overline{C})$. We would like to compute rational solutions of symmetric powers (and other constructions) of differential operators. In the regular singular case [50] gives the bound for the integer exponents of $L^{\circledS m}$ in terms of the exponents of L. In the irregular singular case, however, we can not obtain a bound for the integer exponents of $L^{\circledS m}$ from the exponents of L. The reason is that in this case there are "too few exponents". More precisely: in the irregular singular case there are, counted with multiplicity, less than order(L) exponents. To handle this difficulty we will use the generalization of exponents from chapter 3. An alternative way to get a bound (a different bound than ours) is found in lemma 3.3 in [46] using a different generalization of exponents in [7]. For convenience of notation we will now assume that the point of interest is the point $x = 0$. Then L in $C(x)[\partial]$ is viewed as an element of the ring $C((x))[\delta] = C((x))[\partial]$ where $\delta = x\partial$.

4.3.1 A few preliminaries

In this section we list a few known facts about differential operators that we will use in later sections.

Definition 14 *The* exponents *of L are those elements $e \in \overline{C}$ for which there is a solution of L of the form*

$$x^e s \quad \text{where} \quad s \in \overline{C((x))}[\log(x)] \quad \text{with} \quad v(s) = 0.$$

For the definition of the valuation $v(s)$ see chapter 3.

The following is a well-known property of exponents. It is generalized in proposition 2.

Lemma 31 *An element $e \in \overline{C}$ is an exponent of L if and only if e is a root of $N_0(L)$.*

Definitions and properties of Newton polygons and polynomials can be found in [35, 54, 3] and chapter 2. Note: In the literature exponents are often also called *indices*, and the Newton polynomial $N_0(L)$ is then called the *indicial polynomial* or *indicial equation.*

Recall the definition in chapter 2 of $\mathrm{Exp}(e)$ for $e \in \overline{C((x))}$ as

$$\mathrm{Exp}(e) = \exp(\int \frac{e}{x} dx)$$

and the substitution map

$$S_e : \overline{C((x))}[\delta] \rightarrow \overline{C((x))}[\delta]$$

for $e \in \overline{C((x))}$ as the $\overline{C((x))}$-homomorphism that maps δ to $\delta + e$.

$\mathrm{Exp}(e)$ is a solution of the operator $\delta - e$. For rational numbers q we have

$$\mathrm{Exp}(q) = x^q \in \overline{C((x))}.$$

Furthermore

$$\mathrm{Exp(e)} \in C((x)) \Longleftrightarrow e \in \mathbb{Z} + x \cdot C[[x]]$$

and

$$\mathrm{Exp(e)} \in \overline{C((x))} \Longleftrightarrow e \in \bigcup_r (\frac{1}{r}\mathbb{Z} + x^{1/r} \cdot \overline{C} \cdot C[[x^{1/r}]]) \subset \overline{C((x))}.$$

Here $\overline{C} \cdot C[[x^{1/r}]]$ denotes the smallest sub-ring of $\overline{C((x))}$ that contains both $C[[x^{1/r}]]$ and $\overline{C}$. Exp behaves like an exponential function:

$$\mathrm{Exp}(e_1 + e_2) = \mathrm{Exp}(e_1)\mathrm{Exp}(e_2).$$

The substitution map has the following well-known property: $\mathrm{Exp}(e)y$ is a solution of L if and only if y is a solution of $S_e(L)$.

4.3.2 Generalized exponents reviewed

Using the substitution map, one can rewrite the standard property of exponents (lemma 31) as follows:

Lemma 32 *Let $L \in C((x))[\delta] \setminus \{0\}$. An element $e \in \overline{C}$ is an exponent of L if and only if 0 is a root of the Newton polynomial $N_0(S_e(L))$.*

With this lemma in mind, we can generalize the exponents by replacing the set $\overline{C}$ by a larger set of exponents

$$E = \bigcup_r \overline{C}[x^{-1/r}].$$

Let $L \in \overline{C((x))}[\delta] \setminus \{0\}$. For an element $e \in E$ the number $\nu_e(L)$ is defined in chapter 3 as the multiplicity of the root 0 in $N_0(S_e(L))$.
$e \in E$ is called a *generalized exponent* of L if $\nu_e(L) > 0$. The number $\nu_e(L)$ is called the multiplicity of the generalized exponent e in the operator L.

Remark: In an older version of chapter 3 the generalized exponents were called canonical exponential parts. This name is no longer used, it is now called generalized exponent. The reason for choosing this name is to point out the use of this notion, which is to generalize methods that use exponents (for example: [50]) to the irregular singular case. Alternative approaches are found in the literature (e.g. [15, 38]). The exponents are those generalized exponents that are in $\overline{C}$.

Computing the generalized exponents can be done using one of the several factorization algorithms. It is a subproblem of computing formal solutions, so the generalized exponents can be computed using a part of the algorithm for computing formal solutions, cf. [54, 3]. We use "algorithm semi-regular parts" in chapter 2. This algorithm is a modified version of Malgrange's factorization algorithm [35]. It uses a different type of ramifications (obtained from [3]) to minimize the algebraic extensions.

The relation between generalized exponents and formal solutions is the following (this is theorem 4 in chapter 3):

Proposition 2 *Let $L \in C((x))[\delta] \setminus \{0\}$. An element $e \in E$ is a generalized exponent of L if and only if L has a solution of the form*

$$\mathrm{Exp}(e)s \quad \text{where} \quad s \in \overline{C((x))}[\log(x)] \quad \text{and} \quad v(s) = 0.$$

Note: Instead of using a Newton polynomial the generalized exponents can be defined from the formal solutions using this proposition. A different generalization of exponents by using formal solutions is found in [7].

4.3.3 Minimal exponents

As already mentioned, our reason for using generalized exponents was to obtain information about the exponents of $L^{\circledS m}$ without computing the operator $L^{\circledS m}$. Now a natural question arises: Given the generalized exponents of L at the point $x = 0$, can we determine all (generalized) exponents of $L^{\circledS m}$? One easily finds a counter-example to this: at the point $x = 0$ the operators $\partial^3 + x$ and $\partial^3 + x + 1$ have the same generalized exponents (the generalized exponents are in fact exponents in this example), but their second symmetric powers do not. So instead of trying to find all generalized exponents of the symmetric powers of L we will settle for a different goal, namely to compute the *minimal generalized exponents.*

Definition 15 *Let r be a positive integer. Define the following partial ordering $\leq_r$ on E*

$$e_1 \leq_r e_2 \Longleftrightarrow e_1 - e_2 \in \frac{1}{r}\mathbb{Z} \text{ and } e_1 - e_2 \leq 0.$$

For a set $S \subset E$ define $\min_r(S)$ as the set of minimal elements of S with respect to the ordering $\leq_r$.
For an element $L \in C((x))[\delta] \setminus \{0\}$ define $\min_r(L)$ as $\min_r(S)$ where S is the set of generalized exponents of L.

If L has an integer exponent $e \in \mathbb{Z}$ then $\min_r(L) \bigcap \frac{1}{r}\mathbb{Z}$ contains 1 element. This element is $\leq e$. So if we can compute $\min_r$ for symmetric powers of L then we find lower bounds for the integer exponents of these symmetric powers. For this we use the following

Proposition 3 *Let L_1 and L_2 be non-zero elements of $C((x))[\delta]$. Let r be the least common multiple of all ramification indices of the generalized exponents of L_1 and L_2. For sets $S_1, S_2 \subset E$ define the sum $S_1 + S_2 = \{s_1 + s_2 | s_1 \in S_1, s_2 \in S_2\} \subset E$. Then*

$$\min_r(L_1 \circledS L_2) = \min_r(\min_r(L_1) + \min_r(L_2)).$$

The *symmetric product* of $L_1 \circledS L_2$ is defined as the monic operator of minimal order such that $y_1 y_2 \in V(L_1 \circledS L_2)$ for all $y_1 \in V(L_1)$, $y_2 \in V(L_2)$. Strictly speaking this is not a mathematically correct name, we use this name because of the resemblance with the symmetric power construction $L^{\circledS m}$.

Corollary 1 *Let m be a positive integer and r the least common multiple of the ramification indices of L. Denote for $S \subset E$ the set $m \cdot S$ as $S + S + \cdots + S$ (m times). Then*

$$\min_r(L^{\circledS m}) = \min_r(m \cdot \min_r(L)).$$

In particular if $L^{\circledS m}$ has an integer exponent e then $\min_r(m \cdot \min_r(L)) \bigcap \frac{1}{r}\mathbb{Z}$ contains 1 element which is a lower bound for e. This lower bound can be computed from r, m and $\min_r(L)$.

We postpone the proof of the proposition till after the proof of theorem 5 below. To prove this theorem we first need to introduce some notations.

Remark: The fact that such a lower bound exists is not new (lemma 3.3 in [46]). However, the bound in our proposition is sharper. It gives precisely the smallest exponent of $L^{\circledS m}$ in $\frac{1}{r}\mathbb{Z}$. So in case all ramification indices are 1 (i.e. $r = 1$) our bound for the smallest integer exponent is sharp.

Recall that V is the *linear universal extension* of $C((x))$ as in chapter 2, and $V_e = \mathrm{Exp}(e) \cdot (\overline{C} \cdot C((x))[e])[\log(x)]$. We have $V_{e_1} = V_{e_2}$ if and only if $e_1 \sim e_2$ and (cf. theorem 3 in chapter 2)

$$V = \bigoplus_{e \in E/\sim} V_e. \tag{4.1}$$

Now define

$$E_r = \overline{C}[x^{-1/r}] \subset E.$$

and

$$V_{*,r} = \bigoplus_{e \in E_r/\sim} V_e.$$

For $e \in E_r$ define

$$V_{e,r} = \mathrm{Exp}(e) \cdot (\overline{C} \cdot C((x^{1/r})))[\log(x)].$$

If $e_1 - e_2 \in \frac{1}{r}\mathbb{Z}$ then $V_{e_1,r} = V_{e_2,r}$ so $V_{e,r}$ is also defined for $e \in E_r/(\frac{1}{r}\mathbb{Z})$. $V_{e,r}$ is the direct sum of the V_{e_1} taken over all $e_1 \in E_r/\sim$ for which e is congruent with e_1 modulo $\frac{1}{r}\mathbb{Z}$. Hence by the direct sum in equation (4.1) it follows that

$$V_{*,r} = \bigoplus V_{e,r} \tag{4.2}$$

where the sum is taken over all $e \in E_r/(\frac{1}{r}\mathbb{Z})$.

From theorem 3 in chapter 2 it follows that $V(L) \subset V_{*,r}$ if and only if the ramification indices of every generalized exponent of L divide the integer r. Now $V_{*,r}$ is closed under differentiation, addition and multiplication. Hence if for operators L_1 and L_2 all ramification indices divide r, then the same holds for $L_1^{(1)}$ (for a definition see lemma 33), for $L_1 \circledS L_2$ and for $\mathrm{LCLM}(L_1, L_2)$.

Theorem 5 *Let $L \in C((x))[\delta] \setminus \{0\}$ be of order d and let r be a positive integer. Suppose that the ramification indices of the generalized exponents divide the integer r.*

1. *There exists a basis $y_1, \ldots, y_n$ of $V(L)$ which satisfies the following condition*

$$y_i = \mathrm{Exp}(e_i) s_i \ \text{ for some } \ s_i \in (\overline{C} \cdot C((x^{1/r})))[\log(x)],\ v(s_i) = 0 \tag{4.3}$$

   where $e_1, \ldots, e_n \in E$.

2. *Suppose $y_1, \ldots, y_n$ is a basis of the solution space $V(L)$ which satisfies condition (4.3). Then*

$$\min_r(L) = \min_r(\{e_1, \ldots, e_n\}).$$

Proof: Let $e \in \min_r(L)$. Since $\{e_1, \ldots, e_n\}$ is a subset of the set of all generalized exponents of L (there are at most $\text{order}(L) = d$ different generalized exponents) it follows that the number of elements in $\min_r(\{e_1, \ldots, e_n\})$ can not be larger than the number of elements in $\min_r(L)$. So we only need to prove that $e \in \min_r(\{e_1, \ldots, e_n\})$. Without loss of generality we may assume that $e_i - e \in \frac{1}{r}\mathbf{Z}$ for $i \leq t$ and $e_i - e \notin \frac{1}{r}\mathbf{Z}$ for $i > t$. We need to show that $t \neq 0$ and that there is one $i \leq t$ with $e_i - e \leq 0$. Then the theorem is proven as follows: We may assume that $e_i - e \in \frac{1}{r}\mathbf{Z}$ is minimal, so $e_i \in \min_r(\{e_1, \ldots, e_n\})$. Because of the minimality of e we can not have $e_i - e < 0$ hence $e = e_i$.

In the basis $y_1', \ldots, y_n'$ of formal solutions in section 2.8.2 each basis element can be written in the form y_i' is a constant times $\text{Exp}(e_i')s_i'$ with $s_i' \in C((x))[e_i', \log(x)]$ and $v(s_i') = 0$. Furthermore (see also the proof of theorem 4 in chapter 3) every generalized exponent e_i' of L occurs. This basis satisfies condition (4.3) because $C((x))[e_i', \log(x)] \subset (\overline{C} \cdot C((x^{1/r})))[\log(x)]$. Furthermore the generalized exponent e of L occurs in this basis. So one of the elements of this basis is of the form $y = \text{Exp}(e)s$ (with $s \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ and $v(s) = 0$). Then $y \in V_{e,r}$ and $y \in V(L)$.

Because of condition (4.3) each y_i is an element of $V_{e_i,r}$. Since the y_i form a basis of $V(L)$ it follows that y is a $\overline{C}$-linear combination of $y_1, \ldots, y_n$. Because of the direct sum in equation (4.2) it follows that y is a linear combination of $y_1, \ldots, y_t$, since e_i for $i > t$ is not equal to e modulo $\frac{1}{r}\mathbf{Z}$ and so y_i is in a different component than $V_{e,r}$ for $i > t$. Dividing by $\text{Exp}(e)$ it follows that $s \in V_{0,r} = (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ is a linear combination of the $\text{Exp}(e_i - e)s_i \in V_{0,r}$ for $i \leq t$. Hence the valuation of at least one of the $\text{Exp}(e_i - e)s_i$ is $\leq v(s) = 0$. The valuation of the s_i is 0 and the valuation of $\text{Exp}(e_i - e) \in C((x^{1/r}))$ is $e_i - e$. So for at least one $i \leq t$ we have $e_i - e \leq 0$ and so the theorem follows.

