

RWTH Aachen University
Lehrstuhl D für Mathematik
Prof. Dr. rer. nat. Eva Zerz

Master Thesis

Factorization, Similarity and Matrix Normal Forms
over certain Ore Domains.

Kandidat: Albert Heinle
Betreuer: Dr. rer. nat. Viktor Levandovskyy
Zweitgutachter: Prof. Dr. rer. nat. Wilhelm Plesken
Beginn: 01.04.2012
Abgabe: 31.09.2012

Ich, Albert Heinle, geboren am 23.09.1986 in Lebedinowka, versichere hiermit an Eides statt, dass ich die hier vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen als Hilfsmittel benutzt und Zitate aus den Quellen kenntlich gemacht habe.

Unterschrift: Albert Heinle

Contents

Introduction	3
1. Preface	3
Acknowledgements	4
2. Basic Notations, Definitions and Results	5
Chapter 1. Factorization	11
Overview	11
1. Homogeneous Polynomials in the First q -Weyl Algebra	11
1.1. Properties of the First q -Weyl Algebra	11
1.2. Factorization of Homogeneous Polynomials in the First q -Weyl Algebra	14
2. Factorization in the Polynomial First Weyl Algebra	17
2.1. <code>ncfactor.lib</code>	17
2.1.1. Quick Reference of <code>ncfactor.lib</code>	17
2.2. A New Approach	18
2.2.1. Preliminaries	18
2.2.2. Determine the Rest of the Homogeneous Summands	19
2.2.3. Preliminary Filtering of Combinations	20
2.2.4. Determination of the Remaining Homogeneous Summands	21
2.2.5. Experimental Implementation and Timings	27
3. The Rational First Weyl Algebra	29
3.1. Localizations in Ore Algebras	30
3.2. Relations between Factorizations: Polynomial vs. Rational	31
3.3. Applications	33
Chapter 2. Similarity	35
Overview	35
1. Similarity in the Polynomial First Weyl Algebra	36
1.1. Similarity of Homogeneous Polynomials	36
1.2. Similarity between a Homogeneous Polynomial and an Inhomogeneous One	40
1.3. Similarity between Two Inhomogeneous Polynomials	48
1.4. Summarizing the Results for the Polynomial First Weyl Algebra	55
2. Similarity in the Rational First Weyl Algebra et al.	55
Chapter 3. Matrix Normal Forms	58
1. Linear Algebra over Ore Domains	58
1.1. Basic Notions	58
1.2. Subresultant Theory for Ore Polynomials	60
1.3. The Hermite Normal Form	62

1.4. The Jacobson Normal Form	63
2. Excursion to Vegas	65
3. On Divisibility	66
4. From Hermite to Jacobson	70
4.1. Experimental Implementation and Results	72
4.2. Degree Bounds and Complexity	73
5. Application to other Ore Domains	74
5.1. Jacobson Normal Forms over the Rational Shift Algebra	74
5.2. What the Shift Case Has Shown Us	77
Conclusion and Future Work	80
Bibliography	82
Appendix	84
From Chapter 1	84
In Subsection 2.2.5	84
From Chapter 2	85
5.3. In Subsection 1.3	85
From Chapter 3	87
In Subsection 5.1	87

Introduction

1. Preface

Factorization, Similarity and Matrix Normal forms over certain Ore domains – as the reader could already see in the table of contents, this thesis works off all three of those topics chapter by chapter.

As incoherent as those topics may seem from the first look, they all have connecting concepts. The topic of similarity – all the notions will be defined later – plays a role in the question of factorization in Ore domains, as well as in the topic of matrix normal forms in noncommutative rings. In the first it is known that the factors of different factorizations are unique up to similarity, and in the so-called Jacobson normal form, which is a generalization of the Smith normal form for commutative principal ideal domains, the diagonal entries are also unique up to similarity. Therefore, the second chapter is the connecting trajectory between the first and the last one.

The motivation for dealing with factorizations in certain Ore extensions came from the Bachelor thesis that was written by the author in 2010. There was a new technique developed to approach the factorization question in graded skew polynomial rings. An implementation especially for the first Weyl algebra was written in the computer algebra system SINGULAR, and due to its good performance especially for homogeneous polynomials, it was added to the SINGULAR distribution. By now, we also added an algorithm to factorize homogeneous polynomials in the first q -Weyl algebra. The main ideas will be presented here.

The design of the algorithm for the first Weyl algebra was not yet optimal, and for complexity reasons the implementation was not able to factorize a special family of polynomials, even though they are reducible. In this thesis we will optimize the approach and make use of some new insights we gained about the first Weyl algebra. This will lead to a modification of the original algorithm that fixes the old problems. Also an experimental implementation is given, and it will appear that it beats the old one in performance as well as in the accuracy of the solutions.

We will also discuss the question about factorization in the rational first Weyl algebra, as it seems to be the most relevant for practice regarding some current problems in the field of computer algebra. For example, a factorization of an element in the rational first Weyl algebra is needed in an approach for the computation of the differential Galois group for a given operator. We will show that there exists actually a generalization of the Gauss Lemma for the noncommutative case; this means, we will show that it suffices to deal with a polynomial factorization in order to obtain representative factors for the rational factorizations.

The motivation for dealing with similarity of polynomials came actually from the last chapter. There, a polynomial time algorithm for computing the Jacobson form of a given matrix in the rational first Weyl algebra is presented. This is the outcome of a joint work with Prof. Mark Giesbrecht during a research internship the author did in 2011 at the University of Waterloo, Ontario, Canada. As already mentioned above, the diagonal elements in the Jacobson normal form are unique up to similarity. As we will see, the size of the polynomials in terms of coefficients can differ enormously between normal forms of the same matrix. An empirical monitoring of different similar polynomials lead to the observation, that not so much various degree notions, but the coefficients in the underlying field \mathbb{K} form the main difference. We will try to find an explanation for that strange fact using our knowledge we gathered from the factorization problem. In the end, we will obtain a point of view for that problem that has a potential to lead to a way to simplify a given polynomial to a certain extent using similarity transformations.

In the last chapter, we will talk about techniques for finding the Jacobson normal form using noncommutative generalizations of concepts like the Smith normal form and divisibility conditions. It will also serve as a little round trip through the field of matrix theory in Ore domains. We will see a generalization of old friends like the resultants, and some concepts for algorithms using random parameters will be presented. The thesis will end with a notion of a strong Jacobson normal form that we developed for the rational first shift algebra. We will also give a family of algebras for which the same structural property of the Jacobson normal form is given.

Acknowledgements

First of all I acknowledge Viktor Levandovskyy for his great support in the last years, especially when writing this thesis. He was always accessible for questions and seem never to lose motivation to teach me new insights and to give me different points of views on the problems in this thesis. Furthermore, he always opened doors for me when it was possible and helped me on whatever project I was contacting him on for help.

I acknowledge Eva Zerz for agreeing to supervise this thesis and let me write about this topic. She was always accessible and provided me patiently with a great support at any time.

I acknowledge Daniel Andres for being a good contact person for questions of mine in the process of writing this thesis.

I acknowledge Mark Giesbrecht from the University of Waterloo for giving me the possibility to make a research internship at his department in Canada in summer 2011 and for his great hospitality there. It was a fruitful time, and part of this thesis is a result of our joint work there. The possibility for me to go there was provided by the international office at RWTH Aachen University, who granted me a scholarship as Research Ambassador. I thank the responsible persons there for it.

I acknowledge my family for being very supportive especially in the last five years of my study. They were always there for me and I love the way how we treat each other.

I acknowledge my friends for giving me great support in difficult, and great fun in good times and that they always let me be my true self and take me as I am, even though it might be exhausting sometimes.

Also for those who I might have forgotten here: Thank you all.

2. Basic Notations, Definitions and Results

We are going to make – besides some new ones – highly use of the notations, definitions and results that were already stated in [Hei10]. We will not give much details here, as the reader can find them and references for further reading on that topics in the Bachelor thesis. We will have as a general assumption that the reader is familiar with the contents of that thesis. Therefore, we will run through the basics. In this section, we will give an overview of what we will use in the proceeding of this thesis.

Further General Assumption: The reader is familiar with the computer algebra system SINGULAR (see [GP07]) and its noncommutative subsystem SINGULAR:PLURAL (see [Lev05]). Also a general knowledge about MAPLE and REDUCE is useful.

- If not specified otherwise, R (and any otherwise named ring) will denote a nonzero not necessarily commutative ring with 1.
- \mathbb{N} represents the natural numbers without zero.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the sets of the integer, rational, real and complex numbers.
- \mathbb{K} represents an arbitrary field of characteristic zero, \mathbb{F}_n denotes a finite field with $n \in \mathbb{N}$ elements.
- A ring homomorphism $\varphi : R \rightarrow S$ always maps 1_R to 1_S .
- Given a ring R , let $R[x_1, \dots, x_n]$ denote the associated polynomial ring. The leading coefficient of a polynomial f – with respect to a given order – will be denoted by $\text{lc}(f)$, and the leading monomial (without the coefficient) by $\text{lm}(f)$. For the degree, we will write $\text{deg}(f)$ (if not specified, we will always mean the total degree).
- Let $n \in \mathbb{N}$. Then \underline{n} denotes the set $\{1, \dots, n\} \subset \mathbb{N}$.

DEFINITION 2.1. Let $r, s \in R$. We say r is a **right divisor** of s (or s is a left multiple of r), if there exists at least one $q \in R$ with $s = qr$. We then write $r \mid_r s$. **Left divisibility** is defined in a similar way and denoted by $r \mid_l s$. When we write $r \mid s$, then it will either be specified in the text whether we mean division on the left hand side or on the right hand side or if no context is given, it means that $r \mid_r s$ as well as $r \mid_l s$.

DEFINITION 2.2. For a, b in a domain R , $\text{lclm}(a, b)$ denotes the **least common left multiple** of a and b , $\text{lcrm}(a, b)$ the **least common right multiple**. The – unique up to multiplication by a unit – element $\text{lclm}(a, b)$ is defined by the property that there exist $r, s \in R$, such that $ra = sb = \text{lclm}(a, b)$ and for every other common left multiple f of a and b it holds that $\text{lclm}(a, b) \mid_r f$. The definition for $\text{lcrm}(a, b)$ is given in an analogous way. If we do not care from which side we multiply or if it is clear from the context, we will just write lcm .

A **greatest common left divisor** of a, b is denoted by $\text{gcl}(a, b)$ and a **greatest common right divisor** by $\text{gcr}(a, b)$. An element $\text{gcl}(a, b)$ is defined in the way that $\text{gcl}(a, b) \mid_l a$, $\text{gcl}(a, b) \mid_l b$ and for every other left divisor g of a and b it holds that $g \mid_l \text{gcl}(a, b)$. The greatest common right divisor is defined in a similar way. If we do not care on which side we are searching for a common divisor or if it is clear from the given context, we will just write $\text{gcd}(a, b)$.

DEFINITION 2.3. An additive subgroup I of R is said to be a **left ideal** of R , if the following condition holds:

$$\forall r \in R, x \in I : rx \in I.$$

Analogously we define a **right ideal**. If I is both a left and a right R -ideal, then we call I a **two-sided** ideal of R .

If a left ideal I in R is generated by elements $e_1, \dots, e_n \in R, n \in \mathbb{N}$, we denote that by

$$I =: {}_R\langle e_1, \dots, e_n \rangle.$$

Analogously, if a right ideal I in R is generated by those elements, we denote that by

$$I =: \langle e_1, \dots, e_n \rangle_R.$$

Now we will introduce a new notion of divisibility, namely the concept of total divisibility. This definition appears to be nonintuitive at the first glance. It is motivated by the so-called Jacobson normal form mentioned in the preface.

DEFINITION 2.4 (see [Jac43], Chapter 3). Let R be a left and a right principal ideal domain. We call $a \in R$ a **total divisor** of $b \in R$, if there exists a two-sided ideal I in R , such that $\langle b \rangle_R \subseteq I \subseteq \langle a \rangle_R$. (In this definition, we can also work with left ideals instead of right ideals).

DEFINITION 2.5. An abelian group $(M, +)$ endowed with a scalar multiplication

$$R \times M \rightarrow M : (r, m) \mapsto rm$$

satisfying the following properties for any $r, s \in R$ and $m, n \in M$:

- (1) $(r + s)m = rm + sm$
- (2) $r(m + n) = rm + rn$
- (3) $(rs)m = r(sm)$
- (4) $1m = m$

is called a **left R -module**. **Right R -modules** are defined similarly.

REMARK 2.6. Recall that for a one sided ideal $I \subseteq R$, the set of residue classes R/I is in general not a ring as it is common if R is commutative, but a module over R .

Convention: If we are talking about an ideal or a module without specifying whether we mean a left, right, or two-sided one, then it will always be a left one.

DEFINITION 2.7. Let R be a domain and let $0 \neq f, g \in R$. We call f and g **similar**, if one of the following equivalent conditions are fulfilled.

- (a) $R/\langle f \rangle \cong R/\langle g \rangle$
- (b) $R/\langle f \rangle_R \cong R/\langle g \rangle_R$ (compare [BGTV03], Definition 4.9 and Lemma 4.11)
- (c) There exist elements $a, b \in R$, such that $af = gb$ and ${}_R\langle f, b \rangle = \langle a, g \rangle_R = R$. (see [Jac43], Theorem 31)

If R is furthermore a principal ideal domain, then those conditions are also equivalent to

- (d) There exists a $u \in R$, such that $g = \text{lcm}(f, u)u^{-1}$ (also due to [Jac43], Chapter 3).

REMARK 2.8. Item d) in the definition above might be confusing in the sense that we seem to multiply by an inverse of u in $g = \text{lcm}(f, u)u^{-1}$. What we actually mean by that is the extraction of the coefficient – in this case g – that we need to multiply to u from the left in order to obtain $\text{lcm}(f, u)$.

DEFINITION 2.9. Let σ be a ring endomorphism of R . A σ -**derivation** of R is an additive endomorphism $\delta : R \rightarrow R$ with the following property:

$$\forall r, s \in R : \delta(rs) = \sigma(r)\delta(s) + \delta(r)s.$$

We will call the pair (σ, δ) a **quasi-derivation** of R . For our purposes, we will assume σ to be an automorphism if not specified otherwise.

DEFINITION 2.10. Let (σ, δ) be a quasi-derivation on R . Then there exists a ring S with the following properties:

- (1) R is a subring of S .
- (2) There exists an element $x \in S$, such that S is freely generated as a left R -module by the non-negative powers $1, x, x^2, \dots$ of x .
- (3) $\forall r \in R : xr = \sigma(r)x + \delta(r)$.

This ring S is a skew polynomial ring and called an **Ore extension of R** , and is further denoted by $R[x; \sigma, \delta]$. (**Convention:** If σ is the identity function, then we will just write $R[x; \delta]$. If $\delta \equiv 0$, then we will denote S by $R[x; \sigma]$.)

Most of the time we are going to deal with Ore algebras in this thesis. Those are Ore extensions of the polynomial ring $\mathbb{K}[x_1, \dots, x_n]$. The most relevant for us will be defined now.

DEFINITION 2.11. The n **th q -Weyl algebra** Q_n for $n \in \mathbb{N}$ is defined as the n times Ore extension of $\mathbb{K}[x_1, \dots, x_n]$ given by

$$Q_n := \mathbb{K}[x_1, \dots, x_n][\partial_1, \dots, \partial_n; (\sigma_1, \delta_1), \dots, (\sigma_n, \delta_n)]$$

where q is a unit in \mathbb{K} , the σ_i are defined by

$$\sigma_i(x_j) = \begin{cases} qx_j, & \text{if } i = j \\ x_j, & \text{otherwise} \end{cases}$$

and $\delta_i := \frac{\partial}{\partial x_i}$ for all $i, j \in \underline{n}$. Q_1 is the operator algebra associated to

$$\partial_q : f(x) \mapsto \frac{f(qx) - f(x)}{(q-1)x},$$

also known as the q -derivative, where $f \in \mathbb{K}[x]$. For further reading consider [KC02].

For $q = 1$, the operator is still well defined. This can be seen in the following way. Let $f = \sum_{i=0}^n a_i x^i$, where $n \in \mathbb{N}_0$ and $a_i \in \mathbb{K}$. Then

$$f(qx) - f(x) = \sum_{i=0}^n a_i (qx)^i - \sum_{i=0}^n a_i x^i = \sum_{i=0}^n a_i x^i (q^i - 1).$$

The expression $q - 1$ is clearly a divisor of $q^i - 1$, and we obtain

$$\frac{f(qx) - f(x)}{(q - 1)x} = \sum_{i=1}^n a_i x^{i-1} \left(\sum_{j=0}^{i-1} q^j \right).$$

For the special case where $q = 1$ we have the n th **Weyl algebra**, which is denoted by A_n .

If we are dealing with the Ore extension given by the same (σ_i, δ_i) as above for $\mathbb{K}(x_1, \dots, x_n)$, we call this the n th **rational q -Weyl algebra** resp. for $q = 1$ the n th **rational Weyl algebra**.

DEFINITION 2.12. The n th **q -shift algebra** \mathcal{Q}_n for $n \in \mathbb{N}$ is defined as the n times Ore extension of $\mathbb{K}[x_1, \dots, x_n]$ given by

$$\mathcal{Q}_n := \mathbb{K}[x_1, \dots, x_n][S_1, \dots, S_n; \sigma_1, \dots, \sigma_n],$$

where q is a unit in \mathbb{K} and the σ_i are defined by

$$\sigma_i(x_j) = \begin{cases} q(x_j + 1), & \text{if } i = j \\ x_j, & \text{otherwise} \end{cases}$$

for all $i, j \in \underline{n}$.

For $q = 1$, we have the special case of the n th **shift algebra**, which is denoted by \mathcal{S}_n .

Again, if we are dealing with the Ore extension given by the same σ_i for $i \in \underline{n}$ as above for $\mathbb{K}(x_1, \dots, x_n)$, we call this the n th **rational q -shift algebra** resp. for $q = 1$ the n th **rational shift algebra**.

If we slightly modify the commutation rules for x_i and S_i above to $S_i x_i - q x_i S_i = 0$, we call the resulting algebra the **ring of n th quantum polynomials**.

REMARK 2.13. Different to \mathcal{Q}_n and A_n , the n th quantum algebra and the n th q -shift algebra are isomorphic. This was proven by Levandovskyy, Koutschan and Motsak in [LKM11].

DEFINITION 2.14. Let $R[x_1, \dots, x_n], n \in \mathbb{N}$ be the ring of multivariate polynomials with coefficients in R , and let $\omega \in \mathbb{R}^n$. Then the **weighted degree** with respect to ω of a monomial $\prod_{i=1}^n x_i^{\alpha_i}, \alpha_i \in \mathbb{N}_0$ for all $i \in \underline{n}$ is defined by

$$\deg_{\omega} \left(\prod_{i=1}^n x_i^{\alpha_i} \right) = \sum_{i=1}^n \omega_i \cdot \alpha_i.$$

The degree of a nonzero polynomial is as usual defined as the maximum of the degrees of its monomials. We will further call ω the **weight vector**. We will also denote $\deg_{\omega}(f)$ for $f \in R[x_1, \dots, x_n]$ and a given ω as the ω -**degree** of f .

For our work we will also need a more general concept of degree for an element in a ring R , which is also applicable if we assume an indeterminate in a polynomial ring to be given rational – like in the rational Weyl algebra.

DEFINITION 2.15. Let Γ be an ordered group and R be a ring. A **valuation** on R – if it exists – with values in Γ is a function

$$\nu : R \rightarrow \Gamma \cup \{\infty\},$$

where the symbol ∞ satisfies the conditions

- $\infty > a$,
- $a + \infty = \infty + a = \infty + \infty = \infty$ for all $a \in R$,

and ν satisfies the following properties for all $a, b \in R$:

- $|\text{im}(\nu)| \geq 2$,
- $\nu(a + b) \geq \min(\nu(a), \nu(b))$,
- $\nu(ab) = \nu(a) + \nu(b)$.

EXAMPLE 2.16. There exists a \mathbb{Z} -valuation ν on the polynomial ring $\mathbb{K}(x)$ given by

$$\nu\left(\frac{f}{g}\right) := \deg(f) - \deg(g),$$

where f and g are in $\mathbb{K}[x]$.

DEFINITION 2.17. A **graded ring** is a ring $R = (R, +, \cdot)$ with a family $\{T_n, n \in G\}$ of subgroups of $(R, +)$, where G is a commutative ordered monoid, such that for all $(i, j) \in G \times G$:

- (1) $T_i T_j \subseteq T_{i+j}$
- (2) $\bigoplus_n T_n = R$

The family $\{T_n\}$ is called a **G -grading** or simply a grading on R . Elements of T_n are then called **homogeneous of degree $n \in G$** (with respect to this grading).

As already known, there is a nontrivial \mathbb{Z} -grading on the first Weyl algebra A_1 induced by the weight vector $\omega := [-u, u]$ for $u \in \mathbb{Z} \setminus \{0\}$. For simplicity, we always set $u := 1$.

DEFINITION 2.18. The graded parts of A_1 with respect to the weight vector $[-1, 1]$ are denoted by $A_1^{(k)}$ for $k \in \mathbb{Z}$ and we have

$$A_1^{(k)} = \left\{ \sum_{j-i=k} r_{i,j} x^i \partial^j \mid i, j \in \mathbb{N}_0, r_{i,j} \in \mathbb{K} \right\}.$$

Convention: Let $f \in A_1$. If not specified otherwise, we set $\deg(f) := \deg_{[-1,1]}(f)$. With a slight abuse of notation, we write $\deg_x(f)$ for $\deg_{[1,0]}(f)$ and $\deg_\partial(f)$ for $\deg_{[0,1]}(f)$. Furthermore, if we are dealing with the rational first Weyl algebra, we denote by $\deg_x(f)$ the maximum of the valuations of the coefficients of ∂ given by the valuation ν introduced in Example 2.16.

DEFINITION 2.19. If we talk about θ in the context of the first Weyl algebra A_1 , we always mean

$$\theta := x\partial.$$

LEMMA 2.20 (Compare with [SST00]). *In A_1 , the following equations do hold:*

$$\begin{aligned} \theta x^m &= x^m(\theta + m) \\ \theta \partial^m &= \partial^m(\theta - m), m \in \mathbb{N}. \end{aligned}$$

COROLLARY 2.21. *Consider $f(\theta) := f \in \mathbb{K}[\theta]$. Then for all $n \in \mathbb{N}$:*

$$\begin{aligned} f(\theta)x^n &= x^n f(\theta + n) \\ f(\theta)\partial^n &= \partial^n f(\theta - n) \end{aligned}$$

We are going to use those formulas from Corollary 2.21 frequently, especially in Chapter 2 and Chapter 1. They will appear in context of larger terms. Therefore it is advisable to introduce a notation in order to distinguish between the multiplication by a θ -polynomial and the application of an affine transform of θ in a given function.

Convention: Given $f := \sum_{i=0}^n f_i \theta^i, p := \sum_{i=0}^{\tilde{n}} p_i \theta^i \in \mathbb{K}[\theta]$, where $n, \tilde{n} \in \mathbb{N}_0$ and $f_i, p_i \in \mathbb{K}$. If it is not clear from the context whether we mean by fp the multiplication of f and p or the application of p to f , i.e. $fp = \sum_{i=0}^n f_i(p)^i$, we will denote the application by

$$f \circ p.$$

The \circ will bind stronger than the multiplication operator. Furthermore, the \circ just refers to the rightmost function on its left hand side.

THEOREM 2.22. *Let $m \in \mathbb{N}$. Then the following identities in A_1 are true:*

$$x^m \partial^m = \prod_{i=0}^{m-1} (\theta - i), \quad \partial^m x^m = \prod_{i=1}^m (\theta + i)$$

THEOREM 2.23. *$A_1^{(0)}$ is a ring and finitely generated, as a \mathbb{K} -algebra, by the element θ . $A_1^{(k)}$ are finitely generated $A_1^{(0)}$ -modules by the element x^{-k} , if $k < 0$, or by ∂^k , if $k > 0$.*

LEMMA 2.24. *The polynomials θ and $\theta + 1$ are the only irreducible monic elements in $\mathbb{K}[\theta]$ that are reducible in A_1 .*

CHAPTER 1

Factorization

Overview

In this chapter, we will first deal with the current developments of the implementation for factoring elements in the first Weyl algebra from the Bachelor thesis. This contains the approach to factor homogeneous polynomials in the first q -Weyl algebra and some additional algorithm we implemented in SINGULAR. We will see, that the techniques for that are very similar to the ones we had for homogeneous polynomials in the first Weyl algebra. After discussing that, we will go on with the modification of our current algorithm for inhomogeneous polynomials in the first Weyl algebra. This will contain the main idea and benchmarks of an experimental implementation against the old one and others in MAPLE and REDUCE. We will finish this chapter with the factorization question for the rational first Weyl algebra, which contains also a little excursion into localization theory of noncommutative rings and an application from the field of differential Galois theory.

1. Homogeneous Polynomials in the First q -Weyl Algebra

“There’s just a slight difference in the spelling between Hard working and Hardly working but once either is followed can lead to results with greatest variations.” – Ritika Bawa Chopra, Indian author

In the Bachelor thesis [Hei10] we dealt with the factorization question especially for the first Weyl algebra and we presented an ansatz how we can use similar techniques for the first shift algebra.

In the shift algebra, dealing with homogeneous polynomials – using the $[0, 1]$ weight vector – appeared to be even easier than in the first Weyl algebra. But when we consider the first q -Weyl algebra, things become a little bit more complicated in terms of formulas we are using. We are going to discuss some properties the first q -Weyl algebra has and at the end we will see how we can factorize homogeneous polynomials there.