$\square$

Remark: Without the condition $s_i \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ the statement need not hold. Take for example $L = \delta^2 - \frac{1}{2}\delta$ and $r = 1$. Then $\min_r(L) = \{0, \frac{1}{2}\}$. Now take $e_1 = e_2 = 0$, $s_1 = 1$ and $s_2 = 1 + x^{1/2}$. Then s_2 does not satisfy condition (4.3) and $\min_r(L) \neq \min_r(\{e_1, e_2\}) = \{0\}$.

Remark: The existence result i) is also found in [15] (in a different terminology, though).

Proof of proposition 3: Let $y_i = \text{Exp}(e_i)s_i$, $i = 1, \ldots, \text{order}(L_1)$ be a basis of $V(L_1)$ and $y_j' = \text{Exp}(e_j')s_j'$, $j = 1, \ldots, \text{order}(L_2)$ be a basis of $V(L_2)$ that both satisfy condition (4.3). Then the products $y_i y_j'$ span $V(L_1 \circledS L_2)$. Let S be a set of pairs (i, j) such that $\{y_i y_j' | (i, j) \in S\}$ is a basis for $V(L_1 \circledS L_2)$. Now $y_i y_j' = \text{Exp}(e_i + e_j')s_i s_j'$ and $s_i s_j' \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ with $v(s_i s_j') = 0$. Hence by theorem 5 it follows that $\min_r(L_1 \circledS L_2) = \min_r(\{e_i + e_j' | (i, j) \in S\})$.

Now $\{e_i + e_j' | (i, j) \in S\}$ is a subset of the set T of all $e_i + e_j'$. So for each $e \in \min_r(\{e_i + e_j' | (i, j) \in S\})$ there must be precisely one $e' \in \min_r(T)$ such that $e' \leq_r e$. Furthermore T is a subset of the set of all generalized exponents of $L_1 \circledS L_2$. Hence for each $e' \in \min_r(T)$ there must be precisely one $e \in \min_r(L_1 \circledS L_2) = \min_r(\{e_i + e_j' | (i, j) \in S\})$ such that $e \leq_r e'$. Then it follows that $\min_r(T)$ equals $\min_r(L_1 \circledS L_2)$.

□

Lemma 33 *Let* $L \in C((x))[\delta]$ *be non-zero and let* r *be the least common multiple of the ramification indices of* L. *Let* $L^{(1)}$ *be the monic differential operator defined by* $V(L^{(1)}) = \{\frac{dy}{dx} | y \in V(L)\}$.
If $0 \notin \min_r(L)$ *then*

$$\min_r(L^{(1)}) = \{e + v(e) - 1 | e \in \min_r(L)\}.$$

If $0 \in \min_r(L)$ *then*

$$\min_r(L^{(1)}) = \{m\} \bigcup \{e + v(e) - 1 | e \in \min_r(L) \setminus \{0\}\}$$

where $m \in \mathbb{Z}$, $m \geq -1$, *or*

$$\min_r(L^{(1)}) = \{e + v(e) - 1 | e \in \min_r(L) \setminus \{0\}\}.$$

Note that $\mathrm{order}(L) - \mathrm{order}(L^{(1)})$ is the dimension of the kernel of $\frac{d}{dx}$ on $V(L)$. So $\mathrm{order}(L^{(1)}) = \mathrm{order}(L) - 1$ if $1 \in V(L)$ and $\mathrm{order}(L^{(1)}) = \mathrm{order}(L)$ otherwise.

Proof: If $y = \mathrm{Exp}(e)s$ where $s \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ with $v(s) = 0$ and $e \neq 0$ then the derivative y' is of the form $\mathrm{Exp}(e + v(e) - 1)t$ for some $t \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ with $v(t) = 0$. Now the first statement follows by applying theorem 5.

For the second statement we note that $\nu_0(L) > 0$ means that there is a formal solution $y \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ of L with $v(y) = 0$. The valuation of the derivative y' is ∞ or is an integer ≥ -1. Now distinguish the two cases: $v(y') \in \min_r(L^{(1)})$ (then: $v(y')$ is an integer $m \geq -1$) or $v(y') \notin \min_r(L^{(1)})$ (then the other case holds).

□

In the case $0 \in \min_r(L)$ one can get a slightly stronger statement about $\min_r(L^{(1)})$ by noting that $-1 \in \min_r(L^{(1)})$ if and only if $\nu_0(L) > 1$. We will not use this small improvement of the lemma.

As in chapter 3, define $v' : E \to \mathbb{Q}$ as follows: $v'(e) = v(e)$ for all $e \in E \setminus \{0\}$ and $v'(0) = 0$. It follows from the lemma that for each $e \in \min_r(L^{(1)})$ there is an $e' \in \min_r(L)$ such that $e - (e' + v'(e') - 1)$ is a non-negative integer.

Denote $L^{(i)}$ as the monic operator of which the solution space consists of the i-th derivatives of the elements of $V(L)$. By repeated application of the lemma it follows that for each $e \in \min_r(L^{(i)})$ there is an $e' \in \min_r(L)$ such that $e - (e' + i \cdot v'(e') - i)$ is a non-negative integer.

Corollary 2 *Let* L *be a non-zero differential operator in* $C((x))[\delta]$ *and let* r *be the least common multiple of the ramification indices of the generalized exponents of* L. *Let* $m_0, \ldots, m_{n-1}$ *be non-negative integers and* M *the symmetric product of the operators* $(L^{(i)})^{\circledS m_i}$. *Let* $B_i = \{e + i \cdot v'(e) - i\} | e \in \min_r(L)\}$ *and* $B = m_0 \cdot B_0 + \cdots + m_{n-1} \cdot B_{n-1}$. *Suppose* M *has a non-zero solution* y *in* $(\overline{C} \cdot C((x^{1/r})))[\log(x)]$. *Then* $B \bigcap \frac{1}{r}\mathbb{Z}$ *contains an element* $\leq v(y)$.

This provides a lower bound for the valuation of solutions in $(\overline{C} \cdot C((x^{1/r})))[\log(x)]$ of M. It can be computed from $m_0, \ldots, m_{n-1}$, r and $\min_r(L)$.

To compute the bound we need to compute the set of sums $m_0 \cdot B_0 + \cdots + m_{n-1} \cdot B_{n-1}$ and to take the smallest element which is in $\frac{1}{r}\mathbb{Z}$. This means computing in a splitting field; it is not sufficient to take only one generalized exponent in each conjugacy class of generalized exponents. One can try to avoid splitting fields for computing this bound by various tricks (for example floating point computations) but we will not go into this.

Procedure global-bounds
Input: $L \in C(x)[\partial]$ and non-negative integers $m_0, \ldots, m_{n-1}$
Output: A rational function $Q \in C(x)$ and an integer N such that every rational solution $y \in \overline{C}(x)$ of $M = (L^{(0)})^{\circledS m_0} \circledS \cdots \circledS (L^{(n-1)})^{\circledS m_{n-1}}$ can be written as the product of Q and a polynomial in x of degree $\leq N$.

1. Denote $n = \mathrm{order}(L)$ and $L = a_n\partial^n + \cdots + a_0\partial^0$. After multiplication on the left by an element of $C(x)$ we may assume that $a_i \in C[x]$ with $\gcd(a_0, \ldots, a_n) = 1$.
2. Factor a_n in $C[x]$.
3. $Q := 1$.
4. For each irreducible factor $p \in C[x]$ of a_n do
   (a) Let $\alpha \in \overline{C}$ be a root of p.
   (b) Let l_α be the $\overline{C}$-automorphism of $\overline{C}(x)[\partial]$ given by $l_\alpha(x) = x + \alpha$ and $l_\alpha(\partial) = \partial$, as in chapter 3. This transformation moves the point $x = \alpha$ to the point $x = 0$. Compute $l_\alpha(L)$.
   (c) Compute the generalized exponents of $l_\alpha(L)$ at the point $x = 0$.
   (d) Let r be the least common multiple of the ramification indices of the generalized exponents and compute the $\min_r$ of the set of generalized exponents.
   (e) Compute the set B in corollary 2.
   (f) If $B \bigcap \frac{1}{r}\mathbb{Z}$ is empty then stop the algorithm and return the following output: $Q = 0$ and $N = 0$.
   (g) Let $b_\alpha \in \mathbb{Z}$ be the smallest element of $B \bigcap \frac{1}{r}\mathbb{Z}$, rounded above to an integer.
   (h) Replace Q by $Q \cdot p^{b_\alpha}$.
5. Let l_∞ be a $\overline{C}$ automorphism of $\overline{C}(x)[\partial]$ given by $l_\infty(x) = 1/x$ and $l_\infty(\partial) = -x^2\partial$. This transformation moves the point infinity to the point $x = 0$. Compute $l_\infty(L)$.
6. Compute the generalized exponents of $l_\infty(L)$.
7. Let r be the least common multiple of the ramification indices of the generalized exponents and compute the $\min_r$ of the set of generalized exponents.
8. Compute the set B in corollary 2.
9. If $B \bigcap \frac{1}{r}\mathbb{Z}$ is empty then stop the algorithm and return the following output: $Q = 0$ and $N = 0$.

10. Let $b_\infty \in \mathbb{Z}$ be the smallest element of $B \bigcap \frac{1}{r}\mathbb{Z}$, rounded above to an integer.
11. Add $2 \cdot (0 \cdot m_0 + 1 \cdot m_1 + \cdots + (n-1) \cdot m_{n-1})$ to b_∞.
12. Let N be $-b_\infty$ plus the valuation of Q at infinity (this valuation is the degree of the denominator of Q minus the degree of the numerator of Q).
13. **Output:** Q and N.

Remark: Note that even if $Q = N = 0$ there may still be an invariant (whose value is zero); see the Hurwitz example in the next section for an illustration.

The fact that the algorithm works follows from the following observations:

- For $\alpha \in \overline{C}$ the map $l_\alpha : \overline{C}(x) \to \overline{C}(x)$ given by $l_\alpha(x) = x + \alpha$ is an automorphism of $\overline{C}(x)$ as a differential field because $\frac{d}{dx} = \frac{d}{d(x+\alpha)}$. Hence by defining $l_\alpha(\partial) = \partial$ this l_α is extended to an automorphism of $\overline{C}(x)[\partial]$. However, l_∞ given by $l_\infty(x) = 1/x$ is not an automorphism of $\overline{C}(x)$ as a differential field; $\frac{d}{d(1/x)} = -x^2 \frac{d}{dx}$. One can check that by defining $l_\infty(\partial) = -x^2\partial$ we obtain an automorphism of $\overline{C}(x)[\partial]$.
- By the valuation of $f \in \overline{C}(x)$ at $x = \alpha$ for $\alpha \in P^1(\overline{C})$ we mean the valuation of $l_\alpha(f) \in \overline{C}((x))$. Let $\alpha \in P^1(\overline{C}) = \overline{C} \bigcup \{\infty\}$. Then $f \in \overline{C}(x)$ is a rational solution of a differential operator M if and only if $l_\alpha(f)$ is a rational solution of $l_\alpha(M)$. So computing a lower bound for the valuation of rational solutions of M at $x = \alpha$ is the same as computing a lower bound for the valuation of rational solutions of $l_\alpha(M)$ at $x = 0$.
- Computing the function $Q \in \overline{C}(x)$ and the number N is equivalent with computing a lower bound b_α for the valuations of rational solutions of M at all $\alpha \in P^1(\overline{C})$ (assuming that b_α is non-zero for only finitely many α).
- If L is regular at a point $x = \alpha$ where $\alpha \in \overline{C}$ then M need not be regular at $x = \alpha$. However, all local solutions of L at $x = \alpha$ are analytic. Products, sums and derivatives of analytic functions are analytic hence all local solutions of M at $x = \alpha$ are analytic. In particular, 0 is a lower bound for the valuation of the solutions at $x = \alpha$. Hence we only need to compute a bound b_α at the singularities of L and the point ∞.
- Because algebraic conjugation over C is an automorphism of the differential field $\overline{C}(x)$, it follows that if $\alpha_1, \alpha_2 \in \overline{C}$ are conjugate over C then the two bounds $b_{\alpha_1}, b_{\alpha_2} \in \mathbb{Z}$ will be the same. Hence we need to take only one α in every conjugacy class of the singularities of L. In other words: We need to compute the bound for only one root of each factor of a_n in $C[x]$. Furthermore the function $Q \in \overline{C}(x)$ will be an element of $C(x)$.
- Note that for all $\alpha \in P^1(\overline{C})$ the map l_α on $\overline{C}(x)[\partial]$ commutes with taking symmetric products and LCLM's (least common left multiples) because the map l_α on $\overline{C}(x)$ commutes with multiplication and addition. However, l_α does not commute with derivation if $\alpha = \infty$. So l_α only commutes with the construction

$L \mapsto L^{(1)}$ on $\overline{C}(x)[\partial]$ if $\alpha \in \overline{C}$. The solution space of $l_\infty(L^{(1)})$ equals x^2 times the solution space of $(l_\infty(L))^{(1)}$. So the valuations are 2 higher than in lemma 33. For the point $x = \infty$ there is a lemma similar to lemma 33 with the following differences: $e + v'(e) - 1$ is replaced by $e + v'(e) + 1$ and $m \geq -1$ is replaced by $m \geq 1$. We need a different corollary 2 specifically for the point $x = \infty$, i.e. for operators $L \in C((\frac{1}{x}))[\partial]$ instead of $L \in C((x))[\partial]$. The only difference will be that $e+i\cdot v'(e)-i$ needs to be replaced by $e+i\cdot v'(e)+i$. The algorithm computes the bound given by corollary 2 and then adds $2\cdot(0\cdot m_0+1\cdot m_1+\cdots+(n-1)\cdot m_{n-1})$ to correct for this difference.

The PSL_3 example: The following example was adapted from N. Katz by Elie Compoint ([16]). Let $\delta = x\frac{d}{dx}$ and

$$L = \delta(\delta - \frac{1}{2})(\delta - \frac{1}{4})(\delta + \frac{1}{4})(\delta - \frac{1}{8})(\delta - \frac{5}{8})(\delta + \frac{1}{8})(\delta + \frac{5}{8}) - x(\delta + \frac{1}{3})(\delta - \frac{1}{3}).$$

We want to compute the invariants of degree 2 and 3. The generalized exponents (which are in fact exponents) of L at $x = 0$ are $-5/8, -1/4, -1/8, 0, 1/8, 1/4, 1/2$ and $5/8$. So the ramification index r is 1. Since all exponents are different modulo $\frac{1}{r}\mathbb{Z}$ the set $\min_r(L)$ equals the set of exponents. Now the smallest element in $(\frac{1}{r}\mathbb{Z})\bigcap(2 \cdot \min_r(L))$ is 0. The smallest element of $(\frac{1}{r}\mathbb{Z})\bigcap(3 \cdot \min_r(L))$ is -1.

The generalized exponents of $l_\infty(L)$ are $-1/3, 1/3$ and all conjugates of $x^{-1/6}+2/3$. The ramification index r is 6. Now $-1/3 \leq_r 1/3$ and all the other generalized exponents are different modulo $\frac{1}{r}\mathbb{Z}$. Hence $\min_r(l_\infty(L))$ contains 7 elements; all generalized exponents except $1/3$. Now the smallest element in $(\frac{1}{r}\mathbb{Z})\bigcap(2 \cdot \min_r(l_\infty(L)))$ is $-2/3$. Rounded above to an integer this is 0. The smallest element in $(\frac{1}{r}\mathbb{Z})\bigcap(3 \cdot \min_r(l_\infty(L)))$ is -1.

So "procedure global-bounds" gives the following output for the second symmetric power of L: $Q = 1$ and $N = 0$. This means that the values of all invariants of degree 2 are constants. For the third symmetric power the output is $Q = 1/x$ and $N = 2$, which means that the values of the invariants of degree 3 must be of the form $\frac{1}{x} \cdot (c_0x^0 + c_1x^1 + c_2x^2)$ for some constants c_0, c_1, c_2.

4.4 The algorithm for computing invariants

4.4.1 Computing candidate invariants

In order to work with the solution space $V(L)$ we will choose a point $x_0 \in P^1(\overline{C})$ and compute the formal solutions at that point. Regular points have the advantage that computing the formal solutions is easier, but irregular points have other advantages that will be mentioned later. So we will not assume that x_0 is a regular point. For convenience of notation we will assume that the point x_0 is 0, if choosing a different point would be more favorable than we can move that point to 0 by the map l_{x_0}.

Denote by A the companion matrix of L. So the equation $L(y) = 0$ corresponds to the matrix differential equation $AY = Y'$ where $Y = (y, y', \ldots, y^{(n-1)})$.

Suppose $\hat{y}_i$, $1 \leq i \leq n = \text{order}(L)$, is a basis of formal solutions satisfying condition (4.3). Then a monomial in these $\hat{y}_i$'s (i.e. a product $\prod(\hat{y}_i)^{m_i}$) is again of the form (4.3), where the generalized exponent equals $\sum m_ie_i$.

Lemma 34 *Let $\hat{y}_i$ be a basis of local formal solutions satisfying condition (4.3) and let r be the least common multiple of the ramification indices. An entry of a vector invariant can only be non-zero if the generalized exponent of the corresponding monomial is in $\frac{1}{r}\mathbb{Z}$.*

Proof: Let $N = \binom{n+m-1}{n-1}$ and let $\hat{U}$ be a formal fundamental matrix of $Y' = AY$ such that the first row is $\hat{y}_1, \ldots, \hat{y}_n$, i.e. the entries of $\hat{U}$ are the $0, \ldots, (n-1)$-th derivatives of $\hat{y}_1, \ldots, \hat{y}_n$. Let P be a polynomial invariant. Let $\mathcal{C}$ be the corresponding vector invariant. Then $Sym^m(\hat{U})\mathcal{C} \in \overline{C}(x)^N \subset (V_{0,r})^N$. Note that each column of $Sym^m(\hat{U})$ is an element of $(V_{e,r})^N$ where e is the generalized exponent of the first element (which is a monomial in the $\hat{y}_i$) of this column. Using the fact that the columns of $Sym^m(\hat{U})$ are linearly independent and the direct sum (4.2) on page 77 it follows from $Sym^m(\hat{U})\mathcal{C} \in (V_{0,r})^N$ that $\mathcal{C}$ can only have a non-zero entry for those columns which are in $(V_{0,r})^N$, i.e. for those monomials whose generalized exponent is in $\frac{1}{r}\mathbb{Z}$.

□

Heuristic for computing invariants:
Algorithm candidate vector invariants.
Input: an operator L, an integer m, a point x_0, and a number ν.
Output: a vector space of candidate invariants of degree m and their corresponding candidate values, given as a parametrized candidate vector invariant and candidate value.

- If $x_0 \neq 0$ then apply recursion on $l_{x_0}(L)$ as follows: replace L and x_0 by $l_{x_0}(L)$ and 0, apply this algorithm and then apply the inverse of l_{x_0} on the candidate values of the invariants.

- Use the procedure global-bounds to find the bounds Q_1, N_1 for rational solutions of the m-th symmetric power of L.

- Compute a basis of formal solution $\hat{y}$ at $x = 0$ having property (4.3) in theorem 5. Let r be the least common multiple of the ramification indices. Let $\mathcal{Y}$ denote the vector of all monomials of degree m in the $\hat{y}_i$. Each of these monomials has a generalized exponent in $\overline{C}[x^{-1/r}]$.

- Take a vector $\mathcal{C}$ of unknown constants and set to zero every entry corresponding to a monomial with a generalized exponent that is not an element of $\frac{1}{r}\mathbb{Z}$.

- Compute $p_1 := \frac{1}{Q_1}\mathcal{Y}\mathcal{C} \bmod x^{N_1+\nu+1}$

- Build a linear system on $\mathcal{C}$ by equating to zero every term with degree higher than N_1 and all terms involving a log or a non-integer power of x.

- **Output:** the solution of this system (this is a vector space consisting of candidate vector invariants) and the corresponding (vector space of) rational functions $f_1 := p_1 Q_1$.

This algorithm is called a heuristic because the candidate invariants that it produces need not be invariants. The choice of the number ν is discussed in the strategies below.

Proposition 4 *Denote by* $W_{L,m,\nu}$ *the vector space of candidate vector invariants produced by the above heuristic. Denote* $W_{L,m,\infty} = \bigcap_\nu W_{L,m,\nu}$. *Then:*

1. *For all* $\nu \in \mathbb{N}$, *any vector invariant of degree* m *is in* $W_{L,m,\nu}$.
2. *There exists* $\nu_0 \in \mathbb{N}$ *such that* $W_{L,m,\infty} = W_{L,m,\nu_0}$.

Proof: From section 4.3, we get that the value of any invariant of degree m is the product of Q_1 by a polynomial of degree at most N_1; thus, the above lemma proves i). Increasing ν adds more conditions on $\mathcal{C}$ so $W_{L,m,i+1} \subset W_{L,m,i}$. As $W_{L,m,\infty}$ is finite dimensional, this implies ii).

$\square$

Remark: $\mathrm{order}(L^{\circledS m}) < \binom{n+m-1}{n-1}$ if and only if the solutions of L satisfy a homogeneous polynomial relation of degree m. In this case the value of a non-zero invariant can be zero, but it can also happen that $W_{L,m,\infty}$ contains elements (candidate vector invariants) that are not vector invariants. Note that since we do not compute $L^{\circledS m}$ we have no easy way of checking if this problem case $\mathrm{order}(L^{\circledS m}) < \binom{n+m-1}{n-1}$ occurs.

Remark: By reasoning as in section 1.c of [46], an application of Cramer's formulas shows that ν_0 is bounded by $N(1 + (N-1)d + Nd_1)$ (where $N = \binom{n+m-1}{n-1}$, d is the maximum degree of the a_i, and d_1 bounds the degrees of the numerator and denominator of Q_1). Thus, the above heuristic could be turned into an algorithm (but then the problem case $\mathrm{order}(L^{\circledS m}) < \binom{n+m-1}{n-1}$ in the previous remark would need to be addressed as well, for example by applying a transformation on L). However, this bound is big and so it is better to use the checking procedure that is given in section 4.4.2.

The PSL_3 example (continued): Let L be the 8-th order operator in the PSL_3 example of section 4.3. We had found the bounds for rational solutions of $L^{\circledS 2}$ and $L^{\circledS 3}$; applying the heuristic with $x_0 = 0$ and $\nu = 10$, we get the following (candidate) invariants:

$$\begin{aligned} P_2 &= \frac{352}{32805}\, c_0\, Y_1\, Y_7 - \frac{3249799168}{215233605}\, c_0\, {Y_4}^2 - \frac{36064}{6561}\, c_0\, Y_3\, Y_5 \\ &\quad + \frac{20240}{6561}\, c_0\, Y_6\, Y_2 + \frac{12397}{3645}\, c_0\, {Y_8}^2 \\ &\quad \text{and } P_2(\hat{y}) = c_0 \end{aligned}$$

$$\begin{aligned} P_3 &= -\frac{15167488}{405}\, c_{17}\, Y_8\, Y_6\, Y_2 + \frac{35500589056}{12301875}\, c_{17}\, {Y_1}^2\, Y_6 \\ &\quad + \frac{659456}{10125}\, c_{17}\, Y_1\, Y_8\, Y_7 - \frac{36929536}{54675}\, c_{17}\, Y_7\, Y_4\, Y_5 \end{aligned}$$

$$
\begin{aligned}
&- \frac{743206912}{22275}\, c_{17}\, Y_8\, Y_3\, Y_5 + \frac{106172416}{3267}\, c_{17}\, Y_2\, {Y_3}^2 \\
&- \frac{3479057727488}{81192375}\, c_{17}\, Y_1\, Y_3\, Y_4 + \frac{46450432}{3375}\, c_{17}\, {Y_8}^3 \\
&+ \frac{12176702046208}{66430125}\, c_{17}\, Y_8\, {Y_4}^2 + \frac{424689664}{18225}\, c_{17}\, Y_6\, {Y_5}^2 \\
&+ c_{17}\, {Y_7}^2\, Y_2 \\
&\text{and } P_3(\hat{y}) = c_{17} \frac{1}{x} (1 + \frac{9144576}{3025} x + \frac{17832200896512}{3826625} x^2)
\end{aligned}
$$

where c_0, c_{17} denote arbitrary constants. Note that $L^{\circledS 2}$ and $L^{\circledS 3}$ have order 36 and 120 respectively. $L^{\circledS 2}$ can be computed in several days on a big computer and $L^{\circledS 3}$ is out of reach of computers, whereas the above computation only takes a few minutes.

□

If one already has some information about the group then sometimes the heuristical algorithm is sufficient to compute the invariants. Because if we know how many linearly independent invariants of degree m exist, one can simply use the heuristic by just increasing the value of ν. If at a certain point the space of candidate vector invariants has the correct dimension then it is certain (even in the problem case $\mathrm{order}(L^{\circledS m}) < \binom{n+m-1}{n-1}$) that all invariants have been determined because the invariants form a subspace of the candidate invariants. In practise, it turns out that the required number ν is much smaller than the theoretical bound.

The Hurwitz example: The following operator has Galois group G_{168} ([50]). Let $\partial = \frac{d}{dx}$ and

$$
L = \partial^3 + \frac{7x-4}{x(x-1)}\partial^2 + \frac{2592x^2 - 2963x + 560}{252x^2(x-1)^2}\partial + \frac{-40805 + 57024x}{24696x^2(x-1)^2}.
$$

The ring of invariants is generated by invariants of degree $4, 6, 14, 21$. The heuristic with $m = 4, x_0 = \infty, \nu = 10$ yields (in 0.75 seconds) a one-dimensional space generated by $P = 1728\, Y_1\, {Y_2}^3 + {Y_1}^3\, Y_3 - 1728\, Y_2\, {Y_3}^3$ together with the value 0. The fact that the space of invariants of degree 4 has dimension exactly 1 proves that P is indeed an invariant. Similarly, the heuristic yields the other invariants quickly (see also [60]): for the invariant of degree 21, we need to compute 37 monomials at infinity (using a regular point it would have been 253 monomials).

□

If we choose a small number ν (even $\nu = 0$), the output of the above heuristic may also contain vectors that are not invariants, but it still is a good pre-conditioning to the algorithm *Invariants* in the following section.

4.4.2 Finding and proving which candidates are invariants

Let the monomial μ be a product of $y^{(i)}$ to the power m_i, $i = 0, \ldots, n-1$. If y is a solution of L then μ is a solution of the symmetric product of the operators $(L^{(i)})^{\circledS m_i}$.

By applying procedure global-bounds on μ we mean applying the procedure global-bounds on these numbers $m_0, \ldots, m_{n-1}$.

Algorithm Invariants:
Input: L, m, x_0 (optional: ν)
Output: the space of invariants in vector and dual forms

- Like in algorithm candidate vector invariants, if $x_0 \neq 0$ then we apply the transformation l_{x_0} and use recursion.
- Now we may assume $x_0 = 0$. Compute a basis of formal solutions of L at the point $x = 0$ having property (4.3) in theorem 5. Construct $\hat{U}$, the fundamental solution matrix of $Y' = AY$ from this.
- Obtain $F_1 = f$ and a vector $\mathcal{C}$ from the algorithm candidate vector invariants. Note that f and $\mathcal{C}$ contain parameters.
- for i from 2 to N do:
  - Let μ_i be the i-th monomial of degree m in $y, y', \ldots$;
    Obtain Q_i and N_i from procedure *global bounds* applied to L and μ_i.
  - Let $p_i := \frac{1}{Q_i} Sym(\hat{U})_i \mathcal{C} \mod x^{N_i+1}$ and $F_i := p_i \cdot Q_i$.
  - equate all terms involving logarithms or fractional powers of x to 0 (this gives a set of linear equations in the parameters. If the equations are non-trivial we use them to reduce the number of parameters).
- This returns a rational vector F parametrized by the entries of $\mathcal{C}$.
  The relation $F' - S^m(A)F = 0$ yields a system of linear equations in the parameters. Solve this system.
- **Output:** a basis of solutions $\mathcal{C}$ of this system and the corresponding dual first integrals $F \in C(x)^N$.