1.1. Properties of the First q -Weyl Algebra. Here, we are going to find analogous statements for the first q -Weyl algebra as we have them for the first Weyl algebra.

First of all, the first q -Weyl algebra possesses a nontrivial \mathbb{Z} -grading using the weight vector $[-v, v]$ for a $v \in \mathbb{Z}$. For simplicity, we will choose $v := 1$. Therefore, the n th graded

part of Q_1 is given by

$$Q_1^{(n)} := \left\{ \sum_{j-i=n} r_{i,j} x^i \partial^j \mid i, j \in \mathbb{N}_0, r_{i,j} \in \mathbb{K}(q) \right\}.$$

Define $\theta := x\partial$. Our aim is to obtain Theorem 2.25 from [Hei10] also for the first q -Weyl algebra. Some preparational work is needed for that.

DEFINITION 1.1. For $n \in \mathbb{N}$, we define the q -**bracket** $[n]_q$ by

$$[n]_q := \frac{1 - q^n}{1 - q} = \sum_{i=0}^{n-1} q^i.$$

LEMMA 1.2. In Q_1 , for $\theta := x\partial$, the following commutation rules do hold:

$$\begin{aligned} \theta x^n &= x^n (q^n \theta + [n]_q) \\ \theta \partial^n &= \frac{\partial^n}{q} \left(\frac{\theta - 1}{q^{n-1}} - \frac{q^{-n+2} - q}{1 - q} \right). \end{aligned}$$

PROOF. We prove our claim using induction by n :

$n = 1$: We have

$$\theta \partial = x \partial \partial = \frac{\partial x - 1}{q} \partial = \frac{\partial}{q} (x \partial - 1) = \frac{\partial}{q} (\theta - 1) = \frac{\partial^1}{q} \left(\frac{\theta - 1}{q^{1-1}} - \frac{q^{-1+2} - q}{1 - q} \right)$$

and

$$\theta x = x \partial x = x (q x \partial + 1) = x (q \theta + 1) = x (q^1 \theta + \frac{1 - q^1}{1 - q})$$

Now let the equations be true for an arbitrary, but fixed $n \in \mathbb{N}$. We prove it for $n + 1$:

$$\begin{aligned} \theta \partial^{n+1} &= (\theta \partial^n) \partial \\ &= \left(\frac{\partial^n}{q} \left(\frac{\theta - 1}{q^{n-1}} - \sum_{i=0}^{n-2} q^{-i} \right) \right) \partial \\ &= \frac{\partial^n}{q} \left(\frac{\theta \partial - \partial}{q^{n-1}} - \partial \sum_{i=0}^{n-2} q^{-i} \right) \\ &= \frac{\partial^n}{q} \left(\frac{\frac{\partial}{q} (\theta - 1) - \partial}{q^{n-1}} - \partial \sum_{i=0}^{n-2} q^{-i} \right) \\ &= \frac{\partial^{n+1}}{q} \left(\frac{\theta - 1}{q^n} - q^{-(n-1)} - \sum_{i=0}^{n-2} q^{-i} \right) \\ &= \frac{\partial^{n+1}}{q} \left(\frac{\theta - 1}{q^n} - \sum_{i=0}^{n-1} q^{-i} \right), \end{aligned}$$

$$\begin{aligned}
\theta x^{n+1} &= (\theta x^n)x \\
&= \left(x^n (q^n \theta + \sum_{i=0}^{n-1} q^i) \right) x \\
&= x^n \left(q^n \theta x + x \sum_{i=0}^{n-1} q^i \right) \\
&= x^n \left(q^n (qx\theta + x) + x \sum_{i=0}^{n-1} q^i \right) \\
&= x^{n+1} \left(q^{n+1} \theta + q^n + \sum_{i=0}^{n-1} q^i \right) \\
&= x^{n+1} \left(q^{n+1} \theta + \sum_{i=0}^n q^i \right).
\end{aligned}$$

Using the equalities

$$\sum_{i=0}^{n-1} q^i = \frac{1-q^n}{1-q}, \text{ and } \sum_{i=0}^{n-2} q^{-i} = \frac{q^{-n+2}-q}{1-q},$$

we obtain the desired results. \square

COROLLARY 1.3. *Consider $f(\theta) := f \in \mathbb{K}(q)[\theta]$, $\theta := x\partial$. Then for all $n \in \mathbb{N}$:*

$$\begin{aligned}
f(\theta)x^n &= x^n f(q^n \theta + [n]_q) \\
f(\theta)\partial^n &= \partial^n f \left(\frac{1}{q} \left(\frac{\theta-1}{q^{n-1}} - \frac{q^{-n+2}-q}{1-q} \right) \right)
\end{aligned}$$

In the case of the first Weyl algebra, we tried to write each element of the zero homogeneous part $A_1^{(0)}$ as a polynomial in $\mathbb{K}(q)[\theta]$. The next lemma and its corollary will show that this is also possible for $Q_1^{(0)}$.

LEMMA 1.4. *We have*

$$x^n \partial^n = \frac{1}{q^{T_{n-1}}} \prod_{i=0}^{n-1} \left(\theta - \sum_{j=0}^{i-1} q^j \right) = \frac{1}{q^{T_{n-1}}} \prod_{i=0}^{n-1} (\theta - [i]_q)$$

for $n \in \mathbb{N}_0$, where T_i denotes the i th triangular number, i.e.

$$T_i := \sum_{j=0}^i j = \frac{i(i+1)}{2}$$

for all $i \in \mathbb{N}_0$.

PROOF. Using induction by n .

$n = 1$:

$$x\partial = \theta = \frac{1}{q^{T_0}} \prod_{i=0}^0 \left(\theta - \sum_{j=0}^{i-1} q^j \right).$$

Now let $n \in \mathbb{N}$ be arbitrary, but fixed.
 $n \mapsto n + 1$:

$$\begin{aligned}
x^{n+1}\partial^{n+1} &= x^n\theta\partial^n \\
&= \frac{x^n\partial^n}{q} \left(\frac{\theta - 1}{q^{n-1}} - \sum_{i=0}^{n-2} q^{-i} \right) \\
&= \frac{x^n\partial^n}{q} \left(\frac{\theta - \sum_{i=0}^{n-1} q^i}{q^{n-1}} \right) \\
&= \frac{\prod_{i=0}^{n-1} (\theta - \sum_{j=0}^{i-1} q^j)}{q^{T_{n-1}+1}} \left(\frac{\theta - \sum_{i=0}^{n-1} q^i}{q^{n-1}} \right) \\
&= \frac{\prod_{i=0}^n (\theta - \sum_{j=0}^{i-1} q^j)}{q^{T_n}}
\end{aligned}$$

Therefore our statement follows. \square

COROLLARY 1.5. *Every element in $Q_1^{(0)}$ can be rewritten as a polynomial in $\mathbb{K}(q)[\theta]$.*

1.2. Factorization of Homogeneous Polynomials in the First q -Weyl Algebra.

With the knowledge we obtained up to this point about the first q -Weyl algebra, we are finally able to state Theorem 2.25 from [Hei10] for the first q -Weyl algebra. The proof is done the same way, therefore we dispense ourselves from including it here.

THEOREM 1.6. *$Q_1^{(0)}$ is a ring and finitely generated as a $\mathbb{K}(q)$ -algebra by the element $\theta := x\partial$. The other graded direct summands $Q_1^{(k)}$ are finitely generated $Q_1^{(0)}$ modules by the element x^{-k} , if $k < 0$, or by ∂^k , if $k > 0$.*

Therefore, as in the case of the first Weyl algebra, in order to obtain one factorization of a homogeneous polynomial in the first q -Weyl algebra, we only have to deal with the factorization of polynomials in $\mathbb{K}(q)[\theta]$. The remaining problem is that elements in $\mathbb{K}(q)[\theta]$ can be reducible in Q_1 . This can easily be seen considering the element $\theta = x\partial$.

But fortunately, compare to Lemma 2.24 from the introduction, there are only two monic polynomials where this case can occur.

LEMMA 1.7. *The polynomials θ and $\theta + \frac{1}{q}$ are the only irreducible monic elements in $\mathbb{K}(q)[\theta]$ that are reducible in Q_1 .*

PROOF. Let $f \in \mathbb{K}(q)[\theta]$ be a monic polynomial. Assume that it is irreducible in $\mathbb{K}(q)[\theta]$, but reducible in Q_1 . Let φ, ψ be elements in Q_1 with $\varphi\psi = f$. Then φ and ψ are homogeneous and $\varphi \in Q_1^{(-k)}, \psi \in Q_1^{(k)}$ for a $k \in \mathbb{Z} \setminus \{0\}$. Without loss of generality let k be positive. For k being negative we can use a similar argument.

Then

$$\begin{aligned}
\varphi &= \tilde{\varphi}x^k \\
\psi &= \tilde{\psi}\partial^k
\end{aligned}$$

for $\tilde{\varphi}, \tilde{\psi} \in \mathbb{K}(q)[\theta]$.

Using Corollary 1.3, we have

$$f = \tilde{\varphi} x^k \tilde{\psi} \partial^k = \tilde{\varphi} x^k \partial^k \tilde{\psi} \left(\frac{1}{q} \left(\frac{\theta - 1}{q^{n-1}} - \frac{q^{-n+2} - q}{1 - q} \right) \right).$$

As we know from Lemma 1.4 the equation

$$x^k \partial^k = \frac{1}{q^{T_{k-1}}} \prod_{i=0}^{k-1} \left(\theta - \sum_{j=0}^{i-1} q^j \right)$$

holds.

Thus, because we assumed f to be irreducible in $\mathbb{K}(q)[\theta]$, we must have $\tilde{\varphi}, \tilde{\psi} \in \mathbb{K}(q)$ and $k = 1$. Because f is monic, we must also have $\tilde{\varphi} = \tilde{\psi}^{-1}$.

As a result, the only possible f is $f = \theta + \frac{1}{q}$. If we originally would have chosen k to be negative, the only possibility for f would be $f = \theta$. This completes the proof. \square

This Lemma was the last piece to the puzzle that we needed for the outcome that we can use the same technique to factorize homogeneous polynomials in the first q -Weyl algebra that we also used for homogeneous polynomials in the first Weyl algebra. The only differences lie in the commutation rules for θ . Therefore we will not give the complete factorization algorithm again here. The algorithm can be found in the library `ncfactor.lib` distributed with the computer algebra system SINGULAR in version 3-1-3 and higher. How to use the algorithm and a timing can be seen in the next example.

EXAMPLE 1.8. Let $h \in Q_1$ be the polynomial

$$\begin{aligned} h := & q^{25} x^{10} \partial^{10} + q^{16} (q^4 + q^3 + q^2 + q + 1)^2 x^9 \partial^9 \\ & + q^9 (q^{13} + 3q^{12} + 7q^{11} + 13q^{10} + 20q^9 + 26q^8 \\ & + 30q^7 + 31q^6 + 26q^5 + 20q^4 + 13q^3 + 7q^2 + 3q + 1) x^8 \partial^8 \\ & + q^4 (q^9 + 2q^8 + 4q^7 + 6q^6 + 7q^5 + 8q^4 + 6q^3 + 4q^2 + 2q + 1) \\ & (q^4 + q^3 + q^2 + q + 1) (q^2 + q + 1) x^7 \partial^7 \\ & + q (q^2 + q + 1) (q^5 + 2q^4 + 2q^3 + 3q^2 + 2q + 1) \\ & (q^4 + q^3 + q^2 + q + 1) (q^2 + 1) (q + 1) x^6 \partial^6 \\ & + (q^{10} + 5q^9 + 12q^8 + 21q^7 + 29q^6 + 33q^5 \\ & + 31q^4 + 24q^3 + 15q^2 + 7q + 12) x^5 \partial^5 + 6x^3 \partial^3 + 24 \end{aligned}$$

We can use SINGULAR to obtain all of its factorizations in the following way.

```
LIB "ncfactor.lib";
ring R = (0,q),(x,d),dp;
def r = nc_algebra (q,1);
setring(r);
poly h = q^25*x^10*d^10+q^16*(q^4+q^3+q^2+q+1)^2*x^9*d^9+
q^9*(q^13+3*q^12+7*q^11+13*q^10+20*q^9+26*q^8+
30*q^7+31*q^6+26*q^5+20*q^4+13*q^3+7*q^2+3*q+
1)*x^8*d^8+q^4*(q^9+2*q^8+4*q^7+6*q^6+7*q^5+
8*q^4+6*q^3+4*q^2+2q+1)*(q^4+q^3+q^2+q+1)*(q^2+
q+1)*x^7*d^7+q*(q^2+q+1)*(q^5+2*q^4+2*q^3+3*q^2+
```

```

2*q+1)*(q^4+q^3+q^2+q+1)*(q^2+1)*(q+1)*x^6*d^6+
(q^10+5*q^9+12*q^8+21*q^7+29*q^6+33*q^5+
31*q^4+24*q^3+15*q^2+7*q+12)*x^5*d^5+
6*x^3*d^3+24;
homogfacFirstQWeyl_all(h);
[1]:
  [1]:
    1
  [2]:
    x5d5+x3d3+4
  [3]:
    x5d5+6
[2]:
  [1]:
    1
  [2]:
    x5d5+6
  [3]:
    x5d5+x3d3+4

```

If the user is interested in just one factorization the command `homogfacFirstQWeyl` instead of `homogfacFirstQWeyl_all` can be used.

On my computer – 2 GB RAM, 2.33GHz Dual Core processor – this calculation needs 2.8 seconds. Compared to the factorization of

$$(x^5\partial^5 + 6)(x^5\partial^5 + x^3\partial^3 + 4)$$

as element in A_1 , which takes less than a second, this seems to be way more slow considering that both algorithms have the same complexity. But this slowdown is not due to more steps that need to be done in the algorithm for the q -Weyl algebra, but due to the parameter q and the speed of calculating in $\mathbb{Q}(q)$ as the basefield instead of just in \mathbb{Q} .

We will end this section here and leave the question how to factorize inhomogeneous polynomials in Q_1 for a later point. If we would just use the techniques from [Hei10], the calculations would be too slow because of the high amount of possibilities we have due to the parameter q . Better techniques are needed for feasible running times, and we are going to present them in the section where we will attend to a new algorithm to deal with inhomogeneous factorizations in the first Weyl algebra.

2. Factorization in the Polynomial First Weyl Algebra

“If I had some duct tape, I could fix that.” – MacGyver, TV Show from the 80s/90s

2.1. `ncfactor.lib`. In the Bachelor thesis [Hei10], we presented a new approach for factorizing the first Weyl algebra. The factorization of $[-1, 1]$ homogeneous polynomials performed efficient and the implementation in SINGULAR is nowadays for a certain family of polynomials the only implementation that is able to give a factorization of these polynomials in a reasonable amount of time.

The factorization of homogeneous polynomials was also used to design an algorithm to factorize also inhomogeneous polynomials. This was done as a proof of concept, and in order to keep the complexity on a low level, we did allow the algorithm to have some families of polynomials it cannot factorize. As an example – as also stated in Chapter 3, Subsection 2.3.2 of the Bachelor thesis – we can take the polynomial

$$h := (1 + x^2\partial)^4.$$

The crux was that the highest homogeneous part of h was 1 and not furthermore split by the combinatorial subalgorithms (for complexity reasons as said before).

Now we are going to deal with the question how we can redesign the algorithm so that it is also able to find factorizations of polynomials like h and does not lose performance in factoring the other kinds of polynomials it was already able to factorize. On our way we are trying to reduce problems to commutative rings as often as possible.

2.1.1. Quick Reference of `ncfactor.lib`. The ideas from the Bachelor thesis for factorization were implemented in the SINGULAR library `ncfactor.lib` and after some testing, it was part of the distribution of SINGULAR since version 3-1-3. Meanwhile, among some bugfixes and code optimization, the library has grown and got some additional functions. Currently, it contains the following procedures.

- `facFirstWeyl` – an algorithm for factorization of polynomials in the first Weyl algebra.
- `testNCfac` – testing of correctness of a given factorization.
- `facSubWeyl` – an algorithm that factorizes polynomials in the first Weyl algebra as a subalgebra of a bigger algebra.
- `facFirstShift` – factorization of polynomials in the first shift algebra.
- `homogfacFirstQWeyl[_all]` – factorization of $[-1, 1]$ -homogeneous polynomials (all or just one) in the first q -Weyl algebra.

The procedure for factoring polynomials in the first shift algebra uses the same techniques as the procedure for factoring polynomials in the first Weyl algebra. The equivalent ideas for the first q -Weyl algebra were already shown in the previous section. The other procedures are just some sugar for the practical use of the library.

The algorithms that are presented here are not yet contained in the library. But they will be distributed as soon as possible.

2.2. A New Approach.

2.2.1. *Preliminaries.* From now on, $h \in A_1$ denotes the polynomial we want to factorize. Its factorization is denoted by $h = h_1 \cdots h_n$, where the h_i are again in A_1 . We can make the general assumption that there exists no homogeneous $f \in A_1$, such that $f \mid_r h$ or $f \mid_l h$. This is due to the fact that we can – as a step of preprocessing – exclude all possible homogeneous right resp. left divisors.

We will briefly sketch how this exclusion can be done. Let us start with restricting ourselves to exclusion of homogeneous factors on one side, namely on the left. There, the following algorithm can do the work.

Algorithm 1 extractHomogeneousDivisorsLeft: Extraction of homogeneous polynomials from the left.

Input: A polynomial h in the first Weyl algebra, $h = k_{n_1} + \dots + k_{n_l}$, where $l \in \mathbb{N}, n_1 > \dots > n_l \in \mathbb{Z}, k_{n_i} \in A_1^{(n_i)}$.

Output: If h is homogeneous, all possible factorizations of h are returned. If h is inhomogeneous, the algorithm returns the set $\{[h_1, \dots, h_n] \mid h_1 \cdots h_n = h, h_n \text{ is inhomogeneous and has no homogeneous left divisors, } h_i \text{ are homogeneous polynomials for all } i \in \{1, \dots, n-1\}\}$.

Preconditions:

- Existence of an algorithm `homogfacFirstWeyl_all` to calculate all factorizations of a homogeneous polynomial in A_1 .
- Existence of an algorithm `divl` to divide a given polynomial p_1 by another given polynomial p_2 from the left in the first Weyl algebra.

```

1: if  $h$  is homogeneous then
2:   return homogfacFirstWeyl_all( $h$ )
3: end if
4: for  $i$  from 1 to  $l$  do
5:    $L_i \leftarrow$  homogfacFirstWeyl_all( $k_{n_i}$ )
6: end for
7:  $tempResult \leftarrow$   $\{[h_1, \dots, h_{\tilde{n}}] \mid \text{for all } i \in \underline{l} \text{ there exists } [h_1, \dots, h_{\tilde{n}}, p_1, \dots, p_m] \in L_i \text{ for } m \in \mathbb{N} \text{ and } p_i \in A_1 \text{ homogeneous}\}$ 
8: return  $\{[h_1, \dots, h_{n-1}, h_n] \mid [h_1, \dots, h_{n-1}] \in tempResult, h_n = \text{divl}(h, h_1 \cdots h_{n-1})\}$ 

```

An algorithm `extractHomogeneousDivisorsRight` can be designed in an analogous way.

The termination and the correctness of that algorithm is clear, as we are only performing loops over finite sets and every homogeneous left factor of h has to be a left factor of every homogeneous summand contained in h .

In order to deal with all possible factorizations of a given polynomial h that has left and right homogeneous divisors, it is not enough to first extract the left and afterwards of the remaining inhomogeneous polynomial the right homogeneous factors, as we would then lose some factorizations. The next example shows why.

EXAMPLE 2.1. Consider

$$h := x^2(x\partial + \partial).$$

If we would first extract all homogeneous factors from the left, we would obtain the only possibility $[x, x, x\partial + \partial]$. Afterwards extracting the homogeneous right factors from the inhomogeneous polynomial $x\partial + \partial$ would yield $[x, x, x + 1, \partial]$. All those are irreducible and one could assume that these are all factorizations. In fact, they are not all of them. If we would start extracting from the right, we could see this quite easy. There, we have two possibilities $[x + 1, x\partial - 1, x]$ and $[x + 1, x, x, \partial]$ and there is no further exclusion to the left possible any more.

This example should sensibilize the reader to be careful with the extraction of homogeneous factors. In fact, to find a way to get around this is a not so hard combinatorial problem, which we will not consider deeply here.

After we have found all possible ways to exclude homogeneous factors from the left and from the right, we obtain a set of inhomogeneous ones, that might still be reducible. The factorization of them will be our task for the rest of the section.

REMARK 2.2. Again, if we are interested in all factorizations, we have to add to that set the original h , as extracting homogeneous factors could make possible factorizations disappear. An example where this can happen will appear in Chapter 2, Example 1.9.

For that, we also assume that we have an algorithm `computeCombinationsMinMaxHomog`, that computes for a given inhomogeneous polynomial all possible tuples

$$((p_{\max}, p_{\min}), (q_{\max}, q_{\min})),$$

such that $\deg(p_{\max}) > \deg(p_{\min})$ and $\deg(q_{\max}) > \deg(q_{\min})$ is true and the operation $h - (p_{\max} + p_{\min})(q_{\max} + q_{\min})$ makes the highest and the lowest homogeneous summands of h disappear. Such an algorithm was already designed in the Bachelor thesis.

REMARK 2.3. In the Bachelor thesis, we actually calculated not just tuples, but n -tuples $((p_{1,\max} + p_{1,\min}), \dots, (p_{n,\max} + p_{n,\min}))$ of combinations doing that work for us. For simplicity, we will just work with tuples here and obtain the missing factorizations by recursively calling the factorization algorithm on every factor again. On the existing algorithms in `ncfactor.lib` for computing such tuples there are just slight modifications to be made in order to obtain just tuples.

2.2.2. *Determine the Rest of the Homogeneous Summands.* We will start with some discussion about the form of a factorization of h consisting of two factors. Let us denote those factors by

$$h := (p_{n_1} + \dots + p_{n_k})(q_{m_1} + \dots + q_{m_l}),$$

where $k, l \in \mathbb{N}$, $n_1 > n_2 > \dots > n_k$ and $m_1 > m_2 > \dots > m_l \in \mathbb{Z}$, $p_{n_i} \in A_1^{(n_i)}$ for all $i \in \underline{k}$, $q_{m_j} \in A_1^{(m_j)}$ for all $j \in \underline{l}$.

Candidates for $p_{n_1}, p_{n_k}, q_{m_1}, q_{m_l}$ are already given by `computeCombinationsMinMaxHomog`. It remains to deal with the rest, i.e. p_i and q_j for $i \in \{n_2, \dots, n_{k-1}\}, j \in \{m_2, \dots, m_{l-1}\}$. And the knowledge of the candidates for the minimum and maximum homogeneous summands is the only knowledge that we have so far. Of course, most of them are not belonging to any factorization of h . We might first check if given $((p_{\max}, p_{\min}), (q_{\max}, q_{\min}))$ can be the maximum resp. minimum homogeneous summands of the factors in order to minimize our computations later for combinations, that will not lead to a solution anyway.

2.2.3. *Preliminary Filtering of Combinations.* A first way how we can check if a combination $((p_{\max}, p_{\min}), (q_{\max}, q_{\min}))$ leads to a valid result is checking whether $\deg(p_{\max}) = \deg(p_{\min}) + 1$ (respectively $\deg(q_{\max}) = \deg(q_{\min}) + 1$). If this is true, it must already be a left factor (respectively a right factor), since we cannot add homogeneous summands of a degree between $\deg(p_{\max})$ and $\deg(p_{\min})$ to the factor any more. If it is not a factor, we dismiss this combination and go on with the next one; if it is a factor, we have a first nontrivial factorization and we are done.

Therefore, we assume from now on that $\deg(p_{\max}) > \deg(p_{\min}) + 1$ and $\deg(q_{\max}) > \deg(q_{\min}) + 1$. The next condition we can check is motivated by the following fact:

The polynomial we get by multiplying

$$(p_{n_1} + \dots + p_{n_k})(q_{m_1} + \dots + q_{m_l}),$$

using the notions above with $n_1 > \dots > n_k$, $m_1 > \dots > m_l$ and $p_{n_1} \neq 0 \neq p_{n_k}$, $q_{m_1} \neq 0 \neq q_{m_l}$, has at least 2 and at most kl different homogeneous summands.

This can be seen as follows. As $p_{n_1}q_{m_1}$ and $p_{n_k}q_{m_l}$ cannot be eliminated for degree reasons by the other terms in the product and they are not zero by assumption, we have at least those two homogeneous summands in the product. The upper bound is clear, because we have kl different products of homogeneous polynomials from the left with homogeneous polynomials on the right.

REMARK 2.4. A pair of polynomials having this upper bound can also always be reached, because we can simply choose the m_i and n_j , $(i, j) \in \underline{l} \times \underline{k}$, such that $m_i + n_j \neq m_{i'} + n_{j'}$ with $(i, j) \neq (i', j')$.

Therefore the next condition can be the following. If h has at most two homogeneous summands, then one of the factors has to have two homogeneous summands. Using this condition for that special case tells us that we have just to go through the complete output of `computeCombinationsMinMaxHomog` and check whether we have already divisors in there and no further calculations are needed.