Theorem 6 *The output of this algorithm is exactly the space of invariants of degree m and the space of corresponding dual first integrals.*

Proof: That any vector invariant is an element of the vector space produced by the algorithm follows from the fact that this was true for our heuristic, and from the fact that we only added necessary linear conditions in this algorithm. Hence also every dual first integral F is an element of the vector space produced by the algorithm. Conversely, as the F produced by the algorithm are rational vectors satisfying $F' = S^m(A)F$, they are first integrals. So the corresponding $\mathcal{C}$ are indeed vector invariants.

$\square$

The advantage of choosing a singular point x_0 is that the number of monomials that need to be considered in the heuristic is often smaller, and so in "algorithm invariants" we need to evaluate fewer columns of $Sym^m(\hat{U})$. However, taking a point in which a ramification occurs can be disadvantageous, because computing modulo x^N in $C[[x^{1/r}]]$ involves more coefficients in C than computing modulo x^N in $C[[x]]$.

The PSL_3 example (continued): In the PSL_3 example of section 4.3, if we would take a regular point x_0 then the heuristic would need to evaluate 36 monomials for the invariants of degree 2, and 120 monomials for degree 3. However, when taking the singularity $x_0 = 0$, only 5 monomials of degree 2 have an integer exponent (the algorithm only considers monomials with an exponent in $\frac{1}{r}\mathbb{Z}$, and $r = 1$ in this example). And only 15 monomials of degree 3 have an integer exponent. So when using the singular point $x_0 = 0$ the computation for both the heuristic and the algorithm is much quicker than, say, with the regular point $x_0 = 1$.

Taking a point in which the generalized exponents require algebraic extensions can have both advantages and disadvantages. The disadvantage is obvious: Computing the formal solutions and evaluating monomials will be more costly. The advantage is that many monomials need not be considered. Suppose for example that $\mathrm{order}(L) = 3$ and that at the point $x_0 = 0$ we have 3 generalized exponents e_1, e_2, e_3 which are algebraic over $C((x))$ of degree 3. From $c_1e_1 + c_2e_2 + c_3e_3 \in \frac{1}{r}\mathbb{Z}$ and $c_1, c_2, c_3 \in \mathbb{Z}$ it follows that $c_1 = c_2 = c_3$. So only 1 monomial needs to be considered. This monomial is a power of $y_1y_2y_3$ where y_1, y_2, y_3 is a basis having property (4.3) in theorem 5. If such a monomial is in $\overline{C}(x)$ then $y_1y_2y_3$ is a radical of this element. Hence in this example L has a non-trivial invariant if and only if $y_1y_2y_3$ is a radical solution of the third symmetric power of L. In general computing radical solutions is a computationally costly problem, this problem is similar to computing first order factors. But in this example it is not so costly because we can use the fact that the radical solution (if it exists) is equal to $y_1y_2y_3$. So for order 3, what would appear to be the worst case (the e_i are algebraic of degree 3), is in fact a relatively easy case.

Taking a higher value of ν in the heuristic can decrease the dimension of the candidates. This can speed up the more costly "algorithm Invariants".

The algorithm is not yet completely implemented. Currently only an experimental version of the implementation is available by e-mail request. When the implementation is ready it will be made available at the authors' WWW addresses[3].

Applications of this algorithm are the computation of first integrals ([59]), the computation of differential relations satisfied by the solutions ([16]), the computation of algebraic and Liouvillian solutions ([49, 58, 60]) and, more generally, to obtain more knowledge on the Galois group.

[3] `http://www-math.sci.kun.nl/math/compalg/diffop/` and `http://medicis.polytechnique.fr/gage/weil.html`

Chapter 5

Rational Solutions of the Mixed Differential Equation and its Application to Factorization of Differential Operators

The topic of this chapter is a fast method to compute the rational solutions of a certain differential equation that will be called the mixed differential equation. This can be applied to speed up the factorization of completely reducible linear differential operators with rational functions coefficients.

5.1 Introduction

A differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y' + a_0 y = 0$$

corresponds to a differential operator of order n

$$f = \partial^n + a_{n-1}\partial^{n-1} + \ldots + a_0\partial^0$$

acting on y. Here the coefficients a_i are elements of the differential field $k(x)$ and ∂ is the differentiation d/dx. The field k is the field of constants. It is assumed to have characteristic 0. $\overline{k}$ is the algebraic closure of k. The differential operator f is an element of the non-commutative ring $k(x)[\partial]$. This is an example of an Ore ring [40]. The equation $\partial x = x\partial + 1$ holds in this ring. We denote the solution space of f as $V(f)$. It is a $\overline{k}$ vector space of dimension order(f). One way to define $V(f)$ without ambiguity is as a subset of the *universal extension*, cf. [24].

A factorization $f = LR$ where $L, R \in k(x)[\partial]$ is useful for computing solutions of f because the solutions $V(R)$ of the right-hand factor R are solutions of f as well.

Given L and R we can ask the following question: How can one compute (if it exists) an operator $R_2 \in \overline{k}(x)[\partial]$ such that $V(f) = V(R) \bigoplus V(R_2)$? In section 5.3.1 it is shown how this question can be reduced to the mixed equation (5.1) with $c = 1$. Such an operator R_2 could also be computed by one of the factorization algorithms for differential operators, cf. [6, 13, 42] and chapter 3. However, these factorization algorithms can be quite costly so we want to have an alternative method.

The mixed equation (called *gemischte Gleichung* in [39]) is the following: Let L and R be in $k(x)[\partial]$. We will assume that L and R are monic (i.e. the coefficient in $k(x)$ of the highest power of ∂ is 1). Let $c \in k(x)[\partial]$ with $\mathrm{order}(c) < \mathrm{order}(L)$. In the applications c is either 1 (cf. section 5.3.1) or 0 (cf. section 5.3.2). Compute the set of all $r \in \overline{k}(x)[\partial]$ such that there exists an $l \in \overline{k}(x)[\partial]$ with

$$Rr + lL = c. \tag{5.1}$$

We call this the mixed equation. An equivalent equation is

$$\mathrm{RRem}(Rr, L) = c. \tag{5.2}$$

Here RRem stands for the remainder after a right-hand division. Note that it is sufficient to compute the following set of solutions

$$\{r \in \overline{k}(x)[\partial] | \mathrm{order}(r) < \mathrm{order}(L) \quad \text{and} \quad \mathrm{RRem}(Rr, L) = c\} \tag{5.3}$$

because the other solutions r of order $\geq \mathrm{order}(L)$ are obtained from these by adding elements of $\overline{k}(x)[\partial]L$.

The set (5.3) of solutions of the mixed equation in the case $c = 0$ is called $\mathcal{E}_{\mathcal{D}}(R, L)$ in [47]. The operators r in this set map solutions of L to solutions of R. The set $\mathcal{E}_{\mathcal{D}}(f, f)$ is called the *eigenring* of f. Singer gives a very interesting application of computing this eigenring, namely the following: If $\mathcal{E}_{\mathcal{D}}(f, f)$ contains a non-constant element r then he shows how one can use r to compute a non-trivial factor in $\overline{k}(x)[\partial]$ of f in an efficient way, cf. section 3.1 in [47]. We will give an example of this in section 5.3.2. If f is completely reducible then either $\mathcal{E}_{\mathcal{D}}(f, f)$ contains a non-constant element (and so f can be factored) or $\mathcal{E}_{\mathcal{D}}(f, f)$ is the set of constants and then f is irreducible. This will be the main application of the mixed equation.

Acknowledgments: I would like to thank J.A. Weil and S.P. Tsarev for useful discussions about these topics. It should also be noted that J.A. Weil has ideas (which have not yet been written down) for similar results about factoring completely reducible operators as well. Both approaches have their own advantages. The advantage of his approach is it can be applied to other problems as well. The advantage of the approach in this chapter is that the algorithm is short and, even though the bound we give in proposition 5 is very technical, easier to implement. A proper comparison between the two methods can be given when both methods are implemented.

Outline of this chapter: The part of this chapter that is new is section 5.4. Sections 5.2 and 5.3 are not new, see also [39, 47]. These sections are intended as an introduction for section 5.4 and to give applications. Section 5.4.1 can be viewed as an introduction for section 5.4.2 because the result of section 5.4.1 is re-done more generally in section 5.4.2. The algorithm in section 4 for solving the mixed equation consists of two parts:

1. For each singularity $p \in P^1(\overline{k})$ compute a bound for the valuation at p of the coefficients in $k(x)$ of r.

2. Solve linear equations over k (a different approach is given in section 5.4 as well).

Computer algebra systems already have code for solving linear equations, so the only thing that needs to be implemented for solving the mixed equation is the bound in section 4.2.

An implementation of the algorithm (currently only the computation of $\mathcal{E}_{\mathcal{D}}(f, f)$ is implemented, but it is not much work to adapt this code for the case of a more general mixed equation) is available from
`http://www-math.sci.kun.nl/math/compalg/diffop/`

5.2 Preliminaries

This section lists a few facts about differential operators. For a more complete introduction see [47]. In section 5.4.2 the reader is assumed to be familiar with section 3 in chapter 3.

The *greatest common right divisor* $R = \mathrm{GCRD}(f_1, f_2)$ of two operators f_1 and f_2 is defined as the monic operator R with maximal order such that R is a right-hand factor of both f_1 and f_2. $V(R) = V(f_1) \bigcap V(f_2)$. By the Euclidean algorithm (cf. [40]) one can find two operators g_1 and g_2 such that

$$R = g_1 f_1 + g_2 f_2$$

and $\mathrm{order}(g_1) < \mathrm{order}(f_2)$. If $R = 1$ then the pair g_1, g_2 is uniquely determined. This can be shown as follows: If there were two different pairs then the difference h_1, h_2 of these pairs would satisfy the equation $h_1 f_1 + h_2 f_2 = 0$ and $\mathrm{order}(h_1) < \mathrm{order}(f_2)$. Then $V(f_2) \subset V(h_1 f_1)$ implying $f_1(V(f_2)) \subset V(h_1)$. However, f_1 is injective on $V(f_2)$ because $V(f_1) \bigcap V(f_2) = V(R) = 0$. So $\mathrm{order}(h_1) = \dim(V(h_1)) \geq \dim(f_1(V(f_2))) = \dim(V(f_2)) = \mathrm{order}(f_2)$ which is a contradiction.

A *valuation* on a ring R is a map $v : R \to \mathbb{Z} \bigcup \{\infty\}$ (other additive groups than $\mathbb{Z}$, such as $\mathbb{Q}$, are allowed as well) such that $v(0) = \infty$, $v(fg) = v(f) + v(g)$ for all $f, g \in R \setminus \{0\}$. Furthermore $v(f+g) \geq \min(v(f), v(g))$ and $v(f+g) = \min(v(f), v(g))$ if $v(f) \neq v(g)$. One can define different valuations on the ring of local (i.e. power series coefficients) differential operators, cf. section 2 in chapter 2. The valuation of a power series $a \in k((x)) \setminus \{0\}$ is defined as the smallest n for which the coefficient of x^n in a is non-zero. The valuation of a non-zero rational function $a \in k(x) \setminus \{0\}$ at a point $p \in P^1(\overline{k}) = \overline{k} \bigcup \{\infty\}$ is defined as follows: If $p = \infty$ then the valuation of a at p is the degree of the denominator minus the degree of the numerator. If $p \in \overline{k}$ then the valuation of a at p is defined as the integer n for which $b = a/(x-p)^n$ has no pole at p and $b(p) \neq 0$. Suppose that B_p for $p \in P^1(\overline{k})$ are given integers for which $B_p \neq 0$ for only finitely many p and that $N \geq 0$ where $N = \sum B_p$. Then the set of all a in $\overline{k}(x)$ for which the valuation of a at p is $\geq -B_p$ is a $\overline{k}$ vector space of dimension $N + 1$. The elements of this vector space are of the form n/D where $D \in \overline{k}(x)$ can be determined from the B_p and where $n \in \overline{k}[x]$ is a polynomial of degree $\leq N$.

In section 3.1 in [47] Singer gives three methods for computing $\mathcal{E}_\mathcal{D}(f,f)$. We will describe here the first method because we can draw two useful conclusions from this method (this method is computationally very costly, however. That is why we give an alternative method in section 5.4). Let $n = \mathrm{order}(L)$ and $m = \mathrm{order}(R)$. Write $r = r_0\partial^0 + \ldots + r_{n-1}\partial^{n-1}$ where the r_i are indeterminates. Write $c = c_0\partial^0 + \ldots + c_{n-1}\partial^{n-1}$. Now $\mathrm{RRem}(Rr, L)$ is a $k(x)$ linear combination of the r_i and the derivatives of the r_i. The highest derivative of r_i that appears in $\mathrm{RRem}(Rr, L)$ is $r_i^{(m)}$. This $r_i^{(m)}$ only appears in the coefficient of ∂^i in $\mathrm{RRem}(Rr, L)$ and the coefficient of $r_i^{(m)}$ in that expression is 1 (recall that R is monic). So equation (5.2) is equivalent with the following set of differential equations

$$\{r_i^{(m)} + \ldots = c_i | 0 \leq i \leq n-1\}$$

where the dots stand for $k(x)$-linear expressions in $r_j^{(m')}$, $j \in \{0, \ldots, n-1\}$, $m' \in \{0, \ldots, m-1\}$. If $c \neq 0$ then this system is not homogeneous. To make it homogeneous we add one extra variable z, one equation $z' = 0$, and replace the c_i by zc_i. We can convert this system to a system of first order equations by introducing new indeterminates $r_{i,j}$ for the j-th derivative of r_i and adding the equations $r_{i,j+1} = r'_{i,j}$. This way we obtain a system of equations of the form

$$Ay = y' \tag{5.4}$$

where A is a $nm+1$ by $nm+1$ matrix (if $c = 0$ then nm instead of $nm+1$ because then z is not needed) over $k(x)$ and y is a vector consisting of the $r_{i,j}$ and z. Such a matrix differential equation can be reduced to a single equation of order $nm+1$ (resp. nm if $c = 0$) by a cyclic vector computation and can then be solved, see [1] for computing rational solutions of a differential operator. We note the following:

Remark 1. If $p \in \overline{k}$ is a regular point for L, R and the c_i have no pole at p then the matrix A has no pole at the point p. If the vector y would have a pole of order t at the point p then the pole order of y' would be $t+1$, but the pole order of Ay is $\leq t$. This contradicts $Ay = y'$ so y (and hence the r_i as well) have no pole at the point p.