EXAMPLE 2.5. Let

$$h := x^2\partial^4 + 2x\partial^3 - 1.$$

The polynomial h has just two homogeneous summands, namely $x^2\partial^4 + 2x\partial^3$ and -1 . The output of `computeCombinationsMinMaxHomog` is the following:

```
> computeCombinationsMinMaxHomog(h);
[1]:
  [1]:
    d-1
  [2]:
    x2d3+1
[2]:
  [1]:
    d+1
  [2]:
    x2d3-1
[3]:
  [1]:
```

```

      xd2-1
[2]:
      xd2+1
[4]:
[1]:
      xd2+1
[2]:
      xd2-1
[5]:
[1]:
      xd2+d-1
[2]:
      xd2-d+1
[6]:
[1]:
      xd2+d+1
[2]:
      xd2-d-1
[7]:
[1]:
      x2d3+2xd2-1
[2]:
      d+1
[8]:
[1]:
      x2d3+2xd2+1
[2]:
      d-1

```

Only combination 3 and 4 lead to a result and we do not have to make further checks.

On the other hand, if h has more than 4 homogeneous summands, it is also not needed to check whether $(p_{\max} + p_{\min})(q_{\max} + q_{\min})$ are already factorizations, as their product has at most 4 summands.

2.2.4. Determination of the Remaining Homogeneous Summands. If we filtered our output of `computeCombinationsMinMaxHomog` due to the preliminaries above, we know that there is at least one nontrivial p_{n_i} and one nontrivial q_{m_j} for $1 < i < k$ and $1 < j < l$ between p_{n_1} and p_{n_k} and q_{m_1} and q_{m_l} in $(p_{n_1} + \dots + p_{n_k})(q_{m_1} + \dots + q_{m_l})$.

As we already know $p_{\max}, p_{\min}, q_{\max}$ and q_{\min} and therefore know their degrees, we consider the possible homogeneous summands between them as indeterminates. Therefore $k = \deg(p_{\max}) - \deg(p_{\min} + 1)$ and $l = \deg(q_{\max}) - \deg(q_{\min} + 1)$. Set $p_{n_1} = p_{\max}, p_{n_k} := p_{\min}, q_{m_1} = q_{\max}, q_{m_l} := q_{\min}$ and $n_{i+1} = n_i + 1, m_{j+1} = m_j + 1$ for all n_i and m_j .

We define for all $i \in \underline{k}$ the polynomial \tilde{p}_{n_i} by $\tilde{p}_{n_i} \partial^{n_i} = p_{n_i}$, if $n_i \geq 0$ and $\tilde{p}_{n_i} x^{-n_i} = p_{n_i}$, if $n_i < 0$, where the $\tilde{p}_{n_i} \in A_1^{(0)}$. In the same way we define \tilde{q}_{m_i} for all $i \in \underline{l}$.

Thus we are actually only searching for the \tilde{p}_{n_i} and the \tilde{q}_{m_j} . An ansatz that could be tried out is the following.

Let $h = \sum_{i=m_l+n_k}^{n_1+m_1} \tilde{h}_i \varphi_i^{|i|}$, $\varphi_i = x$, if $i < 0$, $\varphi_i = \partial$ otherwise, $\tilde{h}_i \in A_1^{(0)}$ the decomposition of h in homogeneous summands, where we also allow zeros to appear among the \tilde{h}_i . Then we know, that our \tilde{p}_i and \tilde{q}_j have to fulfill the following set of equations.

$$\left\{ \sum_{\substack{j_1, j_2 \in \mathbb{K} \times \mathbb{L} \\ n_{j_1} + m_{j_2} = i}} \tilde{p}_{n_{j_1}} \tilde{q}_{m_{j_2}} \circ (\theta + n_{j_1}) \gamma_{n_{j_1}, m_{j_2}} = \tilde{h}_i |n_k + m_l < i < n_1 + m_1 \right\},$$

where

$$\gamma_{i,j} := \begin{cases} 1, & \text{if } i, j \geq 0 \vee i, j \leq 0 \\ \prod_{\kappa=0}^{|i|-1} (\theta - \kappa), & \text{if } i < 0, j > 0, |i| \leq |j| \\ \prod_{\kappa=0}^{|j|-1} (\theta - \kappa - |i| + |j|), & \text{if } i < 0, j > 0, |i| > |j| \\ \prod_{\kappa=1}^i (\theta + \kappa), & \text{if } i > 0, j < 0, |i| \leq |j| \\ \prod_{\kappa=1}^{|j|} (\theta + \kappa + |i| - |j|), & \text{if } i > 0, j < 0, |i| > |j| \end{cases}.$$

As the reader recognizes: these are a couple of shift equations with a lot of indeterminates. The nice thing about it is that those computations can be made in $\mathbb{K}[\theta]$, a commutative ring. One can even recognize that the solution is obtained step by step. For example

$$\tilde{h}_{n_1+m_1-1} = \tilde{p}_{n_1} \tilde{q}_{m_2} \circ (\theta + n_1) \gamma_{n_1, m_2} + \tilde{p}_{n_2} \tilde{q}_{m_1} \circ (\theta + n_2) \gamma_{n_2, m_1},$$

where only \tilde{p}_{n_2} and \tilde{q}_{m_2} are unknown. Of course, the solution set is given by the syzygy module of the generators of the ideal $\langle \tilde{h}_{n_1+m_1-1}, p_{n_1}, q_{m_1} \circ (\theta + n_2) \rangle$, with the restriction that the coefficient of $\tilde{h}_{n_1+m_1-1}$ is 1. This is in general an infinite set, which will only later be restricted by more equations it has to fulfill. One can continue with the next equation, namely for $\tilde{h}_{n_1+m_1-2}$, where again just two new indeterminates appear that fulfill another relation as syzygy vector. But we will not follow that path, as we consider later another similar – yet using other properties of the homogeneous summands – approach that we think might be the best way to deal with that problem. We will show an example where we would face some difficulties using the described approach.

EXAMPLE 2.6. We consider the polynomial

$$\begin{aligned} h &:= (\theta \partial + \theta^5 + x)((\theta + 1)\partial - (\theta - 1)^5 + x) \\ &= (\theta^2 + 2\theta)\partial^2 + \theta^5\partial - \theta^{10} + 5\theta^9 - 10\theta^8 + 10\theta^7 - 5\theta^6 + \theta^5 + 2\theta^2 + \theta \\ &\quad (10\theta^4 - 40\theta^3 + 80\theta^2 - 80\theta + 32)x + x^2, \end{aligned}$$

and assume that we are right now checking the combination, where

$$p_{\max}^{(0)} = \theta, p_{\min}^{(0)} = 1 = q_{\min}^{(0)}, q_{\max}^{(0)} = \theta + 1.$$

Therefore, we set $k := l := 3$, $p_1 := p_{\max}^{(0)}$, $p_{-1} := q_{-1} := 1$, $q_1 := q_{\max}^{(0)}$ and thus it remains to solve for q_0 and p_0 .

We have the following equations:

$$\begin{aligned} \theta q_0 \circ (\theta + 1) + p_0(\theta + 1) &= \theta^5 & (\text{deg} = 1) \\ \theta(\theta + 1) + \theta^2 + p_0 q_0 &= -\theta^{10} + 5\theta^9 - 10\theta^8 + 10\theta^7 - 5\theta^6 + \theta^5 + 2\theta^2 + \theta & (\text{deg} = 0) \\ p_0 + q_0 \circ (\theta - 1) &= 10\theta^4 - 40\theta^3 + 80\theta^2 - 80\theta + 32. & (\text{deg} = -1) \end{aligned}$$

Here, we see a lot of approaches we can try out. As the example is very simple, it would be enough due to the second equation to check all factorizations of $-\theta^{10} + 5\theta^9 - 10\theta^8 + 10\theta^7 - 5\theta^6 + \theta^5 + 2\theta^2 + \theta - \theta(\theta + 1) - \theta^2$ and find our q_0 and p_0 among the solutions. But this is not possible in general, if we have more than one indeterminate on both sides.

To obtain q_0 and p_0 , we would start off with the first equation. There, we are searching for all $a, b \in K[\theta]$, such that $a\theta + b(\theta + 1) = \theta^5$. We consult SINGULAR with this task and obtain

```
> ring r = 0,theta,dp;
> LIB "nctools.lib";
> def r2 = makeModElimRing(r);
> setring(r2);
> module m = syz(ideal(theta^5,theta,theta+1)); m;
_[1]=[0,theta+1,-theta]
_[2]=[1,-1,-theta4+theta3-theta2+theta]
```

The solution we are actually searching for is of course contained in that module as we can check by

```
> NF([-1,-theta^5,theta^5],std(m));
0
```

But it is very hard to computationally extract the right solution out of this set without evaluating the further equations. Therefore we have to take a general solution set (which is an affine set given by one solution plus the syzygy module) with us to the next equation we want to solve.

As said before, we will choose another ansatz from this point on. From the equation set we know that

$$\begin{aligned} \tilde{h}_{n_1+m_1-1} &= \tilde{p}_{n_1}\tilde{q}_{m_2} \circ (\theta + n_1)\gamma_{n_1,m_2} + \tilde{p}_{n_2}\tilde{q}_{m_1} \circ (\theta + n_2)\gamma_{n_2,m_1} \\ \iff \tilde{p}_{n_2} &= \frac{\tilde{h}_{n_1+m_1-1} - \tilde{p}_{n_1}\tilde{q}_{m_2} \circ (\theta + n_1)\gamma_{n_1,m_2}}{\tilde{q}_{m_1} \circ (\theta + n_2)\gamma_{n_2,m_1}}. \end{aligned}$$

As we see here, the only unknown factor on the right hand side is \tilde{q}_{m_2} . The third equation is

$$\begin{aligned} \tilde{h}_{n_1+m_1-2} &= \tilde{p}_{n_1}\tilde{q}_{m_3} \circ (\theta + n_1)\gamma_{n_1,m_3} + \tilde{p}_{n_3}\tilde{q}_{m_1} \circ (\theta + n_3)\gamma_{n_3,m_2} + \tilde{p}_{n_2}\tilde{q}_{m_2} \circ (\theta + n_2)\gamma_{n_2,m_2} \\ \iff \tilde{p}_{n_3} &= \frac{\tilde{h}_{n_1+m_1-2} - \tilde{p}_{n_1}\tilde{q}_{m_3} \circ (\theta + n_1)\gamma_{n_1,m_3} - \tilde{p}_{n_2}\tilde{q}_{m_2} \circ (\theta + n_2)\gamma_{n_2,m_2}}{\tilde{q}_{m_1} \circ (\theta + n_3)\gamma_{n_3,m_2}}. \end{aligned}$$

The indeterminate \tilde{p}_{n_2} on the right hand side can be replaced by the term above and we only have \tilde{q}_{m_2} and \tilde{q}_{m_3} as indeterminates there. Going on in this fashion we obtain a set of expressions for all $p_{n_i}, i \in \{2, \dots, k-1\}$ which carry only the $\tilde{q}_j, j \in 2, \dots, l-1$ as indeterminates.

The same can be done starting from the bottom. This means that we know that

$$\begin{aligned} \tilde{h}_{n_k+m_l+1} &= \tilde{p}_{n_k}\tilde{q}_{m_{l-1}} \circ (\theta + n_k)\gamma_{n_k,m_{l-1}} + \tilde{p}_{n_{k-1}}\tilde{q}_{m_l} \circ (\theta + n_{k-1})\gamma_{n_{k-1},m_l} \\ \iff \tilde{p}_{n_{k-1}} &= \frac{\tilde{h}_{n_k+m_l+1} - \tilde{p}_{n_k}\tilde{q}_{m_{l-1}} \circ (\theta + n_k)\gamma_{n_k,m_{l-1}}}{\tilde{q}_{m_l} \circ (\theta + n_{k-1})\gamma_{n_{k-1},m_l}}, \end{aligned}$$

and in the same way as above we get another set of equations for $p_{n_i}, i \in \{2, \dots, k-1\}$. Those equations have to coincide of course. This leads to $k-2$ shift equations for the $\tilde{q}_{m_j}, j \in \{2, \dots, l-1\}$.

Now we use another knowledge. As we have a degree restriction in x and ∂ given by $\deg_{\partial}(h)$ and $\deg_x(h)$, the degrees of the \tilde{q}_{m_i} are limited. Therefore, we can assume that they have a certain degree and set their coefficients as new indeterminates. The rest is solving a nonlinear system of equations, which can be done using Gröbner bases (see [Buc97]). We show this in the following example.

EXAMPLE 2.7. Let us consider

$$p := \theta\partial + \theta + 1 + (\theta + 5)x, \quad q := (\theta^2 + 1)\partial + \theta + 3 + (\theta + 7)x.$$

We want to find the factorization of the product

$$\begin{aligned} h := pq &= (\theta^3 + 2\theta^2 + 2\theta)\partial^2 + (\theta^3 + 2\theta^2 + 5\theta + 1)\partial + \theta^4 + 4\theta^3 + 2\theta^2 + 22\theta + 3 \\ &\quad + (2\theta^2 + 15\theta + 17)x + (\theta^2 + 11\theta + 30)x^2 \end{aligned}$$

and assume, that we do not know p and q yet.

From the first step of the algorithm, the combination

$$p_{max} = \theta\partial, p_{min} = (\theta + 5)x, q_{max} = (\theta^2 + 1)\partial, q_{min} = (\theta + 7)x$$

will appear as output of `computeCombinationsMinMaxHomog`. The polynomials $p_{max} + p_{min}$ and $q_{max} + q_{min}$ are no factorizations of pq yet, therefore we will have to solve for one more homogeneous summand.

In pq , we have $\kappa := \min(\deg_x(pq), \deg_{\partial}(pq)) = 4$. Furthermore, we already know using the notations of the algorithm that

$$\begin{aligned} p_1 &= \theta, \\ p_{-1} &= \theta + 5 \\ q_1 &= \theta^2 + 1 \\ q_{-1} &= \theta + 7. \end{aligned}$$

The remaining unknowns are p_0 and q_0 . As $\kappa = 4$ we can assume that they have the form

$$p_0 = p_0^{(4)}\theta^4 + p_0^{(3)}\theta^3 + p_0^{(2)}\theta^2 + p_0^{(1)}\theta + p_0^{(0)}, \quad q_0 = q_0^{(4)}\theta^4 + q_0^{(3)}\theta^3 + q_0^{(2)}\theta^2 + q_0^{(1)}\theta + q_0^{(0)},$$

with $p_0^{(i)}, q_0^{(i)} \in \mathbb{K}$ for $i \in \{0, 1, 2, 3, 4\}$.

The product $(p_1\partial + p_0 + p_{-1}x)(q_1\partial + q_0 + q_{-1}x)$ does look like

$$\begin{aligned} & p_1q_1 \circ (\theta + 1)\partial^2 \\ & + p_1q_0 \circ (\theta + 1)\partial + p_0q_1\partial \\ & + p_1(q_{-1} \circ (\theta + 1))(\theta + 1) + p_0q_0 + p_{-1}(q_1 \circ (\theta - 1))\theta \\ & + p_{-1}q_0 \circ (\theta - 1)x + p_0q_{-1}x \\ & + p_{-1}q_{-1} \circ (\theta - 1)x^2. \end{aligned}$$

Replacing p_1, p_{-1}, q_1, q_{-1} by the known factors, we have

$$(\theta\partial + p_0 + (\theta + 5)x)((\theta^2 + 1)\partial + q_0 + (\theta + 7)x),$$

which is equal to

$$\begin{aligned}
& \theta(\theta^2 + 2\theta + 2)\partial^2 \\
& + \theta q_0 \circ (\theta + 1)\partial + p_0(\theta^2 + 1)\partial \\
& + \theta(\theta + 8)(\theta + 1) + p_0 q_0 + (\theta + 5)(\theta^2 - 2\theta + 2)\theta \\
& + (\theta + 5)q_0 \circ (\theta - 1)x + p_0(\theta + 7)x \\
& + (\theta + 5)(\theta + 6)x^2.
\end{aligned}$$

We know h . Therefore, we obtain starting from the top the equation

$$p_0 = \frac{\theta^3 + 2\theta^2 + 5\theta + 1 - \theta q_0 \circ (\theta + 1)}{\theta^2 + 1}$$

and starting from the bottom the equation

$$p_0 = \frac{2\theta^2 + 15\theta + 17 - (\theta + 5)q_0 \circ (\theta - 1)}{\theta + 7}.$$

Thus q_0 has to fulfill the equation

$$(\theta^3 + 2\theta^2 + 5\theta + 1 - \theta q_0 \circ (\theta + 1))(\theta + 7) = (2\theta^2 + 15\theta + 17 - (\theta + 5)q_0 \circ (\theta - 1))(\theta^2 + 1).$$

For the coefficients $q_0^{(i)}$ with $i \in \{0, 1, 2, 3, 4\}$ we get the system of equations

$$(2.1) \quad -q_0^{(4)} = 0$$

$$(2.2) \quad -q_0^{(3)} = 0$$

$$(2.3) \quad -q_0^{(2)} - q_0^{(3)} + 24q_0^{(4)} = 0$$

$$(2.4) \quad -q_0^{(1)} - 2q_0^{(2)} + 21q_0^{(3)} + 7q_0^{(4)} + 1 = 0$$

$$(2.5) \quad -q_0^{(0)} - 3q_0^{(1)} + 17q_0^{(2)} + 8q_0^{(3)} + 79q_0^{(4)} + 6 = 0$$

$$(2.6) \quad -4q_0^{(0)} + 12q_0^{(1)} + 7q_0^{(2)} + 39q_0^{(3)} - 2q_0^{(4)} = 0$$

$$(2.7) \quad 6q_0^{(0)} + 3q_0^{(1)} + 16q_0^{(2)} - 7q_0^{(3)} + 26q_0^{(4)} - 21 = 0$$

$$(2.8) \quad -5q_0^{(0)} + 5q_0^{(1)} - 5q_0^{(2)} + 5q_0^{(3)} - 5q_0^{(4)} + 10 = 0.$$

Side note: That the system above is given linear is only due to the shape of the given example. In general we would expect nonlinear terms to appear in the system of equations.

Calculating a reduced Gröbner Basis of this system, we obtain

$$q_0^{(4)} = 0, q_0^{(3)} = 0, q_0^{(2)} = 0, q_0^{(1)} = 1, q_0^{(0)} = 3,$$

which means that $q_0 = \theta + 3$. Comparing this to our original factors, we see that this unique solution coincides with the homogeneous summand of degree 0 in our originally chosen q . Therefore, we find this solution using our technique.

Let us formulate the technique which we described informally above as an algorithm.

Algorithm 2 `determineRestOfHomogParts`: Determination of the rest of the homogeneous summands in two factors given the maximal and the minimal ones. PART 1

Input: Polynomials p_{\max} , p_{\min} , q_{\max} , q_{\min} and h .

Output: A list of right factors q of h that have q_{\max} and q_{\min} as their maximum respectively minimum homogeneous summand. Empty list, if those elements are not existent

Preconditions:

- Existence of an algorithm `solveNLS` to compute the solution of a nonlinear system of equations in a multivariate polynomial ring over \mathbb{K}
- $\deg(p_{\max}) > \deg(p_{\min}) + 1$
- $\deg(q_{\max}) > \deg(q_{\min}) + 1$
- $p_{\max}q_{\max} = h_{\max}$
- $p_{\min}q_{\min} = h_{\min}$

$n_1 := \deg(p_{\max})$

$k := \deg(p_{\max}) - \deg(p_{\min})$

$n_k := \deg(p_{\min})$

$n_i := n_1 - i$ for all $i \in \{2, \dots, k-1\}$

5: $p_{n_1} := p_{\max}^{(0)}$, $p_{n_k} := p_{\min}^{(0)}$

for i from 2 to $k-1$ **do**

if $n_i > 0$ **then**

$\kappa_i := \min(\deg_x(h), \deg_{\partial}(h) - |n_i|)$

else

10: $\kappa_i := \min(\deg_x(h) - |n_i|, \deg_{\partial}(h))$

end if

$p_{n_i} := \sum_{j=0}^{\kappa_i} p_{n_i}^{(j)} \theta^j$, where $p_{n_i}^{(j)}$ are variables

end for

$m_1 := \deg(q_{\max})$

15: $l := \deg(q_{\max}) - \deg(q_{\min})$

$m_l := \deg(q_{\min})$

$q_{m_1} := q_{\max}^{(0)}$; $q_{m_l} := q_{\min}^{(0)}$

for i from 2 to $l-1$ **do**

if $m_i > 0$ **then**

20: $\kappa_i := \min(\deg_x(h), \deg_{\partial}(h) - |n_i|)$

else

$\kappa_i := \min(\deg_x(h) - |n_i|, \deg_{\partial}(h))$

end if

$q_{m_i} := \sum_{j=0}^{\kappa_i} q_{m_i}^{(j)} \theta^j$, where $q_{m_i}^{(j)}$ are variables

25: **end for**

The termination of this algorithm follows as we do only iterate over finite sets. The correctness follows from our preparatory work about the equations the different q_{m_i} .

The only problem we are facing is that our set of solutions in line 13 in Part 2 of the algorithm might be an infinite set. But after several experiments with the solution sets we were solving we have the following conjecture.

Algorithm 3 determineRestOfHomogParts: PART 2

```

for  $i$  from 2 to  $k - 1$  do
   $lhs_i := \frac{h_{n_1+m_1-i+1-\sum n_{j_1}+m_{j_2}=n_1+m_1-i+1} p_{n_{j_1}} q_{m_{j_2}} \circ(\theta-n_{j_1})\gamma_{j_1,j_2}}{q_{m_1} \circ(\theta-n_i)\gamma_{n_i,m_1}}$ 
  Substitute all  $p_{n_i}$  by the formerly calculated terms in  $p_{n_1}$  and  $q_{m_j}$  in  $lhs_i$ 
end for
5: for  $i$  from  $k - 1$  to 2 do
   $rhs_i := \frac{h_{n_k+m_l+i-1-\sum n_{j_1}+m_{j_2}=n_k+m_l+i-1} p_{n_{j_1}} q_{m_{j_2}} \circ(\theta-n_{j_1})\gamma_{j_1,j_2}}{q_{m_l}(\theta-n_i)\gamma_{n_i,m_l}}$ 
  Substitute all  $p_{n_i}$  by the formerly calculated terms in  $p_{n_1}$  and  $q_{m_j}$  in  $rhs_i$ 
end for
for  $i$  from 2 to  $k - 1$  do
10:   $temp := \text{lcm}(\text{denominator}(lhs_i), \text{denominator}(rhs_i))$ 
     $eq_{i-1} := (lhs_i - rhs_i) \cdot temp$ 
end for
  solveNLS( $\{eq_i = 0 | i = 1 \dots k - 2\}$ ) for the coefficients  $q_{m_i}^{(j)}$  in  $q_{m_i}$ .
  if Solution(s) do(es) exist then
15:  return The different solutions for  $q$  that are right divisors of  $h$ 
  end if
return  $\emptyset$ 

```

CONJECTURE 2.8. For the sets of equations appearing in the algorithm there exists always a finite solution set.

Together with `computeCombinationsMinMaxHomog` and the extraction algorithm for homogeneous factors, this algorithm can be embedded in a complete algorithm to factorize a polynomial h in A_1 . Of course, a recursive call on the factors is needed since we are only computing tuples of factors. We have an experimental implementation of that algorithm in SINGULAR which will be subject of the next subsection.

2.2.5. *Experimental Implementation and Timings.* First of all, we are interested how much better this technique is compared to the existing one stated in the Bachelor thesis. Furthermore, we will check how fast we obtain our results compared to existing implementations of factorization algorithms in REDUCE (version 2.8, [MA94]) and MAPLE (version 16, [vH97]).

EXAMPLE 2.9. Let us start with the counterexample for our former implementation, namely $h_1 := (1 + x^2\partial)^4$. Our new algorithm finds 24 different factorizations for that polynomial. The complete output of SINGULAR can be found in the appendix.

The “original” factorization there is in the 6th entry. The computation took 55 minutes and 54 seconds. This timing does not come from Gröbner Basis computations, but from the huge amount of combinations for the maximum homogeneous part of h_1 .

Asking REDUCE, we did not get any result after 9 hours of computation and quit the task.

MAPLE tells us in less than a second, that there is one factorization, namely

$$h_1 = (x^8\partial + x^6(-1 + 3x)) \cdot \left(\partial + \frac{-1 + 3x}{x^2}\right) \cdot \left(\partial + \frac{-1 + 3x}{x^2}\right) \cdot \left(\partial + \frac{-1 + 3x}{x^2}\right).$$

EXAMPLE 2.10. Another interesting example is the polynomial

$$h_2 := (x^6 + 2x^4 - 3x^2)\partial^2 - (4x^5 - 4x^4 - 12x^2 - 12x)\partial + (6x^4 - 12x^3 - 6x^2 - 24x - 12).$$

It is taken from [Tsa00], Example 5.7.

Our old implementation was able to find just one factorization, namely

$$h_2 = ((x^4 - x^3 + 3x^2 - 3x)\partial - 3x^3 + 6x^2 - 3x + 12) \cdot ((x^2 + x)\partial - 3x - 1)$$

and it took around 5 minutes to obtain that result.

Our new implementation finds two factorizations; the one above and the additional factorization

$$h_2 = ((x^4 + x^3 + 3x^2 + 3x)\partial - 4x^3 + 3x^2 + 6x + 3) \cdot ((x^2 - x)\partial - 2x + 4).$$

The calculation did take 8 seconds.

REDUCE returns in less than 10 seconds a result, if we only ask for one factorization (i.e. applying the command `nc_factorize` instead of `nc_factorize_all`). The output is the second factorization above. If we ask for all factorizations, REDUCE did not find any result after more than 9 hours of computation; so we cancelled the task.

MAPLE again takes less than a second and returns one factorization, namely

$$h_2 = ((x^6 + 2x^4 - 3x^2)\partial - 2x^2(x^3 - x^2 - x - 3)) \cdot \left(\partial - \frac{2(-2 + x)}{(x - 1)x} \right).$$

EXAMPLE 2.11. A third interesting example is

$$h_3 := (x^4 - 1)x\partial^2 + (1 + 7x^4)\partial + 8x^3.$$

This example is taken from [Koe98], page 200.