Remark 2. Every basis of the solutions y of equation 5.4 over $k(x)$ is a basis of solutions y over $\overline{k}(x)$ as well. Hence, for the mixed equation, to compute a basis for the solutions $r \in \overline{k}(x)[\partial]$ it suffices to compute a basis for the solutions $r \in k(x)[\partial]$.

5.3 Applications of the mixed equation

5.3.1 Computing a complement of $V(R)$

Let $f = LR$ where $f, L, R \in k(x)[\partial]$ are monic and suppose there exists a different factorization $f = L_2R_2$ in $\overline{k}(x)[\partial]$ such that $V(f) = V(R) \bigoplus V(R_2)$. We assume that the operators f, L, R, L_2 and R_2 are monic. The greatest common right divisor $\mathrm{GCRD}(R, R_2)$ of R and R_2 must be 1 because R and R_2 have no common non-zero solutions. Then, by the Euclidean algorithm, it follows that

$$rR + r_2R_2 = 1$$

for some $r, r_2 \in \overline{k}(x)[\partial]$ which are uniquely determined under the condition $\mathrm{order}(r) < \mathrm{order}(R_2)$ (note that $\mathrm{order}(R_2) = \mathrm{order}(L)$).

The map $rR + r_2R_2 = 1$ is the identity and the map r_2R_2 acts like the zero map on $V(R_2) \subset V(f)$. Hence the map rR acts like the projection of $V(f)$ to $V(R_2)$. So rR acts like the identity on $V(R_2)$. Now R maps $V(f)$ onto $V(L)$, the kernel is $V(R)$. Hence R is a bijection from $V(R_2)$ to $V(L)$. So r is the inverse bijection from $V(L)$ to $V(R_2)$. Hence Rr acts like the identity on $V(L)$, then $Rr - 1$ maps $V(L)$ to 0 so L must be a right-hand factor of $Rr - 1$. In other words

$$Rr + lL = 1 \tag{5.5}$$

for some $l \in \overline{k}(x)[\partial]$. R_2 can be constructed from r using the equation $V(R_2) = r(V(L))$ as follows: Write $z = r(y)$. We can write the derivatives of z as vectors over $\overline{k}(x)$ on the basis $y, y', \ldots, y^{(n-1)}$ (the higher order derivatives of y can be simplified using the relation $L(y) = 0$). Here $n = \mathrm{order}(L)$. The n-th derivative of z must be $\overline{k}(x)$ linearly dependent on the lower order derivatives $z, z', \ldots, z^{(n-1)}$. Computing this linear dependence gives R_2.

So: *computing the set of monic operators R_2 with $V(f) = V(R) \bigoplus V(R_2)$ is equivalent with solving the mixed equation (5.1) for $c = 1$.* These monic R_2 are in 1-1 correspondence to the solutions r in (5.3) of this mixed equation. Because of remark 2 in section 5.2 the existence of such an $R_2 \in \overline{k}(x)[\partial]$ is equivalent with the existence of such an $R_2 \in k(x)[\partial]$.

5.3.2 Singer's Factorization method

In this section we describe a factorization method of Singer (cf. section 3.1 in [47]) and show in an example how to combine Singer's method with the method from section 5.4. Note that our f and r are called L and R in [47]. In the previous section a factorization $f = LR$ was given and the goal was to compute different factorizations. In this section only $f \in k(x)[\partial]$ is given and we want to factor f using the solutions of the following mixed equation

$$fr + lf = 0. \tag{5.6}$$

This equation is a special case of (5.1). The set of solutions (5.3) is called $\mathcal{E}_{\mathcal{D}}(f, f)$.

Suppose the dimension of $\mathcal{E}_{\mathcal{D}}(f, f)$ is greater than 1. Then we can take an element $r \in k(x)[\partial]$ in $\mathcal{E}_{\mathcal{D}}(f, f)$ which is not a constant. Now r is a $\overline{k}$-linear map from $V(f)$ to $V(f)$. We can compute a basis of $V(f)$ by computing formal solutions of f at a point (this is easiest at a regular point). Then compute the matrix of the map r in this basis and compute an eigenvalue $a \in \overline{k}$. Then $\mathrm{GCRD}(f, r - a) \in \overline{k}(x)[\partial]$ is a non-trivial factor of f. Note that the only algebraic extension over k that was used to compute a right-hand factor is the eigenvalue a.

Corollary 3 *If $f \in k(x)[\partial]$ has an irreducible right-hand factor in $\overline{k}(x)[\partial]$ of order d then f has an irreducible right-hand factor of order d in $l(x)[\partial]$ for some algebraic extension l of k of degree $\leq \mathrm{order}(f)/d$.*

Proof: Let g be the LCLM of all irreducible right-hand factors of f of order d. Now the statement follows by applying Singer's factorization method to g.

□

Example: Given is the following differential operator

$$f = \partial^4 + \frac{6}{x}\partial^3 + \frac{2(x^2-1)}{x^4}\partial^2 - \frac{2(3x^2-1)}{x^5}\partial + \frac{1}{x^8}$$

which is the LCLM of two irreducible operators in $\overline{\mathbb{Q}}(x)[\partial]$. The problem is to find a right-hand factor of f. In section 5.4 we will compute $\mathcal{E}_{\mathcal{D}}(f, f)$, the solutions r of order $<$ order(f) of equation (5.6). It has dimension 2. Then we can choose a non-constant solution:

$$r = -x^5\partial^3 - x^4\partial^2 + 2x^3\partial + x\partial.$$

Now we need a basis for $V(f)$. We compute a basis $b_1, \ldots, b_4 \in \mathbb{Q}((x-1))$ of formal solutions at the point $x = 1$. These b_i are uniquely determined by requiring that b_i is $(x-1)^{i-1}$ mod $(x-1)^4$. The operator r acts on this basis as

$$\begin{pmatrix} 0 & 3 & -2 & -6 \\ 1 & 3 & -2 & 0 \\ -3/2 & 1/2 & 2 & -3 \\ 13/6 & -5/3 & 1/3 & 7 \end{pmatrix}.$$

The eigenvalues of this matrix are $3 + \sqrt{2}$ and $3 - \sqrt{2}$. From the eigenvalue $3 + \sqrt{2}$ we obtain the following right-hand factor of f

$$\text{GCRD}(f, r - 3 - \sqrt{2}) = \partial^2 + \frac{\sqrt{2}}{x}\partial - \frac{1}{x^4}.$$

The other eigenvalue $3 - \sqrt{2}$ gives the conjugate over $\mathbb{Q}$ of this factor.

Note that $\dim(\mathcal{E}_{\mathcal{D}}(f, f)) > 1$ implies that f is reducible but not that f is completely reducible. For example if $f = (\partial + 1/x)\partial$ then $r = x\partial \in \mathcal{E}_{\mathcal{D}}(f, f)$ (giving the right-hand factor ∂) but f is not the LCLM of irreducible operators.

5.4 Solving the mixed equation

Write

$$r = \sum_{i=0}^{\text{order}(L)-1} r_i \partial^i$$

and suppose r is a solution of the mixed equation (5.2) or equation (5.1) which is equivalent. In section 5.2 we have seen that the r_i can not have a pole at a point $p \in \overline{k}$ if R, L and c have no pole at p. In section 5.4.1 (lemma 35) and section 5.4.2 (proposition 5 and the comments after proposition 5) we show how to compute a bound for the valuation of each r_i in the remaining places (i.e. the point ∞ and the points in $\overline{k}$ where R, L or c has a pole). Then we can write

$$r_i = \frac{n_i}{D_i}$$

with $n_i \in k[x]$ of degree $\leq N_i$ and $D_i \in k(x)$ where N_i and D_i are computed from the bounds. So given the bounds, we only need to determine the polynomials n_i. This can be done in several different ways:

- **Approach 1**. Write the n_i as a polynomials in x of degree N_i with undetermined coefficients. Then substitute r in the mixed equation (5.2) and find linear equations for these undetermined coefficients. Solving these equations gives the solutions of the mixed equation.

- **Approach 2**.

  Let L_1 be an operator such that $V(L_1) = c(V(L))$. If $c = 0$ then put $L_1 = 1$, if $c = 1$ then $L_1 = L$. In the remaining cases L_1 can be obtained as follows: write $z = c(y)$ where y is a solution of L. Denote $n = \mathrm{order}(L)$. Using $L(y) = 0$ we write the derivatives of z as $k(x)$ linear expressions in $y, y', \ldots, y^{(n-1)}$. Computing a $k(x)$-linear dependence between $z, z', \ldots, z^{(n)}$ gives L_1.

  Compute a basis for $V(L)$ and a basis $z_1, \ldots, z_m$ for $V(L_1 R)$ (for example a basis of formal solutions at a regular point). Let $y \in V(L)$. Then $Rr(y) = c(y) \in V(L_1)$ so $r(y) \in V(L_1 R)$. Assume that all the D_i are equal to one polynomial D (if they are not polynomials we can take the numerator, and if they are not equal we can replace the D_i by the least common multiple). Then

  $$r(y) = \frac{1}{D} \sum n_i \partial^i(y) \in V(L_1 R)$$

  so

  $$\sum n_i y^{(i)} = C_1 D z_1 + \ldots + C_m D z_m. \qquad (5.7)$$

  Here the n_i and C_i are polynomials in x with a bounded degree (the degree of the C_i is 0). The $y^{(i)}$ and Dz_i are power series in $x - p$ (if we computed the formal solutions at a regular point p). For each basis element y of $V(L)$ we obtain an equation of this form. The problem of computing all polynomials n_i and C_i satisfying the given conditions on their degrees, such that equation (5.7) holds up to a given accuracy $a \in \mathbb{N}$ (i.e. modulo $(x-p)^a$) is handled efficiently by the Beckermann-Labahn algorithm, cf. [17, 5]. A good guess for the accuracy a that is required to obtain solutions of the mixed equation to take a such that the number of linear conditions over k is at least the number of unknown coefficients of the n_i and C_i. If we took the accuracy a too small then we find too many solutions, i.e. we find a basis $b_1, \ldots, b_t$ such that the solutions of the mixed equation form a subspace of the vector space spanned by $b_1, \ldots, b_t$. Then we can pick out the correct solutions from this vector space as follows: Substitute $r = c_1 b_1 + \ldots c_t b_t$, where the c_i are variables, in the mixed equation (5.2) and solve linear equations to find the right $c_1, \ldots, c_t$.

- **Approach 3**. One can compute the n_i from the formal solutions $r_i \in k((x-p))$ of the mixed equation where p is a regular point, in a way that is similar to the way that the rational solutions of a differential operator are obtained from the formal solutions in [1]. This way we have to solve linear equations over k in $\mathrm{order}(L) \cdot \mathrm{order}(R)$ variables.

5.4.1 The local bound problem, regular singular case

Define $\delta = x\partial$. The ring $k(x)[\partial]$ is a sub-ring of the ring $k((x))[\partial] = k((x))[\delta]$. In section 2.2 we have defined a valuation

$$v_0 : k((x))[\delta] \to \mathbb{Z} \bigcup \{\infty\}$$

as follows: For non-zero $f = \sum_{i,j} f_{i,j} x^i \delta^j$ the valuation $v_0(f)$ is the smallest i for which $f_{i,j} \neq 0$ for some j. For this f we can define the *Newton polynomial for slope 0* (as in section 2.3.4) using a variable T as follows

$$N_0(f) = \sum_j f_{v_0(f),j} T^j \in k[T].$$

The substitution map

$$S_{T=T+i} : k[T] \to k[T]$$

is a k homomorphism defined by $T \mapsto T + i$.

We recall a few facts about the Newton polynomial N_0

- degree$(N_0(f))$ = order(f) if and only if f is regular singular.
- The roots of $N_0(f)$ in $\overline{k}$ are called the *exponents* of f.
- For all L, R in $k((x))[\delta]$ we have

$$N_0(L \cdot R) = S_{T=T+v_0(R)}(N_0(L)) \cdot N_0(R).$$

Note that we assumed that L and R are monic in $k(x)[\partial]$. So if the order is > 0 they are not monic when considered as elements of $k((x))[\delta]$.

The *local bound problem* is the following: Given R, L and c in $k((x))[\delta]$ with order(c) < order(L) compute a lower bound for $v_0(r)$ (or a lower bound for each coefficient of r in $k((x))$ separately) for all solutions $r \in \overline{k}((x))[\delta]$ of the mixed equation (5.1), i.e. for all $r \in \overline{k}((x))[\delta]$ with order(r) < order(L) for which there exists an $l \in \overline{k}((x))[\delta]$ such that $Rr + lL = c$.

Lemma 35 (Bound for $v_0(r)$ in the regular singular case). *Let R, r, l, L and c be in $k((x))[\delta]$ with $Rr + lL = c$,* order(c) < order(L), order(r) < order(L), *$R \neq 0$, $L \neq 0$ and $r \neq 0$. Assume that L is regular singular. Then*

$$c \neq 0 \quad \text{and} \quad v_0(r) \geq v_0(c) - v_0(R)$$

or

$$\gcd(S_{T=T+v_0(r)}(N_0(R)), N_0(L)) \neq 1. \tag{5.8}$$

Proof: If $v_0(r) \geq v_0(c) - v_0(R)$ then $v_0(c)$ must be finite and so $c \neq 0$. Now assume $v_0(r) < v_0(c) - v_0(R)$. Then $v_0(Rr) < v_0(c) = v_0(Rr + lL)$. This is only possible if the lowest power of x in Rr and lL cancel, in other words

$$N_0(Rr) + N_0(lL) = 0.$$

The assumption that L is regular singular means

$$\text{degree}(N_0(L)) = \text{order}(L).$$

Apply the multiplication formula for the Newton polynomials

$$\begin{aligned} 0 &= N_0(Rr) + N_0(lL) \\ &= S_{T=T+v_0(r)}(N_0(R)) \cdot N_0(r) + S_{T=T+v_0(L)}(N_0(l)) \cdot N_0(L). \end{aligned}$$

Because degree$(N_0(r))$ < order(L) = degree$(N_0(L))$ equation 5.8 follows.

□

Note that equation 5.8 can hold for only finitely many integers $v_0(r)$. So the minimum of these integers (and the integer $v_0(c) - v_0(R)$ if $c \neq 0$) is a lower bound for $v_0(r)$. The bound can be computed from $v_0(c)$, $v_0(R)$, $N_0(L)$ and $N_0(R)$.

5.4.2 The local bound problem, general case

We can generalize the valuation v_0 and the Newton polynomial N_0 to $\overline{k((x))}[\delta]$ as follows: If $f \in \overline{k((x))}[\delta]$ then f is an element of $\overline{k}((x^{1/n}))[\delta]$ for some $n \in \mathbb{N}$. Write $f = \sum_i x^i f_i$ where $f_i \in \overline{k}[\delta]$ and where the sum is taken over $i \in \frac{1}{n}\mathbb{Z}$. If $f \neq 0$ then $v_0(f)$ is defined as the smallest i for which $f_i \neq 0$ and the Newton polynomial $N_0(f)$ is defined as this f_i (with δ replaced by the variable T).

First let us recall a few definitions and notations from section 3.3. We have defined a set $E = \bigcup_n \overline{k}[x^{-1/n}]$ and a partially defined valuation v from the universal extension V to the set E. This v is defined on the set $V_* \subset V$, which is the set of all non-zero $y \in V$ that can be written in the form $\mathrm{Exp}(e)s$ for some $e \in E$ and $s \in \overline{V}_0$. Here

$$\overline{V}_0 = \overline{k((x))}[\log(x)].$$

The map

$$\mathrm{Exp} : E \to V_*$$

is defined as $\mathrm{Exp}(e) = \exp(\int \frac{e}{x} dx)$. We have $v(\mathrm{Exp}(e)) = e$. For $e \in \overline{k((x))}$ the *substitution map*

$$S_e : \overline{k((x))}[\delta] \to \overline{k((x))}[\delta]$$

is defined as the $\overline{k((x))}$-homomorphism given by $S_e(\delta) = \delta + e$. For $e \in E$ and $f \in \overline{k((x))}[\delta] \setminus \{0\}$ we have defined the multiplicity $\nu_e(f)$ of the generalized exponent e in f as the multiplicity of the root 0 in $N_0(S_e(f))$. Note: $\nu_e(f)$ is not the same as the multiplicity of the exponential part $\mu_e(f)$. The exponential parts are the generalized exponents modulo a certain equivalence, hence their multiplicity $\mu_e(f)$ is $\geq$ the multiplicity $\nu_e(f)$ of the generalized exponent. The sum of $\nu_e(f)$ taken over all $e \in E$ is the number of elements of the list of generalized exponents which equals $\mathrm{order}(f)$.

The generalized exponents are a generalization of the classical notion of exponents. The exponents of an operator f are those generalized exponents which are in $\overline{k}$. An operator is regular singular if and only if all generalized exponents are exponents, i.e. if they are elements of $\overline{k}$.

Our approach for the general (i.e. not necessarily regular singular) case is quite technical. To explain the idea we will first reformulate the previous section into the terminology of exponents instead of Newton polynomials. Then we can generalize by replacing the exponents by generalized exponents. If

$$Rr + lL = c \quad \text{and} \quad c = 0$$

and e is an exponent of L then e is an exponent of Rr as well. If $\nu_e(r) < \nu_e(L)$ then (the proof follows later in the more general case) $v_0(r) + e$ is an exponent of R. This must happen for at least one exponent e of L because if L is regular singular then the number of exponents e (counting with multiplicity) is greater than the order of

r. By comparing the exponents of R and L, and taking the smallest possible integer difference, we obtain a bound for $v_0(r)$. If $c \neq 0$ we have to consider the possibility $v_0(Rr) \geq v_0(c)$ as well.

If L is not regular singular (L is irregular singular) then the number of exponents e is not necessarily larger than order(r). Then there need not be an exponent e with $\nu_e(r) < \nu_e(L)$. This problem can be fixed by using generalized exponents instead of exponents. Using generalized exponents we always have an e with $\nu_e(r) < \nu_e(L)$ because order$(r) <$ order(L). Then we can take a solution $y \in V_*$ of L with $v(y) = e$. By substituting y in the mixed equation (5.1) we get the equation $Rr(y) = c(y)$. The idea is now to relate the multiplicity of a generalized exponent to a property *degl* of elements of V_*. Using this property we can study the relation between the valuation of f, $f(y)$ and y. We apply this two times on the equation $Rr(y) = c(y)$, first to find a relation between the valuations of R, $R(r(y))$ and $r(y)$ (note that R and $R(r(y)) = c(y)$ are known, so this relation gives information on the valuation of $r(y)$) and then to find a relation between the valuations of r, $r(y)$ and y to obtain information on the valuation of r.

Definition 16 *For a non-zero element $y \in \overline{V}_0$ define* $\mathrm{degl}(y)$ *as follows: Write y as $y = \sum_{i,j} a_{ij} x^i \log(x)^j$ where the sum is taken over $j \in \mathbb{N}$ and $i \in \frac{1}{n}\mathbb{Z}$ for some $n \in \mathbb{N}$. Then* $\mathrm{degl}(y)$ *is the maximal j for which $a_{v(y),j} \neq 0$.*

Every element $y \in V_*$ is of the form $\mathrm{Exp}(e)z$ *for some $e \in E$ and $z \in \overline{V}_0$. Then* $\mathrm{degl}(y)$ *is defined as* $\mathrm{degl}(z)$.

Lemma 36 *Let $e \in \overline{k}$, $f = \delta - e + s$ with $s \in \overline{k((x))}$ with $v(s) > 0$ and $y \in \overline{V}_0 \setminus \{0\}$. If $e \neq v(y)$ then*

$$v(f(y)) = v(y) \quad \text{and} \quad \mathrm{degl}(f(y)) = \mathrm{degl}(y).$$

If $e = v(y)$ and $\mathrm{degl}(y) > 0$ *then*

$$v(f(y)) = v(y) \quad \text{and} \quad \mathrm{degl}(f(y)) = \mathrm{degl}(y) - 1$$

and if $e = v(y)$ and $\mathrm{degl}(y) = 0$ *then*

$$v(f(y)) > v(y).$$

Since the proof of the lemma is easy we skip it. Note that $f(y) = 0$ is only possible in the case $e = v(y)$ and $\mathrm{degl}(y) = 0$.

Lemma 37 *Let $f \in \overline{k((x))}[\delta] \setminus \{0\}$, $y \in \overline{V}_0 \setminus \{0\}$ and $d = \mathrm{degl}(y)$. Let $e = v(y) \in \mathbb{Q}$ and $d' = \nu_e(f)$. If $d' \leq d$ then*

$$v(f(y)) = v_0(f) + v(y) \quad \text{and} \quad \mathrm{degl}(f(y)) = d - d'.$$

If $d' > d$ then

$$v(f(y)) > v_0(f) + v(y)$$

Note that $f(y) = 0$ is only possible in the case $d' > d$.

Proof: Factor (cf. section 5 in chapter 2) f as $f = L \cdot (\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)$

where $v(s_i) > 0$, $e_1, \ldots, e_n \in \overline{k}$ are the exponents of f and L has no regular singular factor (i.e. L has no slope 0 in the Newton polygon). Then $v_0(f) = v_0(L)$. Denote $z = (\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)(y) \in \overline{V}_0$. Now either $v(z) \in \mathbb{Q}$ or $z = 0$. d' is the number of i for which $e_i = v(y)$.

Assume $z \neq 0$. Write $L = L_0\delta^0 + \ldots + L_m\delta^m$. Now $v(L_i) > v(L_0)$ for $i > 0$ (because L has no slope 0) and $v(\delta^i(z)) \geq v(z)$ so $v(L_i\delta^i(z)) > v(L_0 \cdot z)$. Hence $v(L(z)) = v(L_0 \cdot z)$ and $\mathrm{degl}(L(z)) = \mathrm{degl}(L_0 \cdot z)$. Now $f(y) = L(z)$ so $v(f(y)) = v(L_0 \cdot z) = v(L_0) + v(z) = v_0(L) + v(z) = v_0(f) + v((\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)(y))$ and $\mathrm{degl}(f(y)) = \mathrm{degl}(L_0 \cdot z) = \mathrm{degl}(z) = \mathrm{degl}((\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)(y))$. Now the lemma follows by repeated use of the previous lemma.

□

Lemma 38 *Let $f \in k((x))[\delta]$. Then f has a solution y in V_* with* $\mathrm{degl}(y) = d$ *and $v(y) = e$ if and only if $\nu_e(f) > d$.*

Note the following consequence of the lemma: If there exists a solution y with $v(y) = e$ and $\mathrm{degl}(y) > 0$ then there exists a solution z with $v(z) = e$ and $\mathrm{degl}(z) = \mathrm{degl}(y) - 1$. This can easily be shown in a different way as well, take $z = y - S_{\log}(y)$ where $S_{\log}$ is the map that replaces $\log(x)$ by $\log(x) + 1$, cf. section 9 in chapter 2.

Proof: Let $y \in V_*$ with $\mathrm{degl}(y) = d$, $v(y) = e$ and $f(y) = 0$. Write $z = \mathrm{Exp}(-e)y$, so $v(z) = 0$ and $z \in \overline{V}_0 \setminus \{0\}$. We have $V(f) = \mathrm{Exp(e)} \cdot V(S_e(f))$. So $S_e(f)(z) = 0$ and hence by lemma 37 it follows that $\nu_0(S_e(f)) > \mathrm{degl}(z) = d$. Since $\nu_e(f) = \nu_0(S_e(f))$ one part of the lemma follows.

Now suppose $\nu_e(f) > d$. We must prove that f has a solution in V_* with valuation e and degl d. Let $R \in k((x))[e, \delta]$ be the right-hand factor of $S_e(f)$ of maximal order which is semi-regular (cf. section 3.2 in chapter 3) over $k((x))[e]$. Now $\nu_0(R) = \nu_0(S_e(f)) = \nu_e(f) > d$.

It is sufficient to prove that R has a solution y with valuation 0 and degl d, because then $\mathrm{Exp}(e)y$ is a solution of f with the desired property. Section 8.1 in chapter 2 gives a recursive algorithm for computing a basis of solutions of R. This algorithm makes repeated use of integration $s_i = \int \frac{a_i}{x} dx$. In this integration process (we take the constant term in the integral equal to 0) we have $v(s_i) = v(a_i)$. Furthermore $\mathrm{degl}(s_i) = \mathrm{degl}(a_i)$ if $v(a_i) \neq 0$ and $\mathrm{degl}(s_i) = \mathrm{degl}(a_i) + 1$ if $v(a_i) = 0$. Using these relations and induction with respect to the order of R it follows that the algorithm in section 8.1 of chapter 2 produces a solution y with valuation e and $\mathrm{degl}(y) = j$ for every exponent e of R and every integer j with $0 \leq j < \nu_e(R)$.

□

Lemma 39 *Let $f \in k((x))[\delta]$ be of order n and $e \in E$. Let $v' = 0$ if $e = 0$ and $v' = v(e)$ otherwise (so $v' \in \mathbb{Q}$ and $v' \leq 0$). Let $d = v_0(S_e(f))$. Then d is an integer divided by the ramification index of e. The coefficient of δ^i in f has valuation $\geq d + (n - i)v'$.*

The proof of the lemma is easy, we skip it. The *ramification index* of e is defined as the smallest positive integer n such that $e \in \overline{k}((x^{1/n}))$.

Proposition 5 (Bound for $v_0(S_e(r))$). *Let $Rr + lL = c$ where R, r, l, L, c in $k((x))[\delta]$ with $R \neq 0$, $L \neq 0$, $r \neq 0$, $\mathrm{order}(c) < \mathrm{order}(L)$ and $\mathrm{order}(r) < \mathrm{order}(L)$.*

Suppose $e \in E$ with $\nu_e(L) > \nu_e(r)$. Let $y \in V_*$ be a solution of L with $v(y) = e$ and $\mathrm{degl}(y) = \nu_e(L) - 1$. Let $M = \infty$ if $c(y) = 0$ and $M = v(c(y)) - e \in \mathbb{Q}$ if $c(y) \neq 0$. Then

$$c(y) \neq 0 \quad \text{and} \quad v_0(S_e(r)) = M - v_0(S_e(R))$$

or $v_0(S_e(r)) + e$ is a generalized exponent of R.

Note: It is not a priori known which e satisfies $\nu_e(L) > \nu_e(r)$. Also note that $\nu_e(L) > \nu_e(r)$ implies that $\nu_e(L) > 0$ in other words: e is a generalized exponent of L.

In the two applications in section 5.3 we have $c = 0$ or $c = 1$. If $c = 0$ then $M = \infty$ so then the first case in the proposition can not occur. If $c = 1$ then $M = 0$. So in both applications the proposition can be used without computing a solution y with the desired properties $\mathrm{degl}(y) = \nu_e(L) - 1$ and $v(y) = e$.

Proof:

$$Rr(y) = (Rr + lL)(y) = c(y).$$

Denote $z = \mathrm{Exp}(-e)y$ and $w = S_e(r)(z)$. Then $v(z) = 0$ and $\mathrm{degl}(z) = \mathrm{degl}(y) = \nu_e(L) - 1 \geq \nu_e(r) = \nu_0(S_e(r))$. Now $S_e(R)S_e(r) + S_e(l)S_e(L) = S_e(c)$ and z is a solution of $S_e(L)$ so

$$S_e(R)(w) = S_e(R)(S_e(r)(z)) = S_e(c)(z) \tag{5.9}$$

Now $S_e(c)(z) = \mathrm{Exp}(-e)c(y)$ so

$$v(S_e(R)(w)) = v(c(y)) - e = M.$$

By lemma 37 and $\mathrm{degl}(z) \geq \nu_0(S_e(r))$ it follows that

$$v(w) = v(S_e(r)(z)) = v_0(S_e(r)) + v(z) = v_0(S_e(r)). \tag{5.10}$$

According to lemma 37 and equation 5.9 there are two possibilities (if $M = \infty$ then the first case can not occur)

$$v(S_e(R)(w)) = v_0(S_e(R)) + v(w)$$

or $\nu_{v(w)}(S_e(R)) > \mathrm{degl}(w)$ which implies that $v(w)$ is a generalized exponent of $S_e(R)$. The latter case implies that $v(w) + e$ is a generalized exponent of R. So $v_0(S_e(r)) = v(w) = v(S_e(R)(w)) - v_0(S_e(R)) = M - v_0(S_e(R))$ or $v_0(S_e(r)) + e = v(w) + e$ is a generalized exponent of R.