Our old algorithm was able to find only one factorization, namely

$$h_3 = (x^3\partial + 3x^2 - x\partial + 1) \cdot (x^2\partial + 2x + \partial)$$

and it took around 3 minutes. The new approach finds 12 distinct factorizations in less than a second. The output can be found in the appendix.

REDUCE returns in 3 seconds 60 factorizations. But some of them contain reducible factors. If those are factorized again and the double entries in the result are removed, we obtain the same 12 different factorizations as we had as output of SINGULAR.

MAPLE finds within a split second one factorization, which is given by

$$h_3 = ((x^5 - x)\partial + 3x^4 + 1) \cdot \left(\partial + \frac{4x^3}{(x - 1)(x + 1)(x^2 + 1)} \right).$$

EXAMPLE 2.12. The last example we want to present here is given by the polynomial

$$h_4 := 10x^5\partial^4 + 26x^4\partial^5 + 47x^5\partial^2 - 97x^4\partial^3.$$

It was suggested by a reviewer (Martin Lee) of our algorithm in the SINGULAR team as a hard example for our previous implementation.

In fact, also after a couple of hours of computation our old algorithm did not terminate. Our new implementation takes two minutes and 46 seconds to find 8 distinct factorizations. Those can be found in the appendix.

REDUCE takes less than one second to find one factorization. It is given by



$$h_4 = (10x^4\partial^2 + 26x^3\partial^3 + 47x^4 - 117x^3\partial - 78x^2\partial^2 + 117x^2 + 156x\partial - 156) \cdot x \cdot \partial \cdot \partial.$$

Trying to find all factorizations, the algorithm did not terminate after 9 hours of computation.

MAPLE takes less than a second and returns one possible factorization

$$h_4 = (26x^4 + 47x^5) \cdot \left(\partial^2 + \frac{10x}{26 + 47x} \partial - \frac{97}{26 + 47x} \right) \cdot \partial \cdot \partial \cdot \partial.$$

As a conclusion we can say, that our new approach is better than our old one in terms of timing and amounts of possible factorizations found. An illustration of that fact is provided by the table below. Compared to other computer algebra systems our algorithm provides the user sometimes with more factorizations in a reasonable time than the other implementations. Therefore it broadens again the amount of polynomials that we are able to factorize with a computer algebra system nowadays. For a future TODO-List one should add some dealing with the question whether the nonlinear system we have to solve in between might lead to an infinite set and – if so – why this happens and how we can extract the correct solution for our algorithm from it.

Poly	 old	 new	# fact. old	# fact. new
h_1	–	55:54min	–	24
h_2	4:30min	0:08min	1	2
h_3	2:35min	0:00.6min	1	12
h_4	–	2:46min	–	8

3. The Rational First Weyl Algebra

“Change your opinions, keep to your principles; change your leaves, keep intact your roots.” – Victor Hugo

The next question on the path is how one can use our techniques to probably find factorizations in the rational first Weyl algebra. This ring has compared to the polynomial first Weyl algebra some handy properties. One is for example, that it is an euclidean domain and therefore also a principal ideal domain. We have therefore several more techniques for dealing with this algebra. The factorization algorithm by Mark van Hoeij – which is the factorization algorithm used in MAPLE – for example computes factorizations in the rational first Weyl algebra. For further reading on that algorithm consider [vH97], and the usage of the algorithm in MAPLE is presented in [Hei10], Chapter 3, subsection 1.1.

As nice as the properties may seem, there is also a flipside of the coin, as the next example shows us.

EXAMPLE 3.1. Let $h := \partial^2$ be an element in the rational first Weyl algebra. One can easily derive a factorization of that element. But h has in fact infinitely many factorizations

in the rational first Weyl algebra. For example, we have for all $c \in \mathbb{K}$

$$\begin{aligned} & (\partial + (x + c)^{-1}) (\partial - (x + c)^{-1}) \\ = & \partial^2 - \partial(x + c)^{-1} + (x + c)^{-1}\partial - (x + c)^{-2} \\ = & \partial^2 - ((x + c)^{-1}\partial - (x + c)^{-2}) + (x + c)^{-1}\partial - (x + c)^{-2} \\ = & \partial^2. \end{aligned}$$

This is an infinite set of factorizations – more explicitly: a one-parametric family depending on $c \in \mathbb{K}$ – of h in the rational first Weyl algebra.

REMARK 3.2. After this example the reader is maybe shocked and thinks that the factorization question in the rational first Weyl algebra might be completely out of control. Fortunately, there are some properties our factorizations do have.

Due to Loewy in [Loe03] and [Loe06], the number of irreducible factors of an ordinary differential operator are always the same. Therefore in our example above we will always deal with two different factors of h , and never more or less.

Furthermore, Tsarev has demonstrated in [TL11] based on his work in [Tsa96] that there actually exists an enumeration algorithm for all distinct factorizations of a differential operator. If there are finitely many, this algorithm can tell exactly how many do exist. If there are infinitely many, the algorithm will also return that. Therefore we have some kind of information on the number of different factorizations.

In order to be more general, we are going to deal with localizations of the first Weyl algebra. As we are noncommutative, the classical notion of localization needs some more concepts.

3.1. Localizations in Ore Algebras. As a reminder, in the commutative ring a localization is defined as follows.

DEFINITION 3.3. Let R be a commutative ring with 1 and $S \subseteq R$ be a multiplicatively closed subset of R containing 1. We define on $R \times S$ the equivalence relation

$$(r_1, s_1) \sim (r_2, s_2) :\Leftrightarrow \exists t \in S : t(r_1s_2 - r_2s_1) = 0.$$

Defining addition and multiplication by

$$\begin{aligned} [(r_1, s_1)] + [(r_2, s_2)] & := [(r_1s_2 + r_2s_1, s_1s_2)], \\ [(r_1, s_1)] \cdot [(r_2, s_2)] & := [(r_1r_2, s_1s_2)], \end{aligned}$$

we obtain a ring which is denoted by $S^{-1}R$.

Informally speaking, one is generalizing the concept of constructing quotient fields, which is in general only possible if R is a domain.

For the case where R is noncommutative, we are facing some problems. For example we have to specify how a set of denominators acts on both sides. If we would take $S \subseteq R$ as a set of denominators, and $S^{-1}R$ as our ring of fractions, we have to be able to give a reasonable definition of how the product $s_1^{-1}r_1 \cdot s_2^{-1}r_2$ of two elements $s_1^{-1}r_1$ and $s_2^{-1}r_2$ in $S^{-1}R$ is defined. It appears that we have to put more conditions on our set S than just being multiplicatively closed.

THEOREM 3.4 (Compare to [BGTV03], Chapter 8, Theorem 1.3). *Let $1 \in S \subseteq R \setminus \{0\}$ be a multiplicatively closed subset of a ring R . The following assertions are equivalent:*

- (1) R admits a left ring of fractions $S^{-1}R$ with respect to S .
- (2) S satisfies the following properties:
 - (a) (left Ore condition) for any $s \in S$ and $r \in R$ there exists $s' \in S$ and $r' \in R$ with $s'r = r's$;
 - (b) (left reversibility) if $rs = 0$ for some $s \in S$ and $r \in R$, then there exists some $s' \in S$ with $s'r = 0$.

We will not give the proof to that here. The interested reader can find it in the literature.

DEFINITION 3.5. A multiplicatively closed subset $1 \in S \subseteq R$ is called a **left Ore set** if it satisfies the left Ore condition introduced in the theorem above. If it furthermore satisfies the left reversibility, we call it a **left denominator set**.

REMARK 3.6. One might think about what happens to σ and δ , if we localize an Ore extension of a ring R with the quasi-derivation (σ, δ) . [BGTV03], Chapter 8, Lemma 1.10 states that if $\sigma(S) \subseteq S$, our pair (σ, δ) canonically extends to a quasi-derivation $(\bar{\sigma}, \bar{\delta})$ on the ring of fractions $S^{-1}R$.

EXAMPLE 3.7. Even though we are already using that fact, we are going to show that $S := \mathbb{K}[x] \setminus \{0\}$ can be chosen as a left denominator set for the first Weyl algebra A_1 .

Left Ore condition: Let $s \in S$ and $r \in A_1 \setminus \{0\}$ be arbitrarily chosen elements. We need to find an element s' , such that $s \mid_r s'r$. If s (respectively r) is a constant or already a right divisor of r (respectively r a left divisor of s), this is trivial. If neither of these properties is given, we can choose $s' := s^{n+1}$, where $n = \deg_{\partial}(r)$. Then $s \mid_r s'r$, because we know that

- $s \mid \frac{d^i}{dx} s' = \frac{d^i}{dx} s^{n+1}$ for every $0 \leq i \leq n$ and we can apply that knowledge to
- $s' \partial^m = \sum_{i=0}^m (-1)^i \binom{m}{i} \partial^{m-i} \left(\frac{d^i}{dx} s' \right)$, $m \in \mathbb{N}$, which means that $s \mid_r s' \partial^m$ if $m \leq n$.

Those formulas – in a more general fashion – can be found in [LS12].

Left reversibility: As A_1 is a domain, there is no $s \in S$ such that $rs = 0$. Therefore this condition holds.

3.2. Relations between Factorizations: Polynomial vs. Rational. Given $h \in S^{-1}R$, where R is a domain and $S \subseteq R$ is a denominator set and $S^{-1}R$ denotes the corresponding ring of fractions, and its factorization $h = h_1 \cdots h_m$, where h_1, \dots, h_m in $S^{-1}R$. The next theorem will show that a multiplication by a unit suffices to obtain a factorization in R .

THEOREM 3.8. *For the setting as given above there exists a unit $q \in S^{-1}R$ such that we have a factorization $qh = \tilde{h}_1 \cdots \tilde{h}_m$, where the \tilde{h}_i are in R .*

PROOF. We will prove this using induction by $m \in \mathbb{N}$. For $m = 1$ the statement is trivial as $h = h_1$ is given as an element of $S^{-1}R$ and we can just multiply by an element of S to obtain an element \tilde{h}_1 in R .

Now let the claim hold for $m \in \mathbb{N}$ arbitrary, but fixed. We prove our statement for $m+1$. Therefore let $h = h_1 \cdots h_{m+1}$. By induction hypothesis there exist invertible $q_1, q_2 \in S^{-1}R$,

such that $q_1 h_1 = \hat{h}_1$ and $q_2 h_2 \cdots h_{m+1} = \tilde{h}_2 \cdots \tilde{h}_n$, where $\hat{h}_1, \tilde{h}_2, \dots, \tilde{h}_{m+1} \in R$. By the left Ore condition satisfied by S , there exist $q_3 \in S$ and $\tilde{h} \in R$ such that $\tilde{h}_1 q_2 = q_3 \hat{h}_1$.

Therefore we choose our q to be equal to $q_3 q_1$ and we have

$$qh = q_3 q_1 h_1 \cdots h_{m+1} = q_3 \hat{h}_1 h_2 \cdots h_{m+1} = \tilde{h}_1 q_2 h_2 \cdots h_{m+1} = \tilde{h}_1 \cdots \tilde{h}_{m+1}.$$

This completes the inductive proof. \square

The techniques used in the given theorem are leading to an algorithm to lift a rational factorization into a polynomial one.

EXAMPLE 3.9. As shown in Example 3.1, ∂^2 can be factorized in the rational first Weyl algebra by

$$\partial^2 = (\partial + (x + c)^{-1}) (\partial - (x + c)^{-1})$$

for all $c \in \mathbb{K}$. Using the techniques of the Theorem above, we can transform it as follows:

$$\begin{aligned} & (\partial + (x + c)^{-1}) \cdot (\partial - (x + c)^{-1}) \\ &= (x + c)^{-1} \cdot ((x + c)\partial + 1) \cdot (x + c)^{-1} \cdot ((x + c)\partial - 1) \\ &= (x + c)^{-1} \cdot ((x + c)\partial(x + c)^{-1} + (x + c)^{-1}) \cdot ((x + c)\partial - 1) \\ &= (x + c)^{-1} \cdot (\partial - (x + c)^{-1} + (x + c)^{-1}) \cdot ((x + c)\partial - 1) \\ &= (x + c)^{-1} \cdot \partial((x + c)\partial - 1). \end{aligned}$$

Thus here we have $q := x + c$ and $\tilde{h}_1 := \partial$, $\tilde{h}_2 := (x + c)\partial - 1$.

By now, we have seen that we can “lift” a rational factorization of an element $h \in S^{-1}R$ into a polynomial one. The next question is, whether we always have a fraction free factorization of h if h is already given with denominator 1, i.e. $h \in R$. Then, if we are just interested in one factorization, lifting would not be necessary any more.

This thought is motivated by the so-called Gauss’s Lemma in commutative algebra.

LEMMA 3.10 (Gauss’s Lemma). *Let R be a commutative factorial ring und $R[x]$ the polynomial ring over R in one variable.*

Let f in $R[x] \setminus R$ be irreducible. Then f as an element in $\text{Quot}(R)[x]$ is also irreducible.

This lemma appears to be very useful when dealing with the factorization question of a polynomial in $\mathbb{Q}[x]$ whose coefficients are given in \mathbb{Z} . Due to this lemma, we are searching for factorizations where the factors also have all their coefficients in \mathbb{Z} . It is moreover the underlying idea of irreducibility criteria like Eisenstein or the reduction criterion.

The next lemma will give us a similar result for the noncommutative case. But before that, we need a proposition dealing with links between left ideals in R and those in $S^{-1}R$.

PROPOSITION 3.11 (Compare to [BGTV03], Chapter 8, Lemma 1.12). *Let I be a left ideal of R . Then we call the ideal $I^e := \{s^{-1}r \mid r \in I, s \in S\}$ the extension of I to $S^{-1}R$. The set I^e is a left ideal in $S^{-1}R$ and $I^e \cap R = \{r \in R \mid \exists s \in S : sr \in I\}$.*

REMARK 3.12. If I is given by a finite set of generators $e_1, \dots, e_n \in R$, then by construction we have $I^e = S^{-1}R \langle e_1, \dots, e_n \rangle$.

LEMMA 3.13. *Let R be an integral domain and f be an element in R . Let further S be a denominator subset of R that does not contain f . If f is irreducible in R , then it is irreducible in $S^{-1}R$.*

PROOF. Assume that there exist irreducible $s^{-1}f_1, \dots, s_n^{-1}f_n \in S^{-1}R$ with

$$f = s_1^{-1}f_1 \cdots s_n^{-1}f_n, \quad n \in \mathbb{N} \setminus \{1\}.$$

Due to Theorem 3.8, there exists a $q \in S$ such that $qf = \tilde{f}_1 \cdots \tilde{f}_n$, where $\tilde{f}_1, \dots, \tilde{f}_n \in R \setminus S$, not units in R .

Therefore, we have the equality of left ideals

$$S^{-1}R\langle f \rangle = S^{-1}R\langle \tilde{f}_1 \cdots \tilde{f}_n \rangle$$

in $S^{-1}R$.

Consider the left ideals $I_1 := R\langle f \rangle$ and $I_2 := R\langle \tilde{f}_1 \cdots \tilde{f}_n \rangle$ in R . Then their extensions to $S^{-1}R$ are

$$\begin{aligned} I_1^e &:= \{s^{-1}r \mid r \in I_1, s \in S\} = S^{-1}R\langle f \rangle, \\ I_2^e &:= \{s^{-1}r \mid r \in I_2, s \in S\} = S^{-1}R\langle \tilde{f}_1 \cdots \tilde{f}_n \rangle. \end{aligned}$$

Due to Proposition 3.11, the intersections $I_i^e \cap R$ consist of those elements r in R , such that there exists an $s \in S$ with $sr \in I_i$. If we extend I_2 to I_2^e , then this is equal to $S^{-1}R\langle \tilde{f}_1 \cdots \tilde{f}_n \rangle$, which is by assumption equal to $S^{-1}R\langle f \rangle = I_1^e$. Therefore $I_1^e \cap R = I_2^e \cap R$ and we have $f = s\varphi\tilde{f}_1 \cdots \tilde{f}_n$, $s \in S, \varphi \in R$. But this contradicts $\tilde{f}_1, \dots, \tilde{f}_n$ being not units and f being irreducible. Therefore our assumption was not valid. \square

COROLLARY 3.14. *Let $f \in R$ be an irreducible element, where R is an integral domain. Then for any localization on a denominator set S the element f is either a unit (i.e. $f \in S$), or it is again irreducible. Therefore it suffices to check for irreducibility in R if we want to determine irreducibility in $S^{-1}R$.*

The conclusion we can draw is that while dealing with the factorization question in the polynomial first Weyl algebra, we are actually already dealing with the factorization question in the rational first Weyl algebra. If we cannot find any factorization in the polynomial first Weyl algebra, there is no need to search for it in the rational Weyl algebra.

If we find factorizations in the polynomial Weyl algebra, the irreducible factors are also irreducible in the rational first Weyl algebra. If one is interested in more factorizations than those of polynomial type then we would suggest to check if the factors are so-called interconvertible (see [Tsa96]) and get to all the other factorizations this way.

3.3. Applications. One application for the factorization of elements in the rational first Weyl algebra was shown to me by Daniel Rettstadt, who is currently writing his Ph.D. thesis at RWTH Aachen University. His topic is computing the so-called differential Galois group of an operator L in the rational first Weyl algebra. As a reference on differential Galois theory we recommend [vdPS03]. He deals with concretizing an idea introduced by E. Hrushovski in [Hru02]. We will not go into much details here, as this topic huge on its own. In the paper, there is an algorithm simply called ‘‘B’’. Proposition 4.1. proves its correctness. According to what Daniel Rettstadt has told, in its second step, this problem can be seen as calculating different right factors of a symmetric power of the given operator,

where factorization comes in. As one is just interested in different right factors here, the use of the techniques presented in this chapter can be applied.

CHAPTER 2

Similarity

Overview

In this chapter, we examine the similarity of two polynomials from the point of view of looking at the algebra as a graded ring. We will mainly concentrate on the first polynomial Weyl algebra and try to state some structural properties two polynomials have to fulfill in order to be similar.

As already said in the introduction, the original motivation was the following.

When we inspect a set of similar polynomials – may as output of the factorization algorithm for some examples, may as the nontrivial entry of a Jacobson normal form (see next chapter) – we can see, that most of the time the difference between them is not a much higher degree in x of the coefficients. Very often we are facing the elements of the underlying field in the coefficients to transform in an exploding way. We are going to try to find explanations why this is happening, and this is the leitmotif of this chapter.

EXAMPLE 0.15. The most drastic similar yet coefficient-wise exploding polynomials come from the computation examples to find the Jacobson normal form over matrices in the rational first Weyl algebra (Chapter 3). One of the examples of two different outputs using the same input matrix are the two polynomials

$$\begin{aligned} p_1 := & 2x^5\partial + 2x^4\partial^2 + 2x^5 + 3x^4\partial - 19x^3\partial^2 - x^4 - 12x^3\partial \\ & + 9x^2\partial^2 + 2x^2\partial - 11x^2 + 10x\partial + 45x - 10 \end{aligned}$$

and

$$\begin{aligned} p_2 := & 88360x^9\partial + 88360x^8\partial^2 + 88360x^9 - 31114x^8\partial - 1003074x^7\partial^2 \\ & - 384554x^8 - 948071x^7\partial + 2133343x^6\partial^2 + 243285x^7 \\ & + 5093247x^6\partial - 2553232x^5\partial^2 + 1104036x^6 - 7538458x^5\partial \\ & + 1769774x^4\partial^2 - 4428356x^5 + 5740077x^4\partial - 739659x^3\partial^2 \\ & + 2474570x^4 - 1935190x^3\partial + 137249x^2\partial^2 + 3533537x^3 \\ & - 20353x^2\partial + 5031x\partial^2 - 3915039x^2 + 154797x\partial + 1431017x \\ & + 10621\partial - 150930. \end{aligned}$$

There are way more wild examples out there. But here we can already see: Even though the degrees do not seem differ a lot, our coefficients become enormous.

For the rational first Weyl algebra, there is a lot of work done in the field to decide whether two polynomials are similar. Besides Tsarev ([**Tsa96**]), also Mark van Hoeij dealt with similar questions in [**vHY10**]. But, as the reader will see, we are approaching the problem from a different point of view. We will not be that much interested in the decision

if two polynomials are similar but more into conditions for them having a chance to be similar that explain the coefficient behavior mentioned above.

1. Similarity in the Polynomial First Weyl Algebra

“In the end we are all separate: our stories, no matter how similar, come to a fork and diverge. We are drawn to each other because of our similarities, but it is our differences we must learn to respect.” – Unknown

Throughout this whole section, R denotes the polynomial first Weyl algebra. We will start with polynomials we are very secure in dealing with, namely the homogeneous ones. There, we will already see some interesting relations two polynomials have to bring with them in order to be similar. Step by step we will go further until we deal with the most difficult case: finding conditions under which two inhomogeneous polynomials are similar. The main result will be, that the differences mainly lie in shifts of the homogeneous factors of degree zero of two similar polynomials.

1.1. Similarity of Homogeneous Polynomials. We have gathered a lot of intuition dealing with $[-1, 1]$ -homogeneous polynomials in the first Weyl algebra by now. Let us therefore start our investigation of similarity conditions with those kinds of polynomials and see what we can find out.

Let $f, g \in R$ be $[-1, 1]$ -homogeneous polynomials (in the further course of the section shortened by the term homogeneous polynomials). The next proposition is a clear but relevant fact.

PROPOSITION 1.1. *Let $a, b \in R$ such that $af = gb$. Then a, b can be chosen homogeneous without loss of generality.*

PROOF. Since f and g are homogeneous, they are a right respectively left divisor of every homogeneous summand of af (which equals gb). Therefore we can pick a random homogeneous summand \hat{a} of a and the corresponding \hat{b} of b . Corresponding means that they must have the same degree after multiplication by f respectively g . Therefore we also have $\hat{a}f = g\hat{b}$. \square

Thus our aim is to find homogeneous a, b , such that $af = gb$ and ${}_R\langle f, b \rangle = \langle a, g \rangle_R = R$. We divide this search into different cases in terms of the degrees of f and g . In what follows, the variable θ denotes the term $x\partial$ as usual. We are going to use some of the swapping rules with x and ∂ , that were given in the introduction, as well as general properties of factorizations of homogeneous polynomials. The main result of this work will be Theorem 1.4, which states that a necessary condition for f and g being similar is a shifted divisibility relation between their factors of degree zero and a product of ascending shifts of θ . If the reader is only interested in the result, he or she can skip the following pages to that theorem.

Case 1: $\deg(g) = \deg(f) = 0$.

This means that we can regard f, g as polynomials in $\mathbb{K}[\theta]$ due to Lemma 2.23 from the introduction.

Let $a = a_0\varphi^k$ and $b = b_0\psi^l$ be homogeneous polynomials in R , where $\psi, \varphi \in \{\partial, x\}$ and $a_0, b_0 \in A_1^{(0)}$, such that $af = gb$. Then we can directly see that $\varphi = \psi$ and $k = l$ for degree reasons. Furthermore, we have – if we swap φ^k to the right using the commutation rules in Corollary 2.21 from the introduction –

$$a_0f \circ (\theta \pm k)\varphi^k = gb_0\varphi^k \iff a_0f \circ (\theta \pm k) = gb_0.$$

Case 1.1: $g \nmid f \circ (\theta \pm k)$ for some $k \in \mathbb{N}_0$.

This means that on the left hand side a_0 must contain factors from g , as they are not completely contained in $f \circ (\theta \pm k)$. Thus $\text{gclid}(a_0, g)$ is a nontrivial polynomial in θ , which contradicts with our aim to have $\langle a, g \rangle_R = R$.

Case 1.2: $g \mid f \circ (\theta \pm k)$ for some $k \in \mathbb{N}_0$.

In this case we have the chance to obtain similarity for f and g . The only thing we have to assure is that the choice of b does not contradict with our desired condition ${}_R\langle f, b \rangle = R$. But when would that happen? From the equality above, we see that b_0 must contain the remaining factors of $f \circ (\theta \pm k)$. If two factors of f are just shifts of each other, we would come to this bad situation. But we can verify or falsify this case very easily. Furthermore, if we can extract φ from f (i.e. if θ or $\theta + 1$ is a factor of f), then the condition would also not hold.

As similarity is an equivalence relation, there must also exist \hat{a} and $\hat{b} \in R$ such that $f\hat{a} = \hat{b}g$ if f and g are similar. Therefore, with the same discussion as above, we come to the result that also $f \mid g \circ (\theta \pm k)$ for a $k \in \mathbb{N}_0$. Therefore $f = g \circ (\theta \pm k)$ for a $k \in \mathbb{N}_0$.

Case 2: $\deg(g) = \deg(f)$.

Let again $a = a_0\varphi^k$ and $b = b_0\psi^l$, $\psi, \varphi \in \{x, \partial\}$ and $a_0, b_0 \in A_1^{(0)}$, such that $af = gb$. Furthermore, write $f = f_0\nu^n, g = g_0\nu^n$, where $g_0, f_0 \in A_1^{(0)}$ and $\nu \in \{x, \partial\}$. Because of degree reasons we must have $\varphi = \psi$ and $k = l$.

Case 2.1: $\varphi = \psi = \nu$

In this case, k, l have to be zero because of the desired divisibility relations between the tuple (f, b) and the tuple (g, a) . That means, $a = a_0, b = b_0$. Therefore we must have

$$a_0f_0 = g_0b_0 \circ (\theta \pm n).$$

Again, we get the subcases $g_0 \mid f_0$ and $g_0 \nmid f_0$.