□

Note that both cases imply a lower bound for $v_0(S_e(r))$. Since we do not know which of these two cases holds (unless $M = \infty$ then the first case can not occur) we have to take the minimum of these two bounds to obtain a lower bound for $v_0(S_e(r))$. In the case where $v_0(S_e(r)) + e$ is a generalized exponent of R we obtain a lower bound for $v_0(S_e(r))$ by taking the minimal $m \in \frac{1}{\mathrm{ram}(e)}\mathbb{Z}$ for which $m + e$ is a generalized exponent of R (recall that $\mathrm{ram}(e)$ is the ramification index of e). Then by lemma 39 we obtain a lower bound for the valuation of the coefficients of r.

The order of an operator equals the sum of the ν_e taken over all $e \in E$. Since $\mathrm{order}(L) > \mathrm{order}(r)$ we must have

$$\nu_e(L) > \nu_e(r) \tag{5.11}$$

for at least one $e \in E$. Note, however, that we do not know for which e equation 5.11 holds. So to obtain a lower bound for the valuations of the coefficients of r we must take the minimum of these lower bounds for all generalized exponents e of L.

Example, continued from section 5.3.2: Now we will use the bound to compute the rational solutions r of the mixed equation in the example of section 5.3.2. We can write

$$r = \frac{n_3}{D_3}\partial^3 + \ldots + \frac{n_0}{D_0}\partial^0.$$

The only singularities of f are $x = 0$ and $x = \infty$. The point $x = 0$ is an irregular singularity so we must compute the list of generalized exponents:

$$\alpha - \frac{1}{x}, 2 - \alpha - \frac{1}{x}, \alpha + \frac{1}{x}, 2 - \alpha + \frac{1}{x}.$$

Here α is a root of the polynomial $1 - 4Z + 2Z^2$ (note that it is not necessary to compute all generalized exponents, it suffices to compute them up to conjugation). Now the smallest possible difference between generalized exponents which is an integer divided by the ramification index is 0. So we have $v_0(S_e(r)) \geq 0$ for some e in the list of generalized exponents. Then by lemma 39 it follows that the coefficient of δ^i in r (here r localized at the point $x = 0$, in δ notation instead of ∂ notation, cf. section 3.4 in chapter 3) has valuation $\geq i - 3$. Now we should convert this bound for the δ notation to a bound in ∂ notation. The result is that $r_i = n_i/D_i$ has valuation $\geq i - 3 + i$ at the point $x = 0$. So we can take $D_i = x^{3-2i}$ (D_i is not a polynomial if $i \geq 2$, however. In these cases the notion of the degree of D_i is problematic. But then we can simply interpret $\mathrm{degree}(D_i)$ as -1 times the valuation of D_i at the point infinity).

Now we want a lower bound for the valuation of r_i at infinity (i.e. an upper bound for $\mathrm{degree}(n_i) - \mathrm{degree}(D_i)$). The operator f is regular singular at infinity and the Newton polynomial is $T^4 - 5T^2 + 2T = T(T-2)(T^2 + 2T - 1)$. Then by lemma 35 it follows that $v_0(l_\infty(r)) \geq -2$. Here $l_\infty(r)$ is r localized at infinity, cf. section 3.4 in chapter 3. We have to convert this to a bound for the valuation of r_i at infinity. The result is that the valuation of r_i at infinity is $\geq -2 - 2i$. This means $\mathrm{degree}(n_i) - \mathrm{degree}(D_i) \leq 2 + 2i$. Hence $\mathrm{degree}(n_i) \leq 2 + 2i + \mathrm{degree}(D_i) = 5$. So we can write r with $4 \cdot (5+1)$ undetermined coefficients. Twenty-four indeterminates is not very much so approach 1 in section 5.4, solving linear equations, will be efficient enough to be able to handle this example. These linear equations are obtained from $\mathrm{RRem}(fr, f) = 0$. By solving these linear equations we can find the following basis of solutions: 1 and $-x^5\partial^3 - x^4\partial^2 + 2x^3\partial + x\partial$.

Example:

$$f = \partial^4 + \frac{6x}{x^2+1}\partial^3 + \frac{8x^2+5}{(x^2+1)^2}\partial^2 + \frac{2x}{(x^2+1)^2}\partial + \frac{1}{(x^2+1)^2}.$$

This operator is completely reducible. Using the implementation in `diffop` one can compute in a few seconds the following basis of the eigenring: $b_1 = 4x + (x^2-2)\partial + 6x(x^2+1)\partial^2 + (x^2+1)^2\partial^3$, $b_2 = x\partial + (x^2+1)\partial^2$, $b_3 = x - \partial + x(x^2+1)\partial^2$, $b_4 = 1$. We choose a $\mathbb{Q}(t)$-linear combination of b_1, b_2, b_3 (the constant term b_4 has no influence on the resulting factorizations) for which the endomorphism that is obtained has eigenvalues that depend on t. Then, by applying Singer's factorization algorithm, we obtain a right-hand factor that depends on t. After simplification this results in the following right-hand factors

$$R_{s,t} = \partial^2 + \frac{tx-1}{(x^2+1)(x+t)}\partial + \frac{2x+t+s}{2(x^2+1)(x+t)}, \quad \text{where} \quad s^2 = -3t^2 - 4,\ t \in P^1(\overline{k}).$$

These $R_{s,t}$ are irreducible. Every $R_{s,t}$ must have the same type otherwise f could not have infinitely many different factorizations (cf. [56] or [39]). Since the set of all irreducible right-hand factors can be parametrized by $P^1(\overline{k})$, cf. [56], and any non-constant morphism from a conic $s^2 = -3t^2 - 4$ to $P^1(\overline{k})$ is surjective, it follows that $\{R_{s,t} | s^2 = -3t^2 - 4,\ t \in P^1(\overline{k})\}$ is the set of all irreducible right-hand factors of f. As one can see none of the $R_{s,t}$ is defined over $\mathbb{Q}$, so f is irreducible in $\mathbb{Q}(x)[\partial]$, even though it has infinitely many different factorizations in $\overline{\mathbb{Q}}(x)[\partial]$.

Proposition 6 *Let $f = LR$ with f, L, R monic elements of $k((x))[\delta]$. Let $s \in \mathbb{Q}$, $s \geq 0$ and v_s be the valuation defined in section 2.2. Then the coprime index (defined in section 2.2) with respect to v_s of this factorization is finite.*

Proof: If the coprime index is $> t$ then there exists an $a \geq t$ and operators L_t, R_t such that

- $\sigma_{a+t+1}(L_tR_t) = \sigma_{a+t+1}(LR)$, in other words: $v_s(L_tR_t - LR) > v_s(LR) + a + t$.
- $\sigma_a(L_t) = \sigma_a(L)$ and $\sigma_a(R_t) = \sigma_a(R)$. In other words:
$$v_s(L - L_t) \geq v_s(L) + a \quad \text{and} \quad v_s(R - R_t) \geq v_s(R) + a \tag{5.12}$$
- $\sigma_{a+1}(L_t) \neq \sigma_{a+1}(L)$ or $\sigma_{a+1}(R_t) \neq \sigma_{a+1}(R)$. In other
$$v_s(L - L_t) < v_s(L) + a + 1 \quad \text{or} \quad v_s(R - R_t) < v_s(R) + a + 1 \tag{5.13}$$

We will assume that f, L, R, L_t, R_t are monic; the definition of the coprime index in section 2.2 is less technical for this case.

Denote $l_t = L_t - L$ and $r_t = R_t - R$. Then $L_tR_t = (L+l_t)(R+r_t) = LR + l_tR + Lr_t + l_tr_t$. Now $v_s(l_tr_t) \geq v_s(LR) + 2a \geq v_s(LR) + a + t$ and $v_s(L_tR_t - LR) \geq v_s(LR) + a + t$. Hence $l_tR + Lr_t$ (which is $L_tR_t - LR$ minus l_tr_t) has valuation $\geq v_s(LR) + a + t$ as well.

Assume $t \geq 1$. From equation (5.13) and from $v_s(l_tR + Lr_t) \geq v_s(LR) + a + t$ it follows that l_tR, or Lr_t has valuation smaller than the valuation of the sum $l_tR + Lr_t$. From this it follows that $v_s(l_tR) = v_s(Lr_t)$, and this equals $v_s(LR) + a$ by equations (5.12) and (5.13).

If a is sufficiently large (take t sufficiently large) then from the assumptions that L, L_t, R, R_t are monic and equation (5.12) it follows that $\mathrm{order}(L) = \mathrm{order}(L_t)$ and $\mathrm{order}(R) = \mathrm{order}(R_t)$. So $\mathrm{order}(l_t) < \mathrm{order}(L)$, $\mathrm{order}(r_t) < \mathrm{order}(R)$.

Let $c = l_t R + L r_t$. Perform a right-division of c by R and let q be the quotient. Then $v_s(q) \geq v_s(c) + c_1 \geq v_s(LR) + a + t + c_1$ for some constant c_1 depending only on R and order(L). Hence $v_s(q) > v_s(l_t)$ for sufficiently large t. After subtracting q from l_t and L_t (note that this does not affect $v_s(l_t)$ and $v_s(L_t)$ because $v_s(q) > v_s(l_t)$) we may assume that order$(c) <$ order(R). Then proposition 5 says that (the effect of S_e on the valuations is bounded by some constants c_2, c_6, c_7 that can be computed from L, R and s) one of the following holds

- $v_0(r_t) \geq M - c_2$ for some constant c_2. Note that $M \geq v_0(c) + c_3$ where c_3 is some constant so $v_0(r_t) \geq v_0(c) + c_4$ where c_4 is some constant. Or:
- $v_0(r_t) + c_5 + e$ is a generalized exponent of L for some generalized exponent e of R, where c_5 is a rational number between some constants c_6 and c_7.

(the names L and R are reversed in proposition 5).

If t goes to infinity, then so do a, hence $v_s(r_t)$, and hence $v_0(r_t)$. So if t is sufficiently large then the second case can not occur, and so the first case must hold. The first case says that $v_0(c) - v_0(r_t)$ is bounded from above. Then $v_s(c) - v_s(r_t)$ is bounded from above. But $v_s(r_t) = v_s(R) + a$ hence $v_s(c)$ is bounded from above by a plus some constant. Furthermore $v_s(c) = v_s(l_t R + L r_t) \geq v_s(LR) + a + t$, hence t is bounded from above, which finishes the proof.

□

Suppose $f = LR$ where f, L, R are monic elements of the commutative ring $k((x))[y]$. For each $s \in \mathbb{Q}$ a valuation v_s on $k((x))[y]$ is defined in section 2.2, and corresponding to v_s a notion of the coprime index. Using the same arguments as in the proof above, one sees that the coprime index of $f = LR$ is finite if and only if there exists a number N such that $v_s(l_t R + L r_t) - v_s(r_t) \leq N$ for all non-zero l_t, r_t with degree$(l_t) <$ degree(L) and degree$(r_t) <$ degree(R). If L, R are coprime, i.e. if $\gcd(L, R) = 1$, then such N exists by the extended Euclidean algorithm. If $\gcd(L, R) \neq 1$ one easily finds l_t, r_t, $t \in \mathbb{N}$ for which $v_s(l_t R + L r_t) - v_s(r_t)$ is not bounded from above. Hence, for a factorization $f = LR$ in $k((x))[y]$ the coprime index (with respect to v_s) is finite if and only if L, R are coprime.

Bibliography

[1] Abramov A., Bronstein M., Petkovšek M., *On polynomial solutions of linear operator equations*. Proceedings ISSAC 95, ACM Press, 290-296, (1995).

[2] Arnaudies J.-M., Valibouze A., *Résolvantes de Lagrange* Preprint, rapport L.I.T.P 93.61, Institut Blaise Pascal (Paris), (1993).

[3] Barkatou M.A., *Rational Newton Algorithm for computing formal solutions of linear differential equations*, Proceedings of ISSAC'88, ACM Press, (1988).

[4] Beckermann B., Labahn G., *A uniform approach for Hermite Padé and simultaneous Padé Approximants and their Matrix-type generalizations*, Numerical Algorithms, **3**, p. 45-54, (1992).

[5] Beckermann B., Labahn G., *A uniform approach for the fast computation of Matrix-type Padé approximants*, SIAM J. Matrix Analysis and Applications, p. 804-823, (1994).

[6] Beke E., *Die Irreduzibilität der homogenen linearen Differentialgleichungen*, Math. Ann. **45**, p. 278-294, (1894).

[7] Bertrand D., Beukers F., *Équations différentielles linéaires et majorations de multiplicités*, Ann. scient. Éc. Norm. Sup. 4 série, t. 18, p. 181-192, (1985).

[8] Beukers F., *Differential Galois theory* In: From Number Theory to Physics (Ed: Waldschmidt, Moussa, Luck, Itzykson), Springer, (1992).

[9] Bertrand D., *Théorie de Galois différentielle* Cours de DEA, Notes rédigées par R. Lardon, Université de Paris VI, (1986).

[10] Björk J.E., *Rings of Differential Operators*, North-Holland Publishing Company, (1979).

[11] Bliss G.A., *Algebraic Functions*, Dover, (1966).

[12] Bourbaki N., *Espaces vectoriels topologiques*, Paris, (1953).

[13] Bronstein M., *Linear Ordinary Differential Equations: breaking through the order two barrier*. Proceedings ISSAC 92, ACM Press, p. 42-48, (1992).

[14] Bronstein M., *An improved algorithm for factoring linear ordinary differential operators*. Proceedings ISSAC 94, Oxford, U.K., ACM Press, p. 336-340, (1994).

[15] Coddington E., Levinson N.,*Theory of ordinary differential equations*, MacGraw-Hill, (1955).

[16] Compoint E., *Équations différentielles, relations algébriques et invariants*, Thèse de Doctorat, Université de Paris 6, (1996).

[17] Derksen H., *An algorithm to compute generalized Padé-Hermite forms* Manuscript. Available by ftp at
`daisy.math.unibas.ch` in `/pub/hderksen/pade.dvi` (1994).