If $g_0 \mid f_0$, we have to make sure that the choice of b with not violating the ${}_R\langle f, b \rangle = R$ condition is possible. This check can be done with not much effort.

If $g_0 \nmid f_0$, then f and g have no chance to be similar, since the choice of a would result in a nontrivial greatest common divisor (in $\mathbb{K}[\theta]$) between a_0 and g_0 .

Case 2.2: $\nu \neq \varphi = \psi$

Observation: In this case, $\varphi^k\nu^n \neq \nu^n\psi^k$ if k is greater than 0. Furthermore, we can assume k to be smaller than n (otherwise we can just swap some φ s to the left in the two products and would compare a shifted g with f). To get a clear image on how those terms

do look like: In the case $\varphi = \psi = x, \nu = \partial$ we have

$$\varphi^k \nu^n = x^k \partial^n = \left(\prod_{i=0}^{k-1} (\theta - i) \right) \partial^{n-k}$$

and

$$\nu^n \varphi^k = \partial^n x^k = \partial^{n-k} \prod_{i=1}^k (\theta + i) = \left(\prod_{i=1}^k (\theta + i + (n - k)) \right) \partial^{n-k}.$$

In the case $\varphi = \psi = \partial, \nu = x$ we analogously have

$$\varphi^k \nu^n = \partial^k x^n = \left(\prod_{i=1}^k (\theta + i) \right) x^{n-k}$$

and

$$\nu^n \varphi^k = x^n \partial^k = x^{n-k} \prod_{i=0}^{k-1} (\theta - i) = \left(\prod_{i=0}^{k-1} (\theta - i - n + k) \right) x^{n-k}.$$

One can reproduce those equations above using Lemma 2.20 respectively Corollary 2.21 and Theorem 2.22 from the introduction at the beginning of this thesis.

Our product $af = gb$ would thus either look like

$$a_0 f_0 \circ (\theta - k) \left(\prod_{i=0}^{k-1} (\theta - i) \right) \partial^{n-k} = g_0 b_0 \circ (\theta + n) \left(\prod_{i=1}^k (\theta + i + (n - k)) \right) \partial^{n-k},$$

or it would look like

$$a_0 f_0 \circ (\theta + k) \left(\prod_{i=1}^k (\theta + i) \right) x^{n-k} = g_0 b_0 \circ (\theta - n) \left(\prod_{i=0}^{k-1} (\theta - i - (n - k)) \right) x^{n-k},$$

as seen from the equations above.

Case 2.2.1: $g_0 \nmid f_0 \circ (\theta \pm k) (\prod_i (\theta \pm i))$ for a $k \in \mathbb{N}_0$. Then we will never be able to choose a_0 without violating the right ideal condition.

Case 2.2.2: $g_0 \mid f_0 \circ (\theta \pm k) (\prod_i (\theta \pm i))$ for a $k \in \mathbb{N}_0$. Only in this subcase f and g have a chance to be similar. Then we have to make sure that the choice of b_0 is possible without violating the left ideal condition for the tuple (f, b) .

Again due to the symmetry of the similarity relation, there also exist $\hat{a}, \hat{b} \in R$, such that $\hat{b}g = f\hat{a}$ if f and g are possible. In case 2.1 this means $f_0 = g_0$, whereas in case 2.2 we have $f_0 \mid g_0 \circ (\theta \pm k) (\prod_i (\theta \pm i))$ for a $k \in \mathbb{N}_0$.

REMARK 1.2. The careful reader detects that the first case is just a special case of the second one. The reason why we split this into two cases is because the degree zero case is interesting in itself, as we do not have the products of θ -shifts in the equation.

Case 3: $\deg(g) \neq \deg(f)$. This case again splits into subcases. We will start by working off a trivial one, namely where we can instantly say that f and g cannot be similar in that case. Without loss of generality, $\deg(f) > \deg(g)$ since the weak similarity is an equivalence relation on R .

Case 3.1: $\deg(g) < 0, \deg(f) > 0$. Therefore, $g = g_0x^k, f = f_0\partial^l$, where f_0 and g_0 denote the homogeneous factor of degree zero in f and g and $k, l \in \mathbb{N}$. There is no chance of f and g to be similar. This is due to the fact that af and gb have to have the same degree. Therefore either f has to be decreased degree-wise by a (i.e. $a = a_0x^{\hat{k}}, \hat{k} \in \mathbb{N}$) or the g has to be increased degree wise by b (i.e. $b = b_0\partial^{\hat{l}}, \hat{l} \in \mathbb{N}$). Then either f has a common divisor with b – namely ∂ – or g has a common divisor with a – namely x . Therefore we cannot fulfill our left resp. right ideal conditions.

REMARK 1.3. Note, that for the rational first Weyl algebra the polynomials f and g would still have a chance to be similar in this subcase. We will discuss that in the next section, albeit not in detail as it is not that much different.

Therefore, similarity has only a chance to occur, if either both are nonnegative or not positive. As dealing with those two cases is analogous, we will just stick to one case and leave the other one as an exercise to the reader.

Case 3.2: $\deg(g) < \deg(f) \leq 0$.

Thus $f = f_0x^n$ and $g = g_0x^m$, where $m > n \in \mathbb{N}_0$. We are searching for a, b , such that $af = gb$. In order to have $\langle g, a \rangle_R = R$, we must have $\deg(a) \geq 0$. For the analogue reason also $\deg(b) > 0$ must hold. Without loss of generality

$$b = b_0\partial^k, a = a_0\partial^l, k > l \in \mathbb{N}_0.$$

Therefore we have the equation

$$a_0f_0 \circ (\theta + l)\partial^l x^n = g_0b_0 \circ (\theta - m)x^m\partial^k,$$

and for degree reasons we must have $-n + l = -m + k$. Furthermore, we can assume that $l \leq n$ and therefore $k \leq m$, because otherwise we could extract ∂ from the right of the product and just check a shifted version of f for similarity with g .

Case 3.2.1: $g_0 \nmid f_0 \circ (\theta + l) \prod_{i=1}^l (\theta + i)$ for an $l \in \mathbb{N}_0$.

In this case, g and f have no chance to be similar, because we have to fill up the missing divisors in $A_1^{(0)}$ with the a_0 on the left hand side of the equation. That would result in a nontrivial left divisor of a and g and violate our right ideal property $\langle a, g \rangle_R = R$.

Case 3.2.2: $g_0 \mid f_0 \circ (\theta + l) \prod_{i=1}^l (\theta + i)$ for an $l \in \mathbb{N}_0$.

In this case there is a chance of g and f being similar. As usual, we just have to ensure that a proper choice of b is possible.

Of course the symmetry remark does hold again here.

This whole running through all the cases might be seen as redundant accounting at this point, but it actually leads us to the following characterization of similarity of polynomials for the homogeneous case.

THEOREM 1.4. *Let $f, g \in R$ be homogeneous polynomials. If f and g are similar, then there exists $n, k \in \mathbb{Z}, m \in \mathbb{N}_0$, such that*

$$f_0 \mid g_0 \circ (\theta + n) \prod_{i=0}^{m-1} (\theta + i + k),$$

where $\theta = x\partial$ and g_0 and f_0 denote homogeneous factors of degree zero of f and g . This also needs to hold analogously for the other direction, i.e.

$$g_0 \mid f_0 \circ (\theta + \hat{n}) \prod_{i=0}^{\hat{m}-1} (\theta + i + \hat{k})$$

for $\hat{n}, \hat{k} \in \mathbb{Z}, \hat{m} \in \mathbb{N}_0$.

This result gives us a hint, why we get such a coefficient difference while observing two different similar polynomials. We see that in the homogeneous case they are related to each other in the way that their homogeneous factors of degree zero have divisibility relations up to shifts of the indeterminate θ . Those shifts, depending on the degree of our polynomials, can of course cause an enormous growth of the coefficients. Take as an example the polynomial θ^5 . If we operate on θ^5 by three times shifting, we obtain

$$(\theta + 3)^5 = \theta^5 + 15\theta^4 + 90\theta^3 + 270\theta^2 + 405\theta + 243$$

due to the binomial theorem.

We finish the discussion about similarity between two homogeneous polynomials by giving some examples of the positive cases above.

EXAMPLE 1.5. *Same degree:* An easy example would be

$$f := x\partial + 7, \quad g := x\partial + 5.$$

Since $f(\theta - 2) = g(\theta)$, we choose $a := b := x^2$ and obtain

$$x^2 f = g x^2.$$

Furthermore, using SINGULAR, one can verify that ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$

Different degree: Take as an example

$$f := (x^2\partial^2 + 8x\partial + 17)\partial^2, \quad g := (x^2\partial^2 + 6x\partial + 11)\partial.$$

We have $f_0(\theta - 1) = g_0(\theta)$. Then a and b must have degree 1 in x and a possible choice would be

$$a := x, \quad b := (x\partial - 1).$$

Then $a f = g b$ and again using SINGULAR one can verify the property ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$.

1.2. Similarity between a Homogeneous Polynomial and an Inhomogeneous One. In this section, we assume that $f \in R$ is a homogeneous polynomial and g is an inhomogeneous one. We are going to deal with the question, whether we can find a, b , such that $a f = g b$ and where the ideal conditions do hold. Let us first think about if the construction is possible at all. For the commutative case, we can falsify this existence very easy, as the following example shows.

EXAMPLE 1.6. Let R be a commutative domain and let $f, g \in R$ be similar polynomials. We will show that f and g being similar in this case is equivalent to f and g being associated, i.e. there exists a unit $u \in R$ such that $f = u g$. Then it is clear for the special case $R = \mathbb{K}[x_1, \dots, x_n]$ that an inhomogeneous polynomial cannot be similar to a homogeneous one as the units there are elements in \mathbb{K} .

If f and g are similar, there exist a, b , such that $af = gb$ and $\langle b, f \rangle = \langle g, a \rangle = R$. Furthermore, we have $u, v, w, x \in R$ such that $ua + vg = 1 = wb + xf$. From the equation $af = bg$, we can derive

$$\begin{aligned} af &= bg & | \cdot u \\ \iff \underbrace{ua}_{=1-vg} f &= ubg \\ \iff f &= (vf + ub)g \end{aligned}$$

and

$$\begin{aligned} af &= bg & | \cdot w \\ \iff waf &= \underbrace{wb}_{=1-xf} g \\ \iff (wa + wg)f &= g. \end{aligned}$$

Thus it is clear that if $f = 0$ also $g = 0$ must hold. If $f \neq 0$, then $f = (vf + ub)(wa + wg)f$ according to the equations above. Therefore $(1 - (vf + ub)(wa + wg))f = 0$, and as f was chosen not equal to zero and R is a domain, we see that $(vf + ub), (wa + wg)$ must be units in R . Therefore f and g are associated. That associated polynomials are also similar is clear anyways.

This means, that the construction is not possible with sticking to elements of commutative subrings of R . We have to consider the more complex elements in R and try to construct a case, where we see the possibility of the construction.

EXAMPLE 1.7. If we assume b to be homogeneous, we can apply the results we had for homogeneous polynomials in the previous subsection to every homogeneous part of g and a . An example, where we succeed in constructing is

$$f := \partial, \quad g := \partial + \partial^2.$$

Then g is inhomogeneous as desired, and we have for

$$b := x\partial + 6 \text{ and } a := (x\partial + 7) + (x\partial + 8)\partial$$

the property $af = gb$ with ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$.

Here we see, that the commutative world is even different in such simple statements. In the Bachelor thesis this would have occurred in the section ‘‘Horrible things happening in the noncommutative case’’ if that example was known by that time.

The example above had one interesting property: The chosen b was homogeneous. The question now arising is whether the b can also be chosen inhomogeneous. The – unfortunate in the sense of the complexity of the problem – answer to this question is yes, as the following example shows.

EXAMPLE 1.8. Again consider

$$f := \partial, \quad g := \partial + \partial^2.$$

Consider also the two polynomials

$$b := \partial + x\partial + 8 \text{ and } a := x\partial^2 + x\partial + \partial^2 + 11\partial + 9.$$

Then b, g and a are inhomogeneous as desired and f is clearly homogeneous. Furthermore, we have $af = gb$ with ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$.

As a result we therefore get that a homogeneous polynomial can be similar to an inhomogeneous one. From the point of view that f and g are considered to be left resp. right factors of two distinct factorizations of the same polynomial, this fact is somewhat surprising. We challenge the reader to find examples where f and g are nontrivial in x and in ∂ to see how ugly the construction can become.

As we used the same f and g in both Example 1.7 and Example 1.8 one can come to the conjecture that if we can find an inhomogeneous b and an arbitrary a , such that $af = gb$, then we can find also a homogeneous one. But we can also falsify that conjecture using the following example.

EXAMPLE 1.9. Let

$$f := x\partial + 14, \quad g := x\partial + 15 + (x\partial + 17)\partial.$$

We begin with showing that we cannot find a homogeneous b with ${}_R\langle f, b \rangle = R$ such that $f \mid_r gb$. Assume, we have such a b . Let $b := b_0\varphi^n$, $n \in \mathbb{N}$, where b_0 is the homogeneous factor of degree zero of b and $\varphi \in \{x, \partial\}$.

We know that $f \nmid b_0(\theta - n)$ in the case of $\varphi = \partial$ and $f \nmid b_0(\theta + n)$ in the case $\varphi = x$ because of the condition on the left ideal generated by f and b . Therefore, for every homogeneous summand of g , we have to be able to swap a zero homogeneous polynomial to the right after multiplication with b . The summand $x\partial + 15$ in g tells us, that b has to be of degree one, i.e. $b = b_0\partial$. But the second summand requires b to be of degree three. Therefore, the choice of a homogeneous b is not possible. But the choice of an inhomogeneous one is possible as we can use

$$a := x^2\partial^5 + x^2\partial^4 + 22x\partial^4 + 33x\partial^3 + 14x\partial^2 + 54\partial^3 + 255\partial^2 + 196\partial$$

and

$$b := x^2\partial^4 + 20x\partial^3 + 14x\partial^2 + 34\partial^2 + 196\partial.$$

Verifying with SINGULAR, the polynomials f, g, b and a do fulfill all the desired properties.

But all hope that we can find as easy conditions for f and g being similar as for the case where both were homogeneous does not die at this point. We only have to work harder. Let us begin with some notions we will use throughout this subsection.

For what follows, we write $g = g_{n_1} + \dots + g_{n_k}$ and $b = b_{m_1} + \dots + b_{m_l}$, where $n_1 > \dots > n_k, m_1 > \dots > m_l \in \mathbb{Z}$ and the g_{n_i} and b_{m_j} denote the homogeneous summands of degree n_i of g resp. m_j of b for $(i, j) \in \underline{k} \times \underline{l}$.

The following Lemma will appear to be useful. We are giving it in a more general context than we need it right now.

LEMMA 1.10. *Let $f, g, a, b \in R$ be nontrivial polynomials, such that $af = gb$ with ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$. Let \tilde{b} be the polynomial b after addition of some left multiple of f . Then $\tilde{b} \neq 0$, ${}_R\langle f, \tilde{b} \rangle = R$ and there exists \tilde{a} , such that $\tilde{a}f = g\tilde{b}$ and $\langle g, \tilde{a} \rangle_R = R$.*

PROOF. Let us assume $\tilde{b} = b + uf$ for some $u \in R$. That $\tilde{b} \neq 0$ is a trivial consequence, since otherwise f and b would have a nontrivial gcd, i.e. ${}_R\langle f, b \rangle \neq R$. The same holds for the desired property that ${}_R\langle f, \tilde{b} \rangle = R$, since

$${}_R\langle f, \tilde{b} \rangle = {}_R\langle f, b + uf \rangle = {}_R\langle f, b \rangle = R.$$

That f is a right divisor of $g\tilde{b}$ is clear as

$$g\tilde{b} = gb + guf = (a + gu)f.$$

The only missing part is if the choice of a suitable \tilde{a} is still possible. We set \tilde{a} to be

$$\tilde{a} := (g\tilde{b})f^{-1}.$$

It remains to show that $\langle g, \tilde{a} \rangle_R = R$. But one can see this using the following fact: $g(b - \tilde{b}) = g(-uf)$ has clearly f as a right divisor. But we also know that

$$g(b - \tilde{b}) = (a - \tilde{a})f.$$

If we divide by f from the right, this would only affect $b - \tilde{b}$ on the left hand side, since f is a right divisor of $b - \tilde{b} = -uf$. Therefore g is a left divisor of $a - \tilde{a}$. Thus we know that

$$R = \langle a, g \rangle_R = \langle \underbrace{(a - \tilde{a})}_{\text{right multiple of } g} + \tilde{a}, g \rangle_R = \langle \tilde{a}, g \rangle_R,$$

which completes the proof. \square

REMARK 1.11. Those readers who see a possible reinvention of the wheel here we want to remind that we are dealing with a noncommutative ring. Usually the statement above is trivial. One just has to calculate inside $R/{}_R\langle f \rangle$, and then the existence of such a \tilde{b} can be derived. The problem why we had to at least discuss it a little bit is because $R/{}_R\langle f \rangle$ is not a ring, but only a left R -module. Therefore we cannot multiply elements there and have no properties of products we can use in general.

What is the benefit the Lemma above provides us with? We will see very soon that it is crucial for having an idea how one can choose b in $af = gb$. Usually, one can choose it arbitrarily, but with that we can assume it to have some more structure.

Now that we are equipped with some additional knowledge, we will discuss when f and g have the chance to be similar. Recall here that we assumed f to be homogeneous, and g to be inhomogeneous. We are going to look at different cases for our given f regarding its degree and reducibility properties.

Case 1: $\deg(f) = 0$.

This case splits into two separately interesting subcases, namely the subcase where f is irreducible and the subcase where f is reducible.

Case 1.1: f is irreducible in the polynomial first Weyl algebra.

This case will turn out quite interesting, as we can also provide a technique how we can decide the similarity between f and g in this case (see below).

Assume that we have a, b with $af = gb$ fulfilling the left resp. right ideal properties. Due to Lemma 1.10, we can assume that we cannot exclude f from the right of any homogeneous summand of b .

We furthermore know that gb has the form

$$gb = \sum_{i=n_1+m_1}^{n_k+m_l} \sum_{\substack{(j_1, j_2) \in \underline{k} \times \underline{l}, \\ n_{j_1} + m_{j_2} = i}} g_{j_1} b_{j_2}.$$

The highest homogeneous summand and the lowest homogeneous summand of that product are just $g_{n_k} b_{m_l}$ and $g_{n_1} b_{m_1}$. In order to obtain f to be a right divisor of those two – and we need this to happen in order to have $af = gb$ –, we have to be able to swap a homogeneous factor of degree zero to the right, and after all the shifts during that swapping it has to result in f . But this zero homogeneous part cannot come from b because of our choice of b . Therefore, g_{n_k} and g_{n_1} must contain a shifted version of f as a homogeneous factor of degree zero.

This is a condition our g has to fulfill in order to have a chance to be similar to f . Let us formulate that in the following corollary.

COROLLARY 1.12. *Consider a homogeneous, irreducible polynomial $f \in R$ of degree zero and an inhomogeneous polynomial $g = g_{n_1} + \dots + g_{n_k} \in R$. If f and g are similar, then there exists $r, s \in \mathbb{Z}$, such that $f \circ (\theta + r) | g_{n_1}^{(0)}$ and $f \circ (\theta + s) | g_{n_k}^{(0)}$.*

But we get even more out of this knowledge, namely an algorithm to check whether f and g are similar in this case.

We have finitely many possibilities for the maximum and minimum degrees of b . We just have to look at the different shifts contained in the highest homogeneous summand and the lowest homogeneous summand of g (there might be multiple ones).

Just think as an example about $f = x\partial + 14$ and $g_{n_1} = (x\partial + 3)(x\partial + 13)(x\partial + 7)\partial^5$. Therefore we get a system of terms for the homogeneous factors of degree zero of the $b_{m_j}, j \in \underline{l}$, which we can solve for right divisibility of gb by f . They have to fulfill the property that for every homogeneous summand in between $g_{n_k} b_{m_l}$ and $g_{n_1} b_{m_1}$ we must be able to extract f . Furthermore, $f(\theta + m_j) \nmid b_{m_j}^{(0)}$ for all $j \in \underline{l}$ since we do not want to have f being a right divisor of any homogeneous summand of b .

Here is a sketch of some steps how one can decide whether a given pair (f, g) is similar.

- If the homogeneous factor of degree zero of g_{n_1} or the homogeneous factor of degree zero of g_{n_k} does not contain a shift of f as a divisor, then f and g have no chance to be similar. Therefore return “False”.
- For all $m_1 > m_l \in \mathbb{Z}$, such that $f | g_{n_1}^{(0)} \circ (\theta + n_1 + m_1)$ and $f | g_{n_k}^{(0)} \circ (\theta + n_k + m_l)$:
 - a) Solve system for $b_{m_j}, j \in \underline{l}$, such that f does divide gb from the right and $f \nmid b_{m_j}^{(0)} \circ (\theta \pm m_j)$.
 - b) $M :=$ The solution set of the system above
- Filter the solutions in M where ${}_R \langle f, b \rangle \neq R$ or $\langle a, g \rangle_R \neq R$, where $a := gb f^{-1}$.
- Return M .

The solution for a) is not that hard to find as it looks like, even though it is is not a system of equations we have there, but a system that has to fulfill a divisibility criterion. Let us perform this algorithm on an example to show how one can use it.

EXAMPLE 1.13. We take f and g from Example 1.9, i.e.

$$f := x\partial + 14, \quad g := x\partial + 15 + (x\partial + 17)\partial.$$

We have $k = 2$, $n_1 = 1$, $n_2 = 0$ and $g_1 = (x\partial + 17)\partial$, $g_0 = x\partial + 15$. We see that a shift of f is dividing the homogeneous factor of degree zero of every summand of g , and the only possibility for the tuple (m_1, m_i) is $(2, 1)$. Therefore we have $b = b_2\partial^2 + b_1\partial$. Unaffected by the choice of b_1 and b_2 is clearly g_0b_2 and g_1b_1 , since f will be a divisor anyway. We just already know that $(\theta + 15) \nmid b_1$ and $(\theta + 16) \nmid b_2$. The term that we are interested in will be

$$\partial^2(b_2 \circ (\theta - 2)g_0 \circ (\theta - 2) + b_1 \circ (\theta - 1)g_1^{(0)} \circ (\theta - 2)),$$

and our aim is that f divides it from the right. Ignoring the ∂^2 on the left hand side and the shifts of the b_i , we have the term

$$(\theta + 13)b_2 + (\theta + 15)b_1.$$

Here, we know that

$$(\theta + 13) \cdot (\theta + 15)\theta + (\theta + 15) \cdot (\theta + 13) \cdot 14 = (\theta + 15)(\theta + 13)(\theta + 14).$$

Therefore, we can choose $b_1 = 14(\theta + 14)$ and $b_2 = (\theta + 17)(\theta + 2)$, which results in the b of Example 1.9.

How unique was that choice? Well, we had to come up with b_i 's not being divisible by f . At first we regarded the equation $(\theta + 13)b_2 + (\theta + 15)b_1$, and we wanted to have $(\theta + 14)$, i.e. our f , being a divisor of it. The only restrictions are that

$$(\theta + 14) \nmid b_1 \text{ and } (\theta + 14) \nmid b_2$$

(recall that we ignored at this points the shifts of the b_i). Therefore, possibilities to choose them were given by $b_1 = (\theta + 13)\tilde{b}_1$ and $b_2 = (\theta + 15)\tilde{b}_2$, where \tilde{b}_1 and \tilde{b}_2 are polynomials not divisible by f , but their sum is divisible by f . And the possibilities b_i having that shape are infinitely many.

But a clear false statement can be given after a finite amount of steps. If one would implement it as an algorithm, then the way would be to try to find at least one b and one a . If the answer is false it will become clear very fast. Otherwise choose just one solution.

Let us proceed with our case discussion. Recall that we are in the case where we assume f to be homogeneous of degree zero. We finished the discussion about the case where f is irreducible. Now we proceed with the case where f is reducible.

Case 1.2: f is reducible in the polynomial first Weyl algebra.

We write $f = f_1 \cdots f_\nu$ for the factorization of f , where the f_i are not units in R . Again, assume that there exists $a, b \in R$ not necessarily homogeneous such that $af = gb$ and the left resp. right ideal condition does hold. Due to Lemma 1.10 we can assume that we cannot extract f completely from the right out of one of the homogeneous summands of b .

Furthermore we can make the following observation.

OBSERVATION 1.14. For every $i \in \underline{\nu}$, there exists a b_{m_j} , such that $f_i \nmid_r b_{m_j}$. In other words: There is at least one homogeneous summand b_{m_j} of b that does not contain $f_i \circ (\theta - m_j)$ as right factor.

This can be seen using the condition that ${}_R\langle f, b \rangle = R$. Would there be an f_i that could be extracted in every homogeneous summand of b then this would be a nontrivial common right divisor of f and b and the left ideal generated by f and b would not be R .

Therefore we can use a similar approach as in Case 1.1. We know that we can extract f from every homogeneous summand of gb . Especially in g_1b_1 and $g_{n_k}b_{m_l}$ we see that the missing divisors f_i that cannot be extracted from the right from b_1 resp. b_{m_l} must appear shifted accordingly in the zero homogeneous part of g_1 resp. g_{n_k} .

This leads to a condition g has to satisfy in order to have a chance to be similar to f . We state it in the following corollary.

COROLLARY 1.15. *Let $f = f_1 \cdots f_\nu \in R$ be a homogeneous polynomial of degree zero and the $f_i, i \in \underline{\nu}$, its nontrivial factors. Let furthermore $g = g_{n_1} + \dots + g_{n_k} \in R$ be a inhomogeneous polynomial. If f and g are similar in the sense of Definition 2.7 given in the introduction, then the homogeneous factor of degree zero of g_{n_1} and the homogeneous factor of degree zero of g_{n_k} contain each at least one shifted f_i as a factor.*

If we have g given and it fulfills the property above, then we have knowledge of the maximum and minimum degree of b and can solve a system for the different $b_{m_j}^{(0)}$ s. This can be done as described in the previous case. Just the conditions on b are a little bit more strict, which makes the falsification a lot more easy.

Now we have finished the discussion about the case where f is homogeneous of degree zero and we go on by discussing the case where it has an arbitrary degree. A specialty of this case is actually that the common divisors of f with g_{n_1} resp. g_{n_k} can also be x or ∂ , not just polynomials in θ .

Case 2: $\deg(f) \neq 0$.

We will assume that without loss of generality we have $\deg(f) > 0$, i.e. $f = f_0 \partial^{\deg(f)}$ where f_0 denotes the homogeneous factor of degree zero of f .

The techniques will be similar as in Case 1, but we have here in all cases but $f = \partial$ that f is reducible. Let us by start working off the easy subcase where $f = \partial$. But first we make the following observation for this case.

OBSERVATION 1.16. In gb we have to be able to extract $\partial^{\deg(f)}$. Furthermore, in order not to violate the condition ${}_R\langle f, b \rangle = R$ there has to be at least one homogeneous summand of b , where we cannot extract ∂ from the right, which also means that it has at least one of degree less or equal to zero.

Case 2.1: $f = \partial$.

As usual, we consider $g_{n_1}b_{m_1}$ and $g_{n_k}b_{m_l}$. And our good friend, Lemma 1.10 does hold again. In this case it means that every homogeneous summand of b has to have degree less or equal to zero. There are the following possibilities that can occur:

- A power of ∂ can be extracted from g_{n_1} or g_{n_k} from the right. Then b_{m_1} resp. b_{m_l} can be chosen such that we can swap one ∂ to the right.
- There is no power of ∂ that can be excluded from g_{n_1} or g_{n_k} from the right, but g_{n_1} contains a shift of θ . Then we can choose b_{n_1} resp. b_{m_l} such that swapping this factor leads to θ on the right (i.e. ∂ can be excluded from the right) and the degree chosen for b_{m_1} and b_{m_l} is less or equal to zero because of Lemma 1.10.
- There is a power of ∂ that can be extracted from g_{n_1} or g_{n_k} from the right, and there is a shift of θ in its homogeneous factor of degree zero as a factor. Then we have the possibility to choose b_{m_1} resp. b_{m_l} such that we can swap ∂ to the right

or such that the shift of θ becomes θ when swapping it completely to the right. Again, b_{m_1} and b_{m_l} have to be of degree less or equal to zero.

Therefore, as a first condition on g for being similar to f would be that we have at least in the highest and in the lowest homogeneous summand either a power of ∂ as a right divisor, or a shift of θ , or both. In the case where there is a shift of θ in it we also have as a condition that swapping it to the right of g will make it a negative shift of θ , since only degrees less or equal to zero are allowed for the b_{m_i} .

As we see here, we can again solve systems for different bs , and additionally to the cases mentioned above, we have some statements for possible highest and lowest degrees for b . Therefore, everything goes down again to the solvability of the systems with some side conditions.

Case 2.2: $\deg(f) > 0$, $f \neq \partial$.

In this case we know that $f = f_0 \partial^{\deg(f)}$ is always reducible with at least two nontrivial factors.

We can make an analogue observation as in Observation 1.14. The difference is that we have not only factors in θ , but also in ∂ . The analogue observation is therefore: Given the homogeneous summands $b_{m_i}^{(0)} \varphi^{m_i}$, $\varphi \in \{x, \partial\}$, of b in standard form. Then there exists at least one b_{m_i} where ∂ is not a right divisor, and for every divisor \hat{f} of f_0 there exists at least one $b_{m_i}^{(0)}$, such that

$$\gcd(b_{m_i}^{(0)} \circ (\theta - m_i), \hat{f} \circ (\theta - \deg(f))) = 1.$$

With that we assure that we keep the condition ${}_R\langle f, b \rangle = R$.

Moreover, we have $f \nmid_r b_{m_i}$ for all $i \in \underline{l}$ because of Lemma 1.10.

From now on, everything is similar to Case 1.2. We again look at the highest homogeneous summand g_{n_1} and the lowest g_{n_k} and check, whether we can find either a power of ∂ as a right divisor, or at least one shifted version of θ , or a shifted divisor of f_0 in $g_{n_1}^{(0)}$ resp. $g_{n_k}^{(0)}$, or both.

If nothing of that can be found in both g_{n_1} and g_{n_k} , we can say that f and g have no chance to be similar. If it can be found, everything reduces to solving systems of terms with divisibility conditions as before. We will not go again through the details because there is nothing completely new, but just state an example.

EXAMPLE 1.17. As an example, we choose

$$f := (\theta + 14)\partial, \quad g := (\theta + 13)\theta + (\theta + 15)\partial.$$

We have several choices for possible maximum and minimum degrees for b . We choose for that example the minimum homogeneous part of b to be of degree 0 due to the observation that

$$(\theta + 13)\theta = (\theta + 13)x\partial = x(\theta + 14)\partial = xf.$$

The next observation

$$(\theta + 15)\partial = \partial(\theta + 14)$$

indicates that a possible choice for the maximum degree of b is one. Therefore we have two unknown variables b_0 and b_1 in $b = b_0 + b_1\partial$, such that $f \mid gb$. We must also have $\theta \nmid b_0$, because ∂ would otherwise be a gcd of f and b . In order for f not being a right divisor of $b_1\partial$, the term $\theta + 14$ also must not divide b_1 .

We have

$$\begin{aligned} gb &= g_0b_0 + g_1b_0 \circ (\theta + 1)\partial + g_0b_1\partial + g_1b_1 \circ (\theta + 1)\partial^2 \\ &= b_0xf + ((\theta + 15)b_0 \circ (\theta + 1) + (\theta + 13)\theta b_1)\partial + b_1 \circ (\theta + 1)\partial f. \end{aligned}$$

Thus, the only term that we have to construct such that f is a right divisor of it is

$$((\theta + 15)b_0 \circ (\theta + 1) + (\theta + 13)\theta b_1)\partial.$$

We can set $b_1 := (\theta + 15)\theta$ and $b_0 := 14(\theta + 12)$. This choice does not violate the conditions and results in f being a right divisor of the term above. Using SINGULAR, we can find a , such that $af = gb$, namely $a := x^2\partial^2 + 14x^2\partial + x\partial^2 + 29x\partial + 182x + 16\partial + 195$. Using SINGULAR again we verify that ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$.

1.3. Similarity between Two Inhomogeneous Polynomials. The case where f and g are both given inhomogeneous is the most general and generic case. The main problem is that we do not have as easy conditions to determine whether f is a right divisor of a given polynomial as we had in the homogeneous case. There, we just had to determine the degree and whether we could swap certain shifts of the homogeneous factor of degree zero of f to the right. In the general case different summands of f are affecting the homogeneous summands of a polynomial if it has f as a right divisor.

Therefore, solving for a $b \in R$ such that $f \mid_r gb$ and $\text{gcd}(f, b) = 1$ will appear way more difficult as we cannot just work off homogeneous part by homogeneous part and try to extract f there.

Another problem appearing is that our former arguments for bounding the degrees of the summands in b are not valid in general. Fortunately, as we will see in this section, we can nevertheless find ways to state some bounds.

For the rest of this section, we denote – partly as it was done before – by

$$\begin{aligned} g &= g_{n_1} + \dots + g_{n_k}, \\ b &= b_{m_1} + \dots + b_{m_l}, \\ a &= a_{\mu_1} + \dots + a_{\mu_c} \text{ and} \\ f &= f_{\nu_1} + \dots + f_{\nu_d}, \end{aligned}$$

where $n_1 > \dots > n_k, m_1 > \dots > m_l, \mu_1 > \dots > \mu_c, \nu_1 > \dots > \nu_d \in \mathbb{Z}, l, c \in \mathbb{N}, k, d > 1 \in \mathbb{N}$, the representation of the polynomials $a, b, f, g \in R$ as sum of their homogeneous summands of degree μ_i , respectively m_i, ν_i , and μ_i .

We always assume f and g to be given and we are searching for a and b such that $af = gb$ and ${}_R\langle f, b \rangle = \langle g, a \rangle_R = R$.

First of all, let us work on the degree bounds for b as mentioned above. For that we will assume that f and g are similar, i.e. a, b with the desired properties do exist, but not yet known to us. We know from the factorization technique for the first Weyl algebra in [Hei10] that in order to have $af = gb$, we can directly conclude that

$$a_{\mu_1}f_{\nu_1} = g_{n_1}b_{m_1} \text{ and } a_{\mu_c}f_{\nu_d} = g_{n_k}b_{m_l}.$$

We will make heavy use of that fact.

As the previous subsection has shown to us, a discussion about the possible shape of b appears to be very fruitful. We will try to start with that here, too. The following proposition gives us some statements about the degree range in b .

PROPOSITION 1.18. *Using the denotations above, one of the two following possibilities can occur:*

- i) $m_1 - m_l < \nu_1 - \nu_d$
- ii) $m_1 - m_l \geq \nu_1 - \nu_d$ and $f_{\nu_1} \nmid_r b_{m_1}$, $f_{\nu_d} \nmid_r b_{m_l}$.

This means that either the range of homogeneous summands in b is bound by the number in f , or f_{ν_1} respectively f_{ν_d} are no right divisors of b_{m_1} or b_{m_l} respectively.

PROOF. Assume we have $m_1 - m_l \geq \nu_1 - \nu_d$ with $f_{\nu_1} \mid_r b_{m_1}$ or $f_{\nu_d} \mid_r b_{m_l}$. Without loss of generality we will assume $f_{\nu_1} \mid_r b_{m_1}$. Then

$$b_{m_1} = \tilde{b}_{m_1} f_{\nu_1}$$

for $\tilde{b}_{m_1} \in R$. Due to Lemma 1.10 our choice of b is invariant up to added left multiples of f . If we perform the subtraction

$$b - \tilde{b}_{m_1} f =: b',$$

we know thus that we again have an a' so that $a'f = gb'$ fulfilling the left respectively right ideal condition.

Our new $b' = b'_{m'_1} + \dots + b'_{m'_{l-1}}$ has the property that its highest homogeneous summand has a degree lower than that of b , and its range of homogeneous summands decreased. If after this reduction step for our new b' already $m'_1 - m'_{l-1} < \nu_1 - \nu_d$ does hold, we are done. If otherwise this new highest homogeneous summand has again f_{ν_1} as a right divisor, we can repeat the step above. After a finite amount of steps we will either reach the point that the highest homogeneous part is not divisible by f_1 from the right any more, or we have $m'_1 - m'_{l'} < \nu_1 - \nu_d$ for the new b' with $l' < l \in \mathbb{N}$, which is possibility i) again. Of course we can both have $m'_1 - m'_{l'} < \nu_1 - \nu_d$ and $f_1 \mid_r b'_1$.

In order not to have a too complicated notion, we denote the resulting b' after the reduction steps from the top again by b from here on.

If after the top reduction steps we still have $m_1 - m_l \geq \nu_1 - \nu_d$ and $f_{\nu_d} \mid b_{m_l}$ for the new b , we can perform the analogue reduction steps from the bottom until either $f_{\nu_d} \nmid b_{m_l}$ or $m_1 - m_{l'} < \nu_1 - \nu_d$. \square

We will demonstrate the reduction steps from the proof in an example.

EXAMPLE 1.19. Choose

$$f := \partial^2 + x^2, \quad b := \partial^3 + 1 + x^3.$$

As a note: Those polynomials do not come from two different factorizations, but we can use them to demonstrate the concept we were using in the proof above.

The range between the homogeneous parts of f is smaller than those of b and the highest, as well as the lowest homogeneous summand of f divides the highest and the lowest homogeneous summand of b . Therefore we can make reduction steps. We will start from the top and obtain

$$b' := b - \partial f = 1 - (\theta + 1)x + x^3.$$

Now the range between the highest homogeneous summand and the lowest homogeneous summand of b' is smaller than the range in f and we can stop.

REMARK 1.20. In fact, in the previous example we could have made one more reduction step and decrease the range even more. But this is just due to the nice form b and f had. In general, if we would keep proceeding, we would definitely run into non termination.

Before we start our discussion about conditions for f and g being similar, let us reflect a little bit about the proposition above and the two items it contains.

Item ii) gives the impression that the range between m_1 and m_l is not bounded at all in this case. Fortunately, it is.

Assume case ii) does hold. Therefore $f_{\nu_1} \nmid b_{m_1}$. Since we must have

$$a_{\mu_1} f_{\nu_1} = g_{n_1} b_{m_1},$$

our remaining factors of f_{ν_1} on the right hand side have to be taken from g_{n_1} .

We either have that a power of ∂ (if $n_1 > 0$), or that a power of x (if $n_1 < 0$) or that some shifts of factors of the zero homogeneous factor $f_{\nu_1}^{(0)}$ are missing in b_{m_1} .

In the case where only a power $s \in \mathbb{N}$ of ∂ (respectively a power of x) is missing in b_{m_1} , we know that $\deg_{\partial}(b_{n_1}) < s$. Otherwise it would not be missing. Also its degree towards the negative side is bounded since we have to be able to swap ∂^s completely to the right.

In the case where we are taking a certain shift of a homogeneous factor of degree zero of $f_{\nu_1}^{(0)}$ from g_{n_1} , the degree of b_{n_1} is even uniquely determined by that shift.

The analogue discussion can be made for b_{m_l} . Therefore we have bounds on them given by the structure of g and f .

Still reflecting on Proposition 1.18, another impression is given to us by item i), namely that in this case the range $[m_1, m_l]$ with $m_1 - m_l < \nu_1 - \nu_d$ can occur arbitrarily among the integer numbers. Fortunately again, this is not true.

To see this is not as easy as in item ii), since we do not necessarily have the divisibility conditions $f_{\nu_1} \nmid_r b_{m_1}$, $f_{\nu_d} \nmid_r b_{m_l}$ on the highest and the lowest homogeneous summands of f and b . The following cases are possible.

Case 1: $\nu_d > 0$.

In other words, a power of ∂ is a right divisor of f . In this case, we must have $m_l \leq 0$ in order to have a chance not to violate the condition $\gcd(f, b) = 1$. Among the homogeneous summands of negative degree we then should have at least one given, where we cannot swap θ to the right from the homogeneous factor of degree zero. Otherwise ∂ would still be a right divisor (compare Lemma 2.24 from the introduction).

Moreover, we are restricted in our choice of m_l towards negativity, since we must be able to extract a certain power of ∂ from every homogeneous summand in gb .

Case 2: $\nu_1 < 0$. In other words, a power of x is a right divisor of f . Here we have analogue arguments as in Case 1.

Case 3: $\nu_1 \geq 0, \nu_d \leq 0$.

We have either $\nu_1 \neq 0$ or $\nu_d \neq 0$ or both. The further we move $[m_1, m_l]$ towards positivity or negativity, we have to still be able to compensate this with our given g . This is due to the fact that we need to have a possibility to extract ∂^{ν_1} from $g_{n_1} b_{m_1}$ and $x^{-\nu_d}$ from $g_{n_k} b_{m_l}$.

At this point we are done reflecting on Proposition 1.18 have some statements about the structure of b in the case where f and g are similar. We will now deal with the question if arbitrarily given inhomogeneous f and g have a chance to be similar. I.e. our assumption that f and g are given similar is not necessarily true any more.

The whole discussion above gives us an idea how to construct such a b , if it is existent. Due to Proposition 1.18 we have two possibilities for the structure of b . Let us make a sketch how to find such a b or to falsify the existence. It will be a 3-Step approach, where results can be found in any step.

First of all, we look at f_{ν_1} and g_{n_1} respectively f_{ν_d} and g_{n_k} .

Step 1: If we find a shift of a factor \tilde{f} of $f_{\nu_1}^{(0)}$ within $g_{n_1}^{(0)}$, we would first try out to choose our m_1 to be of an appropriate degree such that swapping that factor in $g_{n_1}^{(0)}$ to the right of $g_{n_1}b_{m_1}$ would result in $\tilde{f}\varphi^{\nu_1}$, $\varphi \in \{x, \partial\}$.

EXAMPLE 1.21. Let for example $f_{\nu_1} := (\theta^2 + \theta + 1)(\theta + 15)\partial^2$ and $g_{n_1} := (\theta^2 + 7\theta + 13)\partial^2$. Then we have $\tilde{f} := (\theta^2 + \theta + 1)$ shifted in $g_{n_1}^{(0)}$ – namely with the factor $\theta^2 + 7\theta + 13$ – and we know that $g_{n_1} = \partial^2(\theta^2 + 3\theta + 3)$. Therefore we need one more shift to obtain \tilde{f} , and furthermore we need $\tilde{f}\partial^2$ to be a right factor of $g_{n_1}b_{m_1}$. Therefore $m_1 = 3$, and a possible choice of b_{m_1} is $(\theta + 16)\partial^3$.

Now it is possible that item i) of Proposition 1.18 does hold, and we would try to solve the system for the range $[m_1, m_l := m_1 - (\nu_1 - \nu_d) + 1]$.

REMARK 1.22. The term “solving the system” has to be treated in the case where f is inhomogeneous in another way than before, but we added a discussion about that to the appendix, since it would be just distracting here.

If we cannot solve it for that range, we can assume that item ii) does hold, and that we have to take at least one factor of f_{ν_d} from g_{n_k} . If there is furthermore neither a shift of a factor of $f_{\nu_d}^{(0)}$ in $g_{n_k}^{(0)}$, nor a $\varphi \in \{x, \partial\}$ a common right factor, we can say, that in this step no appropriate b can be constructed and proceed with Step 2.

If a shift of a factor \tilde{f} of $f_{\nu_d}^{(0)}$ is in g_{n_k} , we can determine the degree m_l directly and try to solve the system for that range. If there is a power of $\varphi \in \{x, \partial\}$ that is a common right divisor of f_{ν_d} and g_{n_k} , then $|m_l| < |\nu_d|$ and since we want to be able to swap φ to the right, its degree has a lower bound determined by g_{n_k} .

EXAMPLE 1.23. Assume $g_{n_k} = x^3$, $f_{\nu_d} = (x\partial + 13)x^2$. In the currently considered case we need to take at least one x from g_{n_k} . Therefore $m_l = -1$ at least. A possible solution such that $g_{n_k}b_{m_l}$ has f_{ν_d} as a right divisor would therefore be $b_{m_l} = (x\partial + 14)x$. A more general solution is given by $b_{m_l} = \tilde{b}(x\partial + 14)x$, where $\tilde{b} \in A_1^{(0)}$.

With this lower bound, we can again try to solve the system for the $b_{m_i}^{(0)}$, and if it is not solvable, then in this step we cannot find any appropriate b .

Of course for dealing with this case we can also start with the lowest homogeneous parts. That works analogously.

Let us summarize Step 1 again here:

Precondition: A shift of a factor \tilde{f} of $f_{\nu_1}^{(0)}$ is a factor of $g_{n_1}^{(0)}$. Assume that item i) from

Proposition 1.18 holds.

Approach: Finding different degree bounds for b and try to solve the system such that f divides gb from the right. If not possible, item ii) might hold or a power of x resp. ∂ is a common divisor of f_{ν_1} and g_{n_1} .

Step 2: If we cannot find any shifted factor of $f_{\nu_1}^{(0)}$ in $g_{n_1}^{(0)}$ respectively a shifted factor of $f_{\nu_d}^{(0)}$ in $g_{n_k}^{(0)}$ or our efforts in step 1 were not leading to an appropriate b , we would as a next step try to check for common right factors in $\{x, \partial\}$ for f_{ν_1} and g_{m_1} .

If f_{ν_1} and g_{m_1} have a power of $\varphi \in \{x, \partial\}$ as a common right factor, we first assume that we have to swap a certain power of φ out of g_{n_1} to the right in $g_{n_1}b_{m_1}$. With that we also have a degree bound for b_{m_1} .

Again, we first try to check how far we can come with item i) from Proposition 1.18 and try to solve the system for the possible ranges $[m_1, m_1 - (\nu_1 - \nu_d) + 1]$.

If that approach was not crowned with success, the last possibility here is that item ii) does hold.

If there is neither a shifted factor of $f_{\nu_d}^{(0)}$ in $g_{n_k}^{(0)}$, nor a $\varphi \in \{x, \partial\}$ a common right factor of f_{ν_d} and g_{n_k} , we can again declare this step as not succeeding.

If such a common factor can be found, we have again a degree bound for b_{m_l} and we can try to solve a system of terms to obtain a divisibility condition. If we do not succeed here, we try our last approach, which is discussed in the next step.

Let us summarize Step 2 again here:

Precondition: Step 1 failed, and f_{ν_1} and g_{n_1} have a power of x resp. a power of ∂ as common factor.

Approach: Finding different degree bounds for b and try to solve the system such that f divides gb from the right. If not possible and we already performed Step 1, item ii) is the last possibility which can occur.

Step 3: If we reach the point where only step 3 is possible, we are very desperate because we did either not succeed in the last two steps or we could not find any common divisors in the highest and in the lowest homogeneous parts.

We can assume without loss of generality that here b_{m_1} is a left multiple of f_{ν_1} and b_{m_l} is a left multiple of f_{ν_d} . Otherwise we would already have tried out to solve for those candidates in the previous steps. Moreover, we are from the perspective of Proposition 1.18 in item i), which means, that $m_1 - m_l < \nu_1 - \nu_l$.

The remaining thing to do is to find out how far this range can go towards positivity or negativity among the integer numbers and try to solve the system for every possibility.

REMARK 1.24. One should not assume that we can leave out those ranges that we checked in the previous steps before. This is due to our new choice of b_{m_1} and b_{m_l} to be left multiples of the corresponding f_{ν_1} and f_{ν_l} . Before at least one factor in each b_{m_1} and b_{m_l} was left out.

After that we either have found our a and b that fulfill all the desired properties, or we can finally state that this choice is not possible at all. In both possibilities we are done.

Let us also summarize this step:

Preconditions: Step 1 and Step 2 failed. No conditions regarding divisibility of homogeneous summands of f with homogeneous summands of g .

Approach: Finding the degree range for b from item ii) in Proposition 1.18. Those are finitely many and then we solve for the b .

This 3-step approach is of course written down in an algorithm way more complex than it seems to be here. The main difficulty lies in the parts where we said that we are solving a system of terms fulfilling a divisibility condition.

Let us summarize what we have encountered on our path dealing with the question when two strictly inhomogeneous polynomials $f, g \in R$ are similar.

We did not have as clear statements as we had when one of them was homogeneous. But Proposition 1.18 helped us to at least have some clarification on the b that we are multiplying to g from the right. Item ii) in this proposition gave us the hint that we are again dealing with shifts from the homogeneous factors of degree zero of the homogeneous summands in f if f and g are similar. If item i) from the proposition does hold, we at least know that in between the solving for an appropriate b we have to take some homogeneous factors of degree zero out of g , which again means that we are shifting. As an ansatz to check whether given polynomials f and g are similar, we have provided a 3-Step approach to do that.

We conclude this subsection with an example.

EXAMPLE 1.25. We take the factors of the different factorizations of h_2 in Chapter 1, subsection 2.2.5. We choose

$$f := x^2\partial - x\partial - 2x + 4, \quad g := x^4\partial - x^3\partial - 3x^3 + 3x^2\partial + 6x^2 - 3x\partial - 3x + 12.$$

Written in terms of $A_1^{(0)}$ -modules (i.e. homogeneous factor of degree zero in $\mathbb{K}[\theta]$), they have the form

$$\begin{aligned} f &= \underbrace{-(\theta - 4)}_{:=f_0} + \underbrace{(\theta - 3)x}_{:=f_{-1}}, \\ g &= \underbrace{-3(\theta - 4)}_{:=g_0} + \underbrace{3(\theta - 2)x}_{:=g_{-1}} - \underbrace{(\theta - 8)x^2}_{:=g_{-2}} + \underbrace{(\theta - 6)x^3}_{:=g_{-3}}. \end{aligned}$$

According to Step 1, we would check the highest homogeneous summands of f and g for (shifted) common factors. In fact, no shift is necessary since $(\theta - 4)$ is already a divisor of both f_0 and g_0 . This leads to our first assumption that $m_1 = 0$, and for this step that $\theta - 4 \nmid b_0 = b_{m_1}$.

Now we check the lowest homogeneous summands f_{-1} and g_{-3} . We observe that $g_{-3} = x^3(\theta - 3)$. Therefore, our next assumption is that $m_l := m_2 = -1$, because there is an x missing on the right in order to have f_{-1} as a right divisor.

Thus our first idea of b is that it is given by

$$b = b_0 + b_{-1}x,$$

where $b_0, b_{-1} \in \mathbb{K}[\theta]$ and $\theta - 4 \nmid b_0$, $\theta - 3 \nmid b_{-1}$.

With this comes our first idea of a to have degree wise components between $\mu_1 = 0$ and $\mu_4 = -3$.

Let us write down $af = gb$ in terms of homogeneous summands.