[18] Duval D., *Rational Puiseux expansions*, Compos. Math. 70, No. 2, p. 119-154, (1989).

[19] Della Dora J., di Crescenzo Cl., Tournier E., *An algorithm to obtain formal solutions of a linear homogeneous differential equation at an irregular singular point*, Proc. Symp. EUROCAM '82 (Lect. Notes Comput. Sci.) **144**, 273-280, (1982).

[20] van den Essen A., Levelt A.H.M., *An Explicit Description of all Simple* $k[[x]][\partial]$*-Modules*, Contemporary Mathematics, **130**, p. 121-131, (1992).

[21] Fulton W., Harris J., *Representation theory, a first course* Graduate Texts in Math. **129**, Springer, (1991).

[22] Geiselmann W., Ulmer F., *Constructing a third order differential equation*, preprint, proceedings of the 4-th Rhine Workshop on Computer Algebra, (1996).

[23] Grigor'ev D.Y., *Complexity of Factoring and Calculating the GCD of Linear Ordinary Differential Operators*. J. Symb. Comp. **10**, 7-37, (1990).

[24] Hendriks P.A., van der Put M., *Galois action on solutions of a differential equation*, J. Symb. Comp. (1995).

[25] Hendriks P.A., van der Put M., *A rationality result for Kovacic's algorithm*, ISSAC '93 Proceedings, ACM press, (1993).

[26] van Hoeij M., *Formal Solutions and Factorization of Differential Operators with Power Series Coefficients*, University of Nijmegen Report nr. 9528, submitted to J. Symb. Comp. Chapter II of this thesis.

[27] van Hoeij M., *Factorization of Differential Operators with Rational Functions Coefficients*, University of Nijmegen Report nr. 9552, submitted to J. Symb. Comp. Chapter III of this thesis.

[28] van Hoeij M., Weil J.A., *An algorithm for computing invariants of differential Galois groups*, submitted to MEGA'96, Chapter IV of this thesis.

[29] van Hoeij M., *Rational Solutions of the Mixed Differential Equation and its Application to Factorization of Differential Operators*, ISSAC'96 Proceedings. Chapter V of this thesis.

[30] Kovacic J., *An algorithm for solving second order linear homogeneous differential equations*, J. Symb. Comp **2** p. 3-43 (1986)

[31] Lang S., *Algebra* Third edition, Addison-Wesley, 1992.

[32] Levelt, A.H.M., *Jordan decomposition for a class of singular differential operators*, Arkiv för matematik, 13 (1), p. 1-27, (1975).

[33] Levelt A.H.M., *Differential Galois theory and tensor products*, Indagationes Mathematicae, 1 (4), p. 439-450, (1990).

[34] Loewy A., *Über vollständig reduzible lineare homogene Differentialgleichungen*, Math. Ann., **62**, 89-117, (1906).

[35] Malgrange, B., *Sur la réduction formelle des équations différentielles à singularités irrégulières*, Manuscript, (1979).

[36] Martinet J., Ramis J.P., *Généralités sur la théorie de Galois différentielle* In *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press, (1990).

[37] Mitschi C., Singer M.F., *The inverse problem in differential Galois theory*, preprint (proceedings of the Stokes Workshop, held in Groningen June 95, to appear), 1995

[38] van der Put M., *Singular complex differential equations: an introduction*, Nieuw Achief voor Wiskunde, 4^de serie **13**, No. 3, p. 451-470, (1995).

[39] Ore O., *Formale Theorie der linearen Differentialgleichungen (Zweiter Teil)*, J. für d. Reine u. angew. Math., **168**, p. 233-252, (1932).

[40] Ore O., *Theory of non-commutative polynomial rings*, Ann. of Math. **34** p. 480-508, (1933).

[41] Robba P., *Lemmes de Hensel pour les operateurs différentiels. Application a la reduction formelle des equations différentielles*, L'Enseignement Mathematique, Ser. II, **26**, p. 279-311, (1980).

[42] Schwarz F., *A factorization Algorithm for Linear Ordinary Differential Equations.* Proceedings of ISSAC 89, ACM Press, p. 17-25, (1989).

[43] Singer M.F., *Liouvillian solutions of n-th order homogeneous linear differential equations.* Amer.J.Mat. **103**, p. 661-682, (1981).

[44] Singer M.F., *An outline of differential Galois theory* In *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press, (1990).

[45] Singer M.F., *Liouvillian Solutions of Linear Differential Equations with Liouvillian Coefficients*, J. Symb. Comp. **11**, p. 251-273, (1991).

[46] Singer M.F., *Moduli of linear differential eq*, Pac J. Math. Vol. 160, No. 2, (1993).

[47] Singer M.F., *Testing Reducibility of Linear Differential Operators: A Group Theoretic Perspective*, Preprint, University of North Carolina, (1994). To appear in J. of Appl. Alg. in Eng. Comm. and Comp.

[48] Singer M.F., Ulmer F., *Galois groups for second and third order linear differential equations* J.Symb.Comp **16**, No. 1, p. 9-36. (1993)

[49] Singer M.F., Ulmer F., *Liouvillian and algebraic solutions of second and third order linear differential equations* J.Symb.Comp, **16**, p. 37-73, (1993).

[50] Singer M.F., Ulmer F., *Necessary conditions for liouvillian solutions of (third order) linear differential equations* J. of Appl. Alg. in Eng. Comm. and Comp. vol **6**, No 1, p. 1-22, (1995).

[51] Singer M.F., Ulmer F., *Linear differential equations and products of linear forms*, Preprint, presented at the MEGA'96 conference, (1996).

[52] Sommeling R., *Characteristic classes for irregular singularities*, Ph.D. thesis, University of Nijmegen. (1993).

[53] Springer T.A., *linear algebraic groups* Progress in maths, Birkhaüser, (1981).

[54] Tournier E., *Solutions formelles d'équations différentielles*, Thèse d'Etat, Faculté des Sciences de Grenoble, (1987).

[55] Tsarev S.P., *On the problem of factorization of linear ordinary differential operators*, Programming & computer software, v. 20, **1**, p. 27-29, (1994).

[56] Tsarev S.P., *An Algorithm for Complete Enumeration of All Factorizations of a Linear Ordinary Differential Operator*, ISSAC'96 Proceedings, (1996).

[57] Ulmer F., *Linear differential equations of prime degree (the imprimitive case)* J. Symb. Comp. vol **18**, No 4, p. 385-401, (1994).

[58] Ulmer F., Weil J.A., *Note on Kovacic's algorithm* Prepublication IRMAR 94-13, Rennes Juillet 1994 (to appear in J. Symb. Comp.).

[59] Weil J.A., *First integrals and Darboux polynomials of homogeneous linear differential systems*, Proceedings of AAECC 11 (Ed. M. Giusti & T. Mora), Lect. Notes in Comp. Sci. 948, Springer, (1995).

[60] Weil J.A., *Constantes et polynômes de Darboux en algèbre différentielle : application aux systèmes différentiels linéaires*, PhD dissertation, École Polytechnique, (1995).

Samenvatting

Voor lineaire differentiaalvergelijkingen bestaat er een Galoistheorie analoog aan die voor polynoomvergelijkingen. De Galoisgroep voor polynoomvergelijkingen kan gebruikt worden om de structuur van de oplossingen te bestuderen en om te beslissen of er exacte (uitgedrukt in geneste worteluitdrukkingen) oplossingen bestaan. De Galoisgroep van differentiaalvergelijkingen heeft soortgelijke toepassingen.

Om de Galoisgroep en eventuele exacte oplossingen te berekenen zijn een aantal algoritmische hulpmiddelen nodig. Een van die hulpmiddelen voor polynoomvergelijkingen is het factorisatie-algoritme voor polynomen. Precies hetzelfde geldt ook voor lineaire differentiaalvergelijkingen; algoritmen voor het ontbinden van differentiaaloperatoren spelen een belangrijke rol in het berekenen van exacte oplossingen en de Galoisgroep. Het hoofddoel van dit proefschrift is nu het vinden van efficiënte methoden voor het ontbinden van differentiaaloperatoren.

Er zijn al algoritmen bekend voor de ontbinding van differentiaaloperatoren. In theorie werken deze algoritmen altijd. Echter, in de praktijk kan een berekening mislukken als een algoritme meer tijd of geheugen gebruikt dan er beschikbaar is. Het mislukken van zo'n berekening is vaak het gevolg van het feit dat er bepaalde constructies gebruikt worden die een explosieve coëfficiëntengroei tot gevolg kunnen hebben. Voorbeelden van zulke constructies zijn splijtlichamen en Gröbnerbasis-berekeningen. Wil men een algoritme hebben dat minder vaak mislukt, dan moeten dit soort constructies dus vermeden worden. De moeilijkheid van het vinden van een goed algoritme is dus dat men werkt met een handicap: de bedoeling is het vinden van een algoritme, maar een aantal constructies die dit eenvoudig zouden maken mag men uit efficiëntie-overwegingen niet gebruiken. Deze handicap heeft men niet als men alleen wil aantonen dat een gegeven probleem berekenbaar is, dat is dus niet hetzelfde probleem als het vinden van een goed algoritme. Het belangrijkste resultaat in dit proefschrift is dus niet zomaar een algoritme voor de ontbinding van differentiaaloperatoren, maar een algoritme dat geen gebruik maakt van splijtlichamen of Gröbnerbasis-berekeningen. Gezien vanuit de vorige methoden, die gebaseerd zijn op Beke's algoritme, lag het niet voor de hand dat zo'n algoritme mogelijk was.

Voor ontbinding van polynomen in $\mathbb{Q}[x]$ beschouwt men gewoonlijk eerst locale ontbindingen; dat wil zeggen ontbindingen over F_p of de p-adische getallen. Voor differentiaaloperatoren volgen we dezelfde strategie. Daarom worden in hoofdstuk 2 eigenschappen van locale differentiaaloperatoren bestudeerd. Het doel hiervan is de toepassing in hoofdstuk 3, de ontbinding van globale (dat wil zeggen: met rationale coëfficiënten) differentiaaloperatoren. Een aantal bekende feiten over locale differentiaaloperatoren worden in hoofdstuk 2 op een andere manier herschreven. Een voorbeeld daarvan zijn de zogenaamde “exponential parts”. In zekere zin zijn deze al bekend in de vorm van “normalized eigenvalues” en “characteristic classes” in Ron Sommeling’s proefschrift. Er zijn echter subtiele verschillen. In de definitie van de characteristic classes wordt gebruik gemaakt van de Jordan-Hölder stelling, impliciet wordt dus gebruik gemaakt van een ontbinding. Echter, in plaats van ontbindingen te gebruiken om characteristic classes uit te rekenen, willen we juist precies het omgekeerde, namelijk een dergelijk begrip gebruiken om locale differentiaaloperatoren te kunnen ontbinden. Daarom wordt in paragraaf 2.6 een alternatieve aanpak gegeven; er wordt een definitie van exponential parts gegeven die berekend kan worden zonder dat een volledig factorisatie-algoritme (zie paragraaf 2.7) nodig is. Deze aanpak is wat technisch, maar wel praktisch voor de doeleinden in dit proefschrift.

In hoofdstuk 3 gaat het om het ontbinden van differentiaaloperatoren met rationale functies als coëfficiënten. We kunnen een differentiaaloperator f eerst locaal ontbinden en locale rechtsfactoren r vinden. Een van de resultaten in hoofdstuk 3 is dat het mogelijk is om, gegeven r, een operator R van minimale orde te vinden zodanig dat r een rechtsfactor van R is. Dan is R een rechtsfactor van f. Echter, men heeft goede kans dat R gelijk aan f is. De kunst is dus het vinden van een locale rechtsfactor van f, die tevens rechtsfactor is van een niet-triviale globale factor van f. Men kan dit ook als volgt formuleren: gezocht wordt een deelruimte van een niet-triviale G-invariante deelruimte van de oplossingsruimte van f, waar G de differentiaal-Galoisgroep is. In deze formulering is de methode in hoofdstuk 3 het eenvoudigst te begrijpen; de “exponential parts” geven op een natuurlijke wijze een directe-som splitsing van de oplossingsruimte van f. Dit helpt bij het vinden van een deelruimte met de gewenste eigenschappen. Het verband met oplossingsruimten wordt echter alleen gebruikt om het algoritme uit te leggen, het algoritme zelf rekent met locale factoren in plaats van met oplossingen. Dit is equivalent vanwege het verband tussen rechtsfactoren en deelruimten van de oplossingen.

Hoofdstuk 4 is gezamelijk werk met Jacques-Arthur Weil. Dit hoofdstuk gaat over het berekenen van invarianten van de differentiaal-Galoisgroep. Locale berekeningen gecombineerd met het idee om gebruik te maken van zogenaamde “dual first integrals” vormen hier de basis van een efficiënte methode om de invarianten te berekenen.

In hoofdstuk 5 gaat het om het berekenen van de rationale oplossingen van de zogenaamde “gemengde vergelijking”. Dit kan dan toegepast worden voor de ontbinding van differentiaaloperatoren. Voor dit doel wordt gebruik gemaakt van de “gegeneraliseerde exponenten” van differentiaaloperatoren, die geïntroduceerd zijn in hoofdstuk 3. De belangrijkste benodigde eigenschap is dat het aantal gegeneraliseerde exponenten, geteld met multipliciteiten, altijd gelijk is aan de orde van de operator. Voor de klassiek bekende exponenten geldt dit alleen in het regulier singuliere geval, vandaar dat voor het irregulier singuliere geval een veralgemening nodig is.

Curriculum Vitae

Ik ben geboren te Someren op 16 augustus 1969. Tijdens mijn studie wiskunde aan de Katholieke Universiteit Nijmegen raakte ik geïntereseerd in de computeralgebra. In deze richting ben ik afgestudeerd op 26 november 1992. Vanaf 1 december 1992 tot 1996 werk ik onder leiding van Prof. Dr. A.H.M. Levelt als assistent in opleiding bij de vakgroep wiskunde te Nijmegen. Mijn werk in de computeralgebra gedurende deze vier jaar heeft zich gericht op twee onderwerpen: algoritmen voor differentiaaloperatoren en algoritmen voor algebraïsche krommen. Ik heb computerprogramma's en 4 artikelen geschreven voor elk van beide onderwerpen. Mijn werk op het gebied van de differentiaaloperatoren vindt U in dit proefschrift.