Degree	af	gb
0	$a_0(-(\theta - 4))$	$-3(\theta - 4)b_0$
-1	$(a_{-1}(-(\theta - 5)) + a_0(\theta - 3))x$	$(3(\theta - 2)b_0 \circ (\theta - 1) + (-3(\theta - 4))b_{-1})x$
-2	$(a_{-2}(-(\theta - 6)) + a_{-1}(\theta - 4))x^2$	$((-\theta - 8)b_0 \circ (\theta - 2) + 3(\theta - 2)b_{-1} \circ (\theta - 1))x^2$
-3	$(a_{-3}(-(\theta - 7)) + a_{-2}(\theta - 5))x^3$	$((\theta - 6)b_0 \circ (\theta - 3) + (-\theta - 8)b_{-1} \circ (\theta - 2))x^3$
-4	$a_{-3}(\theta - 6)x^4$	$(\theta - 6)b_{-1} \circ (\theta - 3)x^4$

We can use a trick here. Since our b just has two homogeneous summands, it is already determined by the equations for degree 0 and the equations for degree -4. What we see there – assuming we take the shifts of factors in f from g – is that $a_{-3} = b_{-1} \circ (\theta - 3)$ and $a_0 = 3b_0$. Since a_0 and a_{-3} are also indeterminates, we have a free choice for b_0 and b_{-1} at this point.

From the equation for degree -1 we get

$$\begin{aligned} & a_{-1}(-(\theta - 5)) + a_0(\theta - 3) = 3(\theta - 2)b_0 \circ (\theta - 1) + (-3(\theta - 4))b_{-1} \\ \iff & a_{-1}(-(\theta - 5)) + 3b_0(\theta - 3) = 3(\theta - 2)b_0 \circ (\theta - 1) + (-3(\theta - 4))b_{-1} \\ \iff & a_{-1}(-(\theta - 5)) = 3(\theta - 2)b_0 \circ (\theta - 1) - 3b_0(\theta - 3) + (-3(\theta - 4))b_{-1}. \end{aligned}$$

Therefore we must have

$$(\theta - 5) \mid 3(\theta - 2)b_0 \circ (\theta - 1) - 3b_0(\theta - 3) + (-3(\theta - 4))b_{-1}.$$

From the equation for degree -3 we can conclude

$$\begin{aligned} & a_{-3}(-(\theta - 7)) + a_{-2}(\theta - 5) = (\theta - 6)b_0 \circ (\theta - 3) + (-\theta - 8)b_{-1} \circ (\theta - 2) \\ \iff & b_{-1} \circ (\theta - 3)(-\theta - 7) + a_{-2}(\theta - 5) = (\theta - 6)b_0 \circ (\theta - 3) + (-\theta - 8)b_{-1} \circ (\theta - 2) \\ \iff & a_{-2}(\theta - 5) = (\theta - 6)b_0 \circ (\theta - 3) + (-\theta - 8)b_{-1} \circ (\theta - 2) - b_{-1} \circ (\theta - 3)(-\theta - 7). \end{aligned}$$

Thus our b_0 and b_{-1} also have to fulfill

$$(\theta - 5) \mid (\theta - 6)b_0 \circ (\theta - 3) + (-\theta - 8)b_{-1} \circ (\theta - 2) - b_{-1} \circ (\theta - 3)(-\theta - 7)$$

In the last equation, namely the one for degree -2, we encounter

$$\begin{aligned} & a_{-2}(-(\theta - 6)) + a_{-1}(\theta - 4) = (-\theta - 8)b_0 \circ (\theta - 2) + 3(\theta - 2)b_{-1} \circ (\theta - 1) \\ \iff & ((\theta - 6)b_0 \circ (\theta - 3) + (-\theta - 8)b_{-1} \circ (\theta - 2) - b_{-1} \circ (\theta - 3)(-\theta - 7))(-\theta - 6) \\ & - (3(\theta - 2)b_0 \circ (\theta - 1) - 3b_0(\theta - 3) + (-3(\theta - 4))b_{-1})(\theta - 4) \\ & = (\theta - 5)((-\theta - 8)b_0 \circ (\theta - 2) + 3(\theta - 2)b_{-1} \circ (\theta - 1)), \end{aligned}$$

which is the last condition we have for b_0 and b_{-1} . Now one can solve for polynomial solutions of those linear recurrency equations with variable coefficients by hand or ask a computer algebra system that can solve recurrency equations. We find besides some other possibilities the known factors

$$b = (\theta - 1) + (\theta - 4)x$$

and the corresponding

$$a = 3\theta - 3 + 3(\theta - 3)x + (\theta - 5)x^2 + (\theta - 7)x^3.$$

Those are known from another example as we might remember, when we dealt with the different factorizations of the polynomial

$$(x^6 + 2x^4 - 3x^2)\partial^2 - (4x^5 - 4x^4 - 12x^2 - 12x)\partial + 6x^4 - 12x^3 - 6x^2 - 24x - 12.$$

Therefore, we are ready and we found the certified answer to the question whether those two polynomials are similar. The answer is – as we already knew before – yes.

1.4. Summarizing the Results for the Polynomial First Weyl Algebra. As I called it before: what was happening in the last 20 and more pages was by the very pure definition accounting. Yet it was necessary to gain some insights about the structure of two similar polynomials in the polynomial first Weyl algebra. Let us reflect again what our original motivation was.

We wanted to find out why we observe such a big difference between similar polynomials considering the size of the coefficients in the underlying field \mathbb{K} . Now we have an idea. Throughout all cases that were discussed in this chapter by now, the existence of shifted common factors in between the homogeneous summands of similar polynomials were either a necessary condition (as for example in Theorem 1.4 and Corollary 1.15), or they were indicators for a possible choice of the cofactors a and b (this subsection). They also appeared on the path of finding an actual solution once one gained some information about the degree range of the cofactors.

Therefore, this is an answer to our original question. The coefficient growth in \mathbb{K} does appear because we are dealing with shifts of certain homogeneous factors of degree zero, and if there are even some powers of θ among the factors of the homogeneous summands, even little shifts can cause large coefficient growth.

A next question would be how we can use that knowledge to get a notion of a normal form or a canonical form or a special normal form for polynomials in the first Weyl algebra in terms of similarity. This normal form should be nice in terms of coefficients respectively degrees, and – if possible – one should also be able to prove that no other polynomial similar to that one can have a nicer shape. As the reader might recognize here, this is just a personal wishlist. Christmas does unfortunately not lie in between my beginning and my handing in of this master thesis. But let us put that question on the agenda for future work.

2. Similarity in the Rational First Weyl Algebra et al.

“Did you ever hear of a kid playing accountant – even if they wanted to be one?” – Jackie Mason

Do not worry, we will not do that whole case running as in the previous section again. We just want to give a quick overview how we can treat other algebras with the knowledge we gained by now.

For the polynomial first shift algebra for example, we can make use of the fact that it is a subalgebra of the polynomial first Weyl algebra. This can easily be seen by the commutation rules we have for θ and ∂ for example shown in the introduction. We have

$$\partial\theta = (\theta + 1)\partial$$

and if we set $S_1 := \partial$ and $x := \theta$, we obtain the first shift algebra. Therefore the discussion above applies if we restrict ourselves to polynomials in θ and ∂ .

For the rational first Weyl algebra, we can first of all use the following trivial, yet interesting fact.

COROLLARY 2.1. *Given $f, g \in A_1$. If f and g are similar, then they are also similar in the rational first Weyl algebra.*

PROOF. Since f and g are similar in the polynomial first Weyl algebra, there exist a, b such that $af = gb$ and $\langle a, g \rangle_{A_1} = {}_{A_1}\langle b, f \rangle = A_1$. As the coefficients $c_1, c_2, \tilde{c}_1, \tilde{c}_2 \in A_1$ such that $ac_1 + gc_2 = 1 = \tilde{c}_1f + \tilde{c}_2b$ and of course a and b do also exist in the rational first Weyl algebra, we have all the conditions we need for f and g being similar as elements in the rational first Weyl algebra. \square

But we have more tuples of polynomials that are similar. Our condition that for $af = gb$ we must have ${}_R\langle f, b \rangle = \langle a, g \rangle_R = R$ is a little bit weaker than in the polynomial case. The gcds resp. the gclds do not have to be 1, but are allowed to be a polynomial in x . With this, we can again go through all cases in the previous chapter and weaken our conditions. But we will recognize, that also here a lot of shifts are responsible for the coefficient difference of similar polynomials.

Let us, just for the sake of interest, consider the similarity question between polynomials f and g in the rational Weyl algebra again, that are given polynomial in both x and ∂ and that are – from the definition given for A_1 – homogeneous. For what follows, by \deg we mean the $[-1,1]$ -degree in A_1 . We will always make sure that we will only give polynomial elements to this degree function.

As x is a unit in the rational first Weyl algebra, we can in general assume that both f and g are given fraction-free.

REMARK 2.2. The last sentence needs a little note here, as it is not that simple as it seems. We need to fix from which side we multiply elements to f and g . From our previous notions we usually chose the left hand side for f and the right hand side for g . Making f fraction-free is easy, but for g the choice of the polynomial making it fraction-free is not that canonical; one has to think more and it usually has a higher degree than the lcm of all denominators. Take as an example

$$g := \frac{1}{x+1}\partial + 1.$$

If we multiply g by $x+1$ (as one would expect it to be the appropriate element) from the right, we obtain

$$\begin{aligned} & \frac{1}{x+1}\partial(x+1) + x+1 \\ &= \frac{1}{x+1}((x+1)\partial + 1) + x+1 \\ &= \partial + \frac{1}{x+1} + x+1 \\ &= \partial + \frac{x^2 + 2x + 2}{x+1}, \end{aligned}$$

which is not fraction-free at all. The correct element in order to obtain a fraction free element here would be $(x+1)^2$. In general, we can say that the least common multiple of the denominators of the coefficients of an element g to the power of $\deg_{\partial}(g) + 1$ would be the element that we need to multiply g from the right with to obtain a fraction-free element (compare Example 3.7 from Chapter 1).

Case 1 and Case 2 (i.e. f and g being homogeneous – from the definition for A_1 – of the same degree) can be copied completely also for the rational first Weyl algebra.

In Case 3 (the case where we considered f and g having different degrees) the first difference occurs, namely in Case 3.1. Therefore let us discuss this case here separately. As it was done in the according chapter, without loss of generality we assume $\deg(f) > \deg(g)$.

Case 3.1: $\deg(g) < 0, \deg(f) > 0$.

Recall that we concluded in the polynomial case that we have no chance for similarity to occur. This is not true now, as we are allowed to have a gcd or a gcd in x . Thus we can premultiply f with a power of x in order to obtain a degree less or equal to zero. The multiplication of g by ∂ is not allowed on the other hand.

After this premultiplication of f by a power of x we land on the ground of Case 3.2, which can again be copied for the case of the rational first Weyl algebra.

Furthermore, as we can equalize the degree using powers of x , we can assume that Case 3 can be completely reduced to Case 2.

As a result, we see directly that more polynomials have a chance to be similar than in the polynomial case. As mentioned before, we will not go through all the cases again. But it might be an interesting task for the future, as we see that there is a wider range of polynomials being similar to each other. Yet the connecting trajectory is still some shifts of homogeneous polynomials of degree zero.

CHAPTER 3

Matrix Normal Forms

In this chapter, we are going to study an approach for calculating the so called Jacobson normal form over Ore Domains. The techniques have been developed recently and were presented at the conference “Symbolic Computation and its Applications” (SCA 2012) and the conference “Computer Algebra in Scientific Computing” (CASC 2012). This was a collaborative work with Prof. Mark Giesbrecht (University of Waterloo, ON, Canada).

Our first step will be to discuss some interesting normal forms over noncommutative rings, and how we can generalize the well known normal forms and concepts from the commutative to the noncommutative case. It turns out that the matrices will be a lot more hard to handle than in the commutative case. We will start with matrices over the rational first Weyl algebra and explain the main ideas using matrices having entries in this algebra. Later, we are going to extend those ideas to other Ore domains and additionally provide some structure properties that have been discovered while working in this field.

Of course, this chapter is not detached from the other chapters of this thesis. The problem of similar polynomials will occur again, but we are going to look at it from another point of view than we did in the chapter about the factorization. We will furthermore be interested in how to manipulate elements to change the gcd or the gld , respectively.

There will also be a need for a little excursion to algebraic probability theory, since the algorithm to be discussed is the so called Las Vegas type. We will define later what this means.

1. Linear Algebra over Ore Domains

1.1. Basic Notions. Let $R := \mathbb{K}(x)[\partial; \sigma, \delta]$ be an Ore domain. We consider matrices $R^{n \times m}$, $n, m \in \mathbb{N}$. Recall that we assumed in general that we are only dealing with Ore extensions, where σ is an automorphism. It is easy to verify by hand that therefore R is a left and right euclidean domain if one chooses the euclidean function given by the degree in ∂ .

In commutative algebra, there are several normal forms, e.g. the Smith normal form for principal ideal domains. In order to make the steps reversible, the transformations are done by so called unimodular matrices. They are defined in the same way for noncommutative algebras.

DEFINITION 1.1. A matrix $A \in R^{n \times n}$ is called **unimodular**, if there exists a matrix $B \in R^{n \times n}$ with the property that $AB = BA = I$, where I denotes the identity matrix.

We will also use those matrices for transformation steps in order to obtain the presented normal forms. But we are facing some problems in deciding whether a given matrix is unimodular or not.

EXAMPLE 1.2. In order to decide whether a matrix A over a commutative domain is unimodular, we just had to compute its determinant. If it is a unit, then A is unimodular; if it is not, the matrix A is not unimodular. In the noncommutative case the determinant defined in the classical way

$$\det(A) = \sum_{\pi \in S_n} \prod_{i=1}^n A_{i\pi(i)}$$

does not have the nice properties we are using constantly in Linear Algebra. As an example take the two matrices over the first Weyl algebra

$$A := \text{diag}(\partial, \partial), \quad B := \text{diag}(x, x).$$

Then $\det(A) = \partial^2$ and $\det(B) = x^2$. Therefore $\det(A) \cdot \det(B) = \partial^2 x^2 \neq x^2 \partial^2 = \det(B) \cdot \det(A)$. Moreover, $AB = \text{diag}(x\partial + 1, x\partial + 1)$ and

$$\det(AB) = (x\partial + 1)^2 = x^2 \partial^2 + 3x\partial + 1 \neq x^2 \partial^2 + 4x\partial + 2 = \det(A) \cdot \det(B).$$

REMARK 1.3. The determinant and its properties were useful tools for proving a large number of theorems in Linear Algebra. Even though we cannot use it any more in the noncommutative case as shown in the previous example, there are maps $R^{n \times n} \rightarrow R$ that have some of the properties the classical determinant has though. The two most famous ones are the quasideterminants developed by Gelfand and Retakh in [GR91] and the Dieudonné determinants presented by Dieudonné in [Die43]. We will not go into details how they are constructed, as it would take a whole section just to present them.

Despite those obstacles, we have mainly one type of transformation matrix that we are interested in, where the unimodularity property is not trivially given. Namely the transformation matrices $A \in R^{2 \times 2}$ that transform a given vector $[u, v]^T \in R^2$ in the way that

$$A \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} \text{gcd}(u, v) \\ 0 \end{bmatrix}.$$

This means, that the entries of A are given by

$$A = \begin{bmatrix} c_1 & c_2 \\ l_1 & -l_2 \end{bmatrix},$$

where $c_1, c_2 \in R$ are the coefficients of the gcd computation of u and v (i.e. $c_1 u + c_2 v = \text{gcd}(u, v)$) and l_1 and l_2 are the smallest elements in terms of degree in ∂ , such that $l_1 u = l_2 v$.

LEMMA 1.4. *Let $u, v \in R$, and*

$$A := \begin{bmatrix} c_1 & c_2 \\ l_1 & -l_2 \end{bmatrix} \in R^{2 \times 2},$$

such that $c_1 u + c_2 v = \text{gcd}(u, v)$ and $l_1 u = l_2 v = \text{lcm}(u, v)$. Then A is unimodular.

PROOF. We can assume without loss of generality that the gcd of u and v is 1. This is due to the fact that if u and v have a nontrivial gcd g , we can write u as $\tilde{u}g$, v as $\tilde{v}g$ for $\tilde{u}, \tilde{v} \in R$ and then $c_1 \tilde{u} + c_2 \tilde{v} = \text{gcd}(\tilde{u}, \tilde{v}) = 1$, $l_1 \tilde{u} = l_2 \tilde{v}$.

We are proving the statement by constructing an inverse $B \in R^{2 \times 2}$ of A . The first column of B can be chosen as $[u, v]^T$. For the second column we use the fact, that l_1 and

We define the **determinant polynomial of M** by

$$|M| := \sum_{i=0}^{c-r} \det(M_i) \partial^i,$$

where M_i is the $r \times r$ matrix with

- $(M_i)_{-,k} := (M)_{-,k}$ for $k \in \underline{r-1}$, i.e. the first $r-1$ columns coincide with M .
- $(M_i)_{-,r} := (M)_{-,c-i}$.

Now let $\mathcal{A} : A_1, \dots, A_r$ be a sequence of polynomials in R and let $d := \max\{\deg_{\partial}(A_i) \mid i \in \underline{r}\}$. Then we define $\text{mat}(\mathcal{A}) \in R^{r \times d+1}$ as the matrix, where $\text{mat}(\mathcal{A})_{ij}$ is the coefficient of ∂^{d+1-j} in A_i , $1 \leq i \leq r, 1 \leq j \leq d+1$. If $r \leq d+1$, the determinant polynomial of \mathcal{A} is defined to be $|\text{mat}(\mathcal{A})|$, which is further denoted by $|A_1, \dots, A_r|$ or $|\mathcal{A}|$.

EXAMPLE 1.7. Take the two polynomials $A_1 := x\partial + 1$ and $A_2 := x\partial^2 + \partial + x$ in the first Weyl algebra and let $\mathcal{A} := A_1, A_2$. Then

$$\text{mat}(\mathcal{A}) = \begin{bmatrix} 0 & x & 1 \\ x & 1 & x \end{bmatrix}$$

and

$$|\text{mat}(\mathcal{A})| = \det \left(\begin{bmatrix} 0 & 1 \\ x & x \end{bmatrix} \right) + \det \left(\begin{bmatrix} 0 & x \\ x & 1 \end{bmatrix} \right) \partial = -x^2\partial - x.$$

With that we can finally give a notion of subresultants in R .

DEFINITION 1.8. Let $p_1, p_2 \in R$ with $\deg_{\partial}(p_1) = m$ and $\deg_{\partial}(p_2) = n$, $m \geq n$. The **n th subresultant** of p_1 and p_2 is p_2 . For $j \in \{n-1, \dots, 0\}$, the **j th subresultant of p_1 and p_2** , $\text{sres}_j(p_1, p_2)$, is

$$|\partial^{n-j-1}p_1, \dots, \partial p_1, p_1, \partial^{m-j-1}p_2, \dots, \partial p_2, p_2|.$$

The sequence $\mathcal{S}(p_1, p_2) : p_1, p_2, \text{sres}_{n-1}(p_1, p_2), \dots, \text{sres}_0(p_1, p_2)$, is called the **subresultant sequence** of p_1 and p_2 .

The next theorem shows how we can use subresultants to calculate and give statements about the gcd of two polynomials $p_1, p_2 \in R$.

THEOREM 1.9. *Let d be the degree in ∂ of the gcd of $p_1, p_2 \in R$. Then sres_d is a gcd of p_1 and p_2 . Furthermore we have*

$$d = 0 \iff \text{sres}_0(p_1, p_2) \neq 0.$$

We will leave the theorem without a proof, since it is not very interesting for our further path. For detailed reading and further properties of the subresultant theory we recommend [Li98] and [Cha91].

Now we are done with the basic preliminary work. Let us continue with two matrix normal forms.

1.3. The Hermite Normal Form. C. Hermite introduced this normal form in [Her08] for matrices with entries in the integer ring. It can be seen as an analogue to the reduced echelon form. The idea can be generalized to matrices over polynomial rings, and also to matrices over Ore polynomials. We will skip the definition for the commutative rings here and go directly to the definition for matrices over R . But before that, we need a notion for the concept of a rank of a Matrix over R . We make use of the fact that our chosen ring $R = \mathbb{K}(x)[\partial; \sigma, \delta]$ possesses a quotient skew field.

DEFINITION 1.10. We define the row (column) rank of a matrix $A \in R^{n \times n}$ as the row (column) rank of the A in the quotient skew field of R .

For further readings on Linear Algebra over skew fields consider [Zer06].

DEFINITION 1.11. Let $A \in R^{n \times n}$ be a matrix with full row rank. There exists a unimodular matrix $Q \in R^{n \times n}$, such that $H = QA$ is an upper triangular matrix with the property that

- The diagonal entries H_{ii} are monic;
- Each superdiagonal entry is of degree (in ∂) lower than the diagonal element in its column (i.e., $\deg_{\partial} H_{ji} < \deg_{\partial} H_{ii}$ for $1 \leq j < i \leq n$)

The matrix H is called the **Hermite normal form** of A .

REMARK 1.12. The Hermite form (with monic diagonals) is unique in the commutative case as well as for entries in the Ore domain R .

EXAMPLE 1.13 (compare [GK12]). Let $A \in R^{3 \times 3}$, where R is the rational first Weyl algebra, be given by

$$A := \begin{bmatrix} 1 + (x+2)\partial + \partial^2 & 2 + (2x+1)\partial & 1 + (1+x)\partial \\ (2x+x^2) + x\partial & (2+2x+2x^2) + \partial & 4x+x^2 \\ (3+x) + (3+x)\partial + \partial^2 & (8+4x) + (5+3x)\partial + \partial^2 & (7+8x) + (2+4x)\partial \end{bmatrix}.$$

The Hermite normal form H of A is

$$H = \begin{bmatrix} (2+x) + \partial & 1+2x & \frac{-2+x+2x^2}{2x} - \frac{1}{2x}\partial \\ 0 & (2+x) + \partial & 1 + \frac{7x}{2} + \frac{1}{2}\partial \\ 0 & 0 & -\frac{2}{x} + \frac{-1+2x+x^2}{x} + \partial^2 \end{bmatrix},$$

and the unimodular transformation matrix Q is given by

$$Q = \begin{bmatrix} \frac{1-x}{2x} & \frac{1}{x} + \frac{1}{2x}\partial & -\frac{1}{2x} \\ \frac{x}{2} - \frac{1}{2}\partial & -\frac{1}{2}\partial & \frac{1}{2} \\ \frac{1+2x^2}{x} + (x-1)\partial & \frac{2}{x} + \frac{1-2x}{x}\partial - \partial^2 & -\frac{1}{x} + \partial \end{bmatrix}.$$

How can one compute the Hermite normal form? Well, the easiest yet not the most efficient way is to eliminate step by step all entries down of the diagonal using matrices as given in Lemma 1.4. In order to obtain the property that the upper diagonal entries have smaller degree than the diagonal entries one simply performs a quotient and remainder computation.

M. Giesbrecht and M.S. Kim presented a more efficient way of computing the Hermite normal form in [GK12]. Describing their technique would be a very long excursion. Therefore I just leave this reference here for the interested reader.

1.4. The Jacobson Normal Form. The Jacobson normal form is a fundamental invariant of matrices over a ring of Ore polynomials. Much like the Smith normal form (see [Smi61] or any random lecture notes in Linear Algebra) over a commutative principal ideal domain, it captures important information about the structure of the solution space of a matrix over the ring, and many important properties of the corresponding system of recurrence or differential equations.

DEFINITION 1.14 (Compare [Jac43], Theorem 16). For every rectangular matrix $A \in R^{n \times m}$ one can find unimodular matrices $U \in R^{n \times n}$, $V \in R^{m \times m}$, such that UAV is associated to a matrix in diagonal form

$$\text{diag}(e_1, \dots, e_s, 0, \dots, 0).$$

Each element e_i is a total divisor of e_j if $j > i$. This is called the **Jacobson normal form** of A .

REMARK 1.15. Unlike the Hermite normal form, the diagonal entries in the Jacobson normal form are unique up to the very weak notion of similarity introduced and discussed in the previous chapter. Therefore one can obtain using different algorithms also different results, which are similar, but they can look arbitrarily ugly.

From now on we set R to be the first rational Weyl algebra. We can state even stronger structure properties to the Jacobson normal form (compare [Coh85]).

COROLLARY 1.16. For every rectangular matrix $A \in R^{n \times m}$, where R is the rational first Weyl Algebra, one can find unimodular matrices $U \in R^{n \times n}$, $V \in R^{m \times m}$, such that UAV is associated to a matrix in diagonal form $\text{diag}(1, \dots, 1, f, 0, \dots, 0)$, where $f \in R$.

PROOF. This follows from the fact that R is a simple domain. A proof of that can e.g. be found in [Zer06], Theorem 4.1. Therefore the generator of any non-zero two-sided ideal is 1. \square

REMARK 1.17. Recall that we consider throughout the whole thesis that the rational Weyl algebra has a field of characteristic zero as basefield. The corollary above is not true in general if the characteristic would not be zero.

EXAMPLE 1.18. Take again A from example 1.13. Then its nontrivial entry of the Jacobson normal form is (up to similarity) given by

$$\begin{aligned} &672x^{13}\partial^2 + 672x^{12}\partial^3 + 1568x^{13}\partial + 2968x^{12}\partial^2 + 56x^{11}\partial^3 + 4648x^{12}\partial \\ &- 1040x^{11}\partial^2 - 1208x^{10}\partial^3 + 112x^9\partial^4 + 1568x^{12} - 4004x^{11}\partial \\ &- 10988x^{10}\partial^2 - 3700x^9\partial^3 - 28x^8\partial^4 - 26232x^{10}\partial - 31624x^9\partial^2 \\ &- 9952x^8\partial^3 - 248x^7\partial^4 - 4984x^{10} - 69324x^9\partial - 61112x^8\partial^2 \\ &- 10564x^7\partial^3 - 632x^6\partial^4 - 14108x^9 - 119476x^8\partial - 63124x^7\partial^2 \\ &- 9508x^6\partial^3 - 1128x^5\partial^4 - 28164x^8 - 118614x^7\partial - 49298x^6\partial^2 \\ &- 6802x^5\partial^3 - 858x^4\partial^4 - 27572x^7 - 80524x^6\partial - 20604x^5\partial^2 - 852x^4\partial^3 \\ &- 392x^3\partial^4 - 14036x^6 - 19624x^5\partial + 3692x^4\partial^2 + 842x^3\partial^3 - 78x^2\partial^4 \\ &+ 7258x^5 + 8270x^4\partial + 2196x^3\partial^2 + 702x^2\partial^3 - 2x\partial^4 + 7630x^4 \\ &+ 1018x^3\partial + 564x^2\partial^2 + 144x\partial^3 + 388x^3 - 508x^2\partial - 136x\partial^2 + 2\partial^3 \\ &- 248x^2 - 424x\partial - 2\partial^2 - 142x - 6\partial - 2. \end{aligned}$$

With this example, one can see how ugly our entries can be compared to the Hermite normal form. For calculating this result, we made use of the computer algebra system

SINGULAR ([GLMS10]) and its library `jacobson.lib` developed by K. Schindelar and V. Levandovskyy ([LS11]).

As mentioned before, the output is just unique up to the weak notion of similarity. That means that there might be a more appealing Jacobson normal form of A , but there is definitely a more ugly one: Using the canonical approach of calculating a lot of gerds and glds to eliminate rows and columns lead to a nontrivial entry, that can fit in 15 pages of this thesis.

Over the past few years, a number of algorithms and implementations have been developed for computing the Jacobson normal form. The initial definition of the Jacobson form [Jac43] was essentially algorithmic, reducing the problem to computing diagonalizations of 2×2 matrices, which can be done directly using gerds and lclms. Unfortunately, this approach lacks not only efficiency in terms of ring operations, but also results in extreme coefficient growth.

Recent methods of [LS11] and [LS12] have developed an algorithm based on Gröbner basis theory. An implementation of it is available in the computer algebra system SINGULAR, which we used in the example above. A second approach by Robertz et al. implementing the algorithm described in [Coh85] can be found in the `Janet` library for MAPLE. Another approach is proposed by [Mid08] for differential polynomials, making use of a cyclic vector computation (for cyclic vectors, see [CK02]). This algorithm requires time polynomial in the system dimension and order, but coefficient growth is not accounted for. Finally, the dissertation of [Mid11] considers an FGLM-like (for details on FGLM see [FGLM93]) approach to converting a matrix of differential polynomials from the Popov to Jacobson form.

The problem with those approaches is that one cannot establish rigorous polynomial-time bounds on the cost of computing the Jacobson form in terms of the dimension, degree and coefficient bound on the input. We are therefore going to avoid Gröbner bases and cyclic vectors, because we do not have sufficiently strong statements about their size or complexity. Gröbner basis calculations were even proven to have double exponential complexity by Mayr and Meyer in 1982 ([MM82]). Nevertheless, the implementation in SINGULAR appeared to be very fast in the practical use. Furthermore, as we will see later, its output is nice in terms of the size of the nontrivial entry in the resulting Jacobson form. The approach discussed here does not outperform their approach in practice, yet we will obtain some complexity bounds.

Our approach will be an algorithm of Las Vegas type. We are going to define this term in the next chapter with some additional preliminary work. The main idea will be a random preconditioning of the given matrix by a unimodular matrix from the right, such that we can obtain the Jacobson normal form directly from the Hermite normal form.

2. Excursion to Vegas

“Las Vegas algorithms are not very well implemented in the system of politics. It produces failures, does not give a notice of it and certain parts never seem to terminate.”

For a short glance, let us go back to some old friends: Multivariate polynomials in $\mathbb{K}[x_1, \dots, x_n]$, $n \in \mathbb{N}$. We are interested in the probability that for a given polynomial $p \in \mathbb{K}[x_1, \dots, x_n]$ a randomly chosen point $[r_1 \ \dots \ r_n] \in \mathbb{K}^n$ is a zero of that polynomial. This was studied in the 80s by J.T. Schwarz and R. Zippel. They are the name givers of the famous Schwartz-Zippel-Lemma, which is given as follows (compare [Sch80]).

LEMMA 2.1 (Schwartz-Zippel). *Let $0 \neq p \in \mathbb{K}[x_1, \dots, x_n]$ of total degree $d \in \mathbb{N}$, where \mathbb{K} is a field. Let S be a finite subset of \mathbb{K} and let r_1, \dots, r_n be randomly selected from S . Then the probability of*

$$p(r_1, \dots, r_n) = 0$$

is less or equal than $\frac{d}{|S|}$.

This lemma has a lot of applications. Some of them are:

- i) Comparison of two polynomials
- ii) Primality testing
- iii) Calculating the Smith normal form of matrices over the polynomial ring $\mathbb{K}[x]$.

Ad i): For testing if two given polynomials $p_1, p_2 \in \mathbb{K}[x_1, \dots, x_n]$ are equal, one can just evaluate both in points chosen randomly. If the evaluation is equal for a certain amount of these points, one can say, that p_1 and p_2 are equal with high probability.

Ad ii): M. Agrawal and S. Biswas presented a technique in [AB99] for primality testing using the Schwartz-Zippel Lemma. It makes use of the fact that due to the Frobenius automorphism we have for all prime numbers n the following polynomial identity in $\mathbb{F}_n[x]$:

$$(1 + x)^n = 1 + x^n.$$

Therefore we use the Schwartz-Zippel Lemma for determining whether the polynomials $(1 + x)^n$ and $1 + x^n$ are equal in $\mathbb{F}_n[x]$ and get a result, that is valid with high probability.

Ad iii): A. Storjohann and G. Labahn developed in the paper [SL97] of 1997 an algorithm to compute the Smith normal form of a matrix over the polynomial ring $\mathbb{K}[x]$. In order to reduce the amount of expensive gcd computations, they utilized the following fact, that was first stated by Kaltofen, Krishnamoorthy and Saunders in [KKS87]: Given polynomials $f_1, \dots, f_n \in \mathbb{K}[x]$ and random elements $k_2, \dots, k_n \in \mathbb{K}$. Then we have

$$\gcd(f_1, \dots, f_n) = \gcd\left(f_1, \sum_{i=2}^n k_i f_i\right)$$

with high probability.

This fact is used for the computation of the Smith normal form of a matrix $A \in \mathbb{K}[x]^{n \times n}$. One takes two invertible matrices $U, V \in \mathbb{K}^{n \times n}$, whose entries are randomly chosen, and

computes the Smith normal form of UAV . The Smith normal form is invariant under this transformation. Thus the output will be the same. But, if we want to eliminate the first row and the first column, we have to calculate just one gcd with high probability. Then we proceed with the remaining rows and columns. With intelligent preconditioning we just have to compute n gcds at most (compared to n^2 gcd computations in the worst case for the naive approach). Of course, the techniques presented in the paper are a lot more sophisticated and they are fixing a certain way of preconditioning, but this is the basic idea.

The application iii) leads to a certain type of algorithms, namely the algorithms of Las Vegas type.

DEFINITION 2.2 (compare [MR10]). An algorithm of **Las Vegas type** is a randomized algorithm – i.e. it employs a degree of randomness as part of its logic – that has a chance of failing to produce a result. It either signals its failure or fails to terminate. But if an output is given, then it will be a correct result.

REMARK 2.3. Informally speaking, Las Vegas type algorithms are gambling with the input the user is providing, but not with the result. Self-explanatory, those algorithms are usually designed such that the failure occurs with very low probability and the non termination is avoided.

REMARK 2.4. The opposite class of Las Vegas type algorithms from the area of randomized algorithms are the so called **Monte-Carlo algorithms**. In contrast to Las Vegas type algorithms, Monte-Carlo algorithms have a chance of producing an incorrect result. Designers of those algorithms are usually trying to bound the error of the output, such that the results can be used in practice. Here, we are close to the point of entering the field of numerics.

3. On Divisibility

“Nothing is irreplaceable, a habit is not a need.” – Paulo Coelho

Now we come to the main idea behind our approach. Let us describe it with the following observation.

OBSERVATION 3.1. Take the element $\partial \in R$. Then clearly

$$\text{gcd}(\partial, \partial) = \partial.$$

But if we multiply x to ∂ from the right, we obtain

$$\text{gcd}(\partial, \partial x) = \text{gcd}(\partial, x\partial + 1) = 1.$$

One can see this directly because $-x \cdot \partial + 1 \cdot (x\partial + 1) = 1$.

This is pretty wild since x is a unit in R and we are used to the accustomed case (in commutative algebra) where a multiplication by a unit does not have any effect at all. This leads to the following lemma.

LEMMA 3.2. *Given $h \in R$, nontrivial in ∂ , there exists a $w \in \mathbb{K}[x]$ with $\deg_x(w) \leq \deg_\partial(h)$, such that*

$$\text{gcd}(h, hw) = 1.$$

PROOF. Without loss of generality assume h is normalized to be monic and has the form $\partial^n + \tilde{h}_{n-1}\partial^{n-1} + \dots + \tilde{h}_1\partial + \tilde{h}_0$.

Case 1: h is irreducible.

The only monic right divisor of h of positive degree is h itself. Thus, brought into normal form (i.e., with leading coefficient one), h and hw should be the same polynomial in order to obtain $\text{gcd}(h, hw) \neq 1$. We have

$$\text{lc}(h) = 1, \text{lc}(hw) = w, \text{tc}(h) = \tilde{h}_0,$$

and

$$\text{tc}(hw) = \tilde{h}_0w + \tilde{h}_1\delta(w) + \dots + \tilde{h}_n\delta^n(w),$$

where δ is the identity-derivation taken from the definition of the Weyl algebra and $\text{lc} : R \rightarrow \mathbb{K}(x)$ and $\text{tc} : R \rightarrow \mathbb{K}(x)$ extract the leading and tailing coefficients respectively. The choice of w , such that the tail coefficients are different, is always possible. If one normalizes both polynomials from the left and subtract them, then the result is a polynomial of strict lower degree in ∂ and not equal 0. This is due to the fact that the tail coefficient of hw after normalizing has the form

$$(3.1) \quad \tilde{h}_0 + \frac{\tilde{h}_1\delta(w) + \dots + \tilde{h}_n\delta^n(w)}{w},$$

and you can choose w such that the fraction above does not equal 0. Since h was assumed to be irreducible, we can reduce these polynomials further to 1 with a linear combination of h and hw (otherwise we would get a nontrivial gcd of two irreducible polynomials).

Case 2: $h = h_1 \cdots h_m$, with h_i irreducible for $1 \leq i \leq m$.

In this case the proof is complicated by non-commutativity. Multiplication with w will affect the rightmost factor. If there is just one possibility to factorize h we can again use the argument from case 1, and we are done.

If we have more than one possible factorization, things become interesting. We show that there are just finitely many monic w , such that $\text{gcd}(h, hw) \neq 1$. We will do this using a constructional argument of those elements.

Let $w_0 \in \mathbb{K}[x]$ be of degree at most $\deg_\partial(h)$, such that

$$\text{gcd}(h_m, h_mw_0) = 1.$$

This choice is possible due to Case 1. If we already have $\text{gcd}(h, hw_0) = 1$, then we are ready. Otherwise we know that h has another factorization of the form $\tilde{h}_1 \cdots \tilde{h}_{m-1}h_mw_0$. As by assumption $\text{gcd}(h_m, h_mw_0) = 1$, we have $\text{lcm}(h_m, h_mw_0) \mid_r h$ and $\text{lcm}(h_m, h_mw_0)$ has a degree in ∂ greater than h_m and of course therefore greater than h_mw_0 .

Thus we choose another $w_1 \in \mathbb{K}[x]$ that fulfills $\text{gcd}(h_m, h_mw_1) = 1$ and $\text{gcd}(h_mw_0, h_mw_0w_1) = 1$. If we have again that $\text{gcd}(h, hw_1) \neq 1$, then there is again a factorization of h that has h_mw_1 and $h_mw_0w_1$ as right factor. We again conclude that $\text{lcm}(h_m, h_mw_0, h_mw_0w_1) \mid_r h$, and it has again a degree bigger than $\text{lcm}(h_m, h_mw_0)$.

Proceeding like that, as the lcm is growing degree-wise and is a right divisor of h , after at most $\deg_\partial(h)$ steps we have found the only possible set of w_i , such that $\text{gcd}(h, hw_i) \neq 1$.

As we can choose w from an infinite set, one can always choose w having the nice property of h not having a nontrivial right divisor with hw . This completes the proof. \square

In the second case of the proof above it was not necessary that we were just looking at h , because we can consider any left multiple of h and get the same result.

COROLLARY 3.3. *For any $f, g \in R$, there exists a $w \in \mathbb{K}[x]$ with*

$$\deg_x(w) \leq \max\{\deg_\partial(f), \deg_\partial(g)\}$$

such that

$$\text{gcd}(fw, g) = 1.$$

PROPOSITION 3.4. *A randomly chosen $w \in \mathbb{K}[x]$ of suitable degree fulfills the property in Lemma 3.2 with high probability.*

PROOF. We use the notions of the proof of Lemma 3.2 and assume without loss of generality that h is irreducible, since otherwise we would just look at the rightmost factors as above.

A sufficient condition which has to hold for h and hw being the same polynomial after normalization, is that

$$\tilde{h}_0 + \frac{\tilde{h}_1\delta(w) + \dots + \tilde{h}_n\delta^n(w)}{w} = \tilde{h}_0,$$

which means

$$(3.2) \quad \tilde{h}_1\delta(w) + \dots + \tilde{h}_n\delta^n(w) = 0.$$

We can write w in the form

$$w = \sum_{i=0}^d w_i x^i$$

with $d \geq n$ and $w_i \in \mathbb{K}$. Thus our polynomial on the left hand side of (3.2) is nothing else but

$$\tilde{h}_1 \sum_{i=0}^{d-1} (i+1)w_{i+1}x^i + \dots + \tilde{h}_n \sum_{i=0}^{d-n} \left(\prod_{j=1}^n (i+j) \right) w_{i+n}x^i.$$

If we regard this as a polynomial in the ring $\mathbb{K}(x)[w_1, \dots, w_d]$, we can use the Schwartz-Zippel lemma and see, that for randomly chosen $w_i \in S$, where S is an adequately large enough subset of \mathbb{K} , the probability that the evaluation of the polynomial in the w_i equals zero is very small. \square

The proposition above and its proof might be easy to understand, but it lacks a concrete probability bound, that is needed in order to use it wisely. But using the generalized subresultants as presented in the section 1.2, we are able to provide a complexity bound.

LEMMA 3.5. *Let $f, g \in R$ have $\deg_\partial(f) = n$ and $\deg_\partial(g) = m$, without loss of generality $n \geq m$. Let $w \in \mathbb{K}[x]$ be chosen randomly of degree n , with coefficients chosen from a subset of \mathbb{K} of size at least nm . Then*

$$\text{Prob} \{ \text{gcd}(fw, g) = 1 \} \geq 1 - \frac{1}{n}.$$

PROOF. Assume the coefficients of $w = w_0 + w_1x + \dots + w_nx^n$ are independent indeterminates commuting with ∂ . Consider the condition that $\text{gcd}(fw, g) = 1$. We can construct the subresultants $\text{sres}_0(fw, g), \dots, \text{sres}_n(fw, g)$ as stated in section 1.2, where determinants are calculated in the coefficients of fw and g over $\mathbb{K}(x)[w_1, \dots, w_n]$. Then $D := \text{sres}_0(fw, g)$ is nonzero if and only if $\text{gcd}(fw, g) = 1$. By Corollary 3.3 we know D is not identically zero for at least one w . Let us have a closer look at $\text{sres}_0(fw, g)$:

$$\text{sres}_0(fw, g) = |\partial^{m-1}fw, \dots, \partial fw, fw, \partial^{n-1}g, \dots, \partial g, g|$$

It is easily derived from the Leibniz formula for the determinant that the total degree of D in the coefficients of w is less or equal to m . The probability stated then follows immediately from the Schwarz-Zippel lemma (Lemma 2.1). \square

As mentioned before, we want to use random preconditioning of a given matrix in order to obtain the Jacobson form directly from the Hermite form.

We now use our results to construct a generic preconditioning matrix $Q \in R^{2 \times 2}$ for a matrix $A \in R^{n \times n}$. First consider the case of a 2×2 matrix $A \in R^{2 \times 2}$ – we will expand to the $n \times n$ case later –, with Hermite form

$$H := \begin{pmatrix} f & g \\ 0 & h \end{pmatrix} = UA$$

for some unimodular $U \in R^{2 \times 2}$. We then precondition A by multiplying it with

$$Q := \begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}$$

from the right, where $w \in \mathbb{K}[x]$ is chosen randomly of degree

$$\max\{\deg_{\partial}(f), \deg_{\partial}(g), \deg_{\partial}(h)\}$$

and we obtain

$$UAQ = \begin{pmatrix} f + gw & g \\ hw & h \end{pmatrix}.$$

Our goal is to have the Hermite form of AQ have a 1 in the $(1, 1)$ position. This is achieved exactly when $\text{gcd}(f + gw, hw) = 1$. The following lemma will thus be useful.

LEMMA 3.6. *Given $f, g, h \in R$. Then there exists a $w \in \mathbb{K}[x]$ with*

$$\deg(w) \leq \max\{\deg_{\partial}(f), \deg_{\partial}(g), \deg_{\partial}(h)\}$$

such that

$$\text{gcd}(f + gw, hw) = 1.$$

PROOF. We consider two different cases.

Case 1: $\text{gcd}(g, h) = 1$. This implies $\text{gcd}(gw, hw) = 1$ for all possible w . Then there exist $e, l \in R$ such that $egw + lhw = 1$. Therefore – because we are aiming to obtain 1 as the gcd – we would proceed by computing the gcd of $ef + 1$ and hw . Lemma 3.2 shows the existence of appropriate w , such that $\text{gcd}(ef + 1, hw) = 1$.

Case 2: $\text{gcd}(g, h) \neq 1$. Without loss of generality, let g be the gcd of h and g (using the euclidean algorithm we can transform $\text{gcd}(f + gw, hw)$ into such a system, and f will just get an additional left factor). Since we can choose w , such that $\text{gcd}(f, hw) = 1$, we have $e, l \in R$, such that $ef + lhw = 1$. This means that we just have to compute the gcd

of hw and $1 + egw$. Let \tilde{h} be such that $\tilde{h}g = h$. If we choose the left factors e_2, l_2 , such that $e_2egw + l_2\tilde{h}gw = gw$, we know that h and e_2 have no common right divisor. Our gcd problem is equivalent to $\text{gcd}(e_2 + gw, \tilde{h}gw)$, which can be further transformed to $\text{gcd}(\tilde{h}e_2, \tilde{h}gw)$ (since we have $\tilde{h}(e_2 + gw) - \tilde{h}gw = \tilde{h}e_2$). As we can choose w from a large set of polynomials, we can adjust our choice of w to fulfill the conditions $\text{gcd}(f, hw) = 1$ and $\text{gcd}(\tilde{h}e_2, \tilde{h}gw) = 1$. This completes the proof. \square

A similar subresultant argument to Lemma 3.5 now demonstrates that for a random choice of w we obtain our co-primality condition. As the proof is very similar to that of 3.5, we leave it.

LEMMA 3.7. *Given $f, g, h \in R$, with*

$$d := \max\{\deg_{\partial}(f), \deg_{\partial}(g), \deg_{\partial}(h)\}.$$

Let $w \in R$ have degree d , and suppose its coefficients are chosen from a subset of \mathbb{K} of size at least d^2 . Then

$$\text{Prob}\{\text{gcd}(f + gw, hw) = 1\} \geq 1 - \frac{1}{d}.$$

4. From Hermite to Jacobson

“Therefore by their fruits you shall know them.” – Jesus in Matthew 7:20, Bible

Our final results in the previous chapter imply that for *any* matrix $A \in R^{2 \times 2}$ and a randomly selected $w \in \mathbb{K}[x]$ of appropriate degree we obtain with high probability

$$A \begin{bmatrix} 1 & 0 \\ w & 1 \end{bmatrix} = U^{-1} \begin{bmatrix} 1 & * \\ 0 & h \end{bmatrix} = U^{-1} \begin{bmatrix} 1 & 0 \\ 0 & h \end{bmatrix} V,$$

where $h \in R$ and $U, V \in R^{2 \times 2}$ are unimodular matrices. Hence A has as Jacobson normal form $\text{diag}(1, h)$. This is accomplished with one Hermite form computation on a matrix of the same degree in ∂ , and not too much higher degree in x than that of A .

REMARK 4.1. Here is an interesting extra result that we obtain for our resulting Hermite form: Since we can find a $w \in \mathbb{K}[x] \setminus \{0\}$, such that $\text{gcd}(f + gw, hw) = 1$, there exist e, l, k, m , such that

$$(4.1) \quad \begin{bmatrix} e & l \\ k & m \end{bmatrix} \begin{bmatrix} f + gw & g \\ hw & h \end{bmatrix} = \begin{bmatrix} 1 & eg + lh \\ 0 & kg + mh \end{bmatrix}.$$

Now, we know, that the following equalities do hold:

$$\begin{aligned} ef + egw + lhw &= 1 \\ \iff egw + lhw &= 1 - ef \\ \iff eg + lh &= w^{-1} - efw^{-1}, \end{aligned}$$

and similarly we get

$$\begin{aligned} kf + kgw + mhw &= 0 \\ \iff kgw + mhw &= -kf \\ \iff kg + mh &= -kfw^{-1}. \end{aligned}$$

This means that on the right hand side of our equation (4.1) we have

$$\begin{bmatrix} 1 & w^{-1} - efw^{-1} \\ 0 & -kfw^{-1} \end{bmatrix}.$$

Therefore, for our next computation (i.e., if we just considered the 2×2 submatrix with this and computed the new Hermite form), we would deal with that same f as right factor multiplied by a unit from the right in the upper left corner of the next 2×2 submatrix and will perform our computations there.

We now generalize this technique to $n \times n$ matrices over R .

THEOREM 4.2. *Let $A \in R^{n \times n}$ have full row rank. Let Q be a lower triangular, banded, unimodular matrix of the form*

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ w_1 & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & w_{n-1} & 1 \end{bmatrix} \in R^{n \times n},$$

where $w_i \in \mathbb{K}[x]$ for $i \in \{1, \dots, n-1\}$, $\deg(w_i) = i \cdot n \cdot d$ and d is the maximum degree in ∂ of the entries in A . Then with high probability the diagonal of the Hermite form of $B = AQ$ is $\text{diag}(1, 1, \dots, 1, m)$, where $m \in R$.

PROOF. Let H be the Hermite form of A and have the form

$$\begin{bmatrix} f_1 & h_1 & * & \dots & * \\ 0 & f_2 & h_2 & \dots & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & h_{n-1} \\ 0 & \dots & 0 & 0 & f_n \end{bmatrix}.$$

By [GK12], Theorem 3.6, we know that the sum of the degrees of the diagonal entries of the Hermite form of A equals $n \cdot d$. Thus we can regard nd as an upper bound for the degrees of the f_i . If we now multiply the matrix

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ w_1 & 1 & 0 & \dots & 0 \\ 0_{n-2 \times 1} & 0_{n-2 \times 1} & I_{n-2} & & \end{bmatrix}$$

from the right, we obtain the following in the upper left 2×2 submatrix:

$$\begin{bmatrix} f_1 + h_1 w_1 & h_1 \\ f_2 w_1 & f_2 \end{bmatrix}.$$

As we have seen in the remark above, after calculation of the Hermite form of this resulting matrix, we get with high probability

$$\begin{bmatrix} 1 & * & * & \dots & * \\ 0 & kf_1w_1^{-1} & * & \dots & * \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & h_{n-1} \\ 0 & \dots & 0 & 0 & f_n \end{bmatrix}.$$

The entry $kf_1w_1^{-1}$ has degree at most $2 \cdot n \cdot d$, where we see, why we have chosen the degree $2 \cdot n \cdot d$ for w_2 . After $n - 1$ such steps we obtain a Hermite form with 1s on the diagonal, and an entry in R . \square

This leads us to the following simple algorithm to compute the Jacobson form by just calculating the Hermite normal form after preconditioning.

Algorithm 4 *JacobsonViaHermite*: Compute the Jacobson normal form of a matrix over the differential polynomials

Input: $A \in R^{n \times n}$, $n \in \mathbb{N}$.

Output: The Jacobson normal form of A .

Preconditions:

- Existence of an algorithm HERMITE to calculate the Hermite normal form of a given matrix over R .
- Existence of an algorithm RANDPOLY which computes a random polynomial of specified degree with coefficients chosen from a specified set.

1: $d \leftarrow \max\{\deg(A_{i,j}) \mid i, j \in \{1, \dots, n\}\}$

2: **for** i from 1 to $n - 1$ **do**

3: $w_i \leftarrow \text{RANDPOLY}(\text{degree} = i \cdot n \cdot d)$

4: **end for**

5: Construct the matrix W , such that

$$W_{ij} \leftarrow \begin{cases} 1 & \text{if } i = j \\ w_i & \text{if } i = j + 1 \\ 0 & \text{otherwise} \end{cases}$$

6: $\text{result} \leftarrow \text{HERMITE}(A \cdot W)$

7: **if** $\text{result}_{ii} \neq 1$ for any $i \in \underline{n - 1}$ **then**

8: FAIL {With low probability this happens}

9: **end if**

10: Eliminate the off diagonal entries in result by simple column operations

11: **return** result

4.1. Experimental Implementation and Results. We have written an experimental implementation in MAPLE as a proof of concept of our algorithm.

Since there are no other implementations of the calculation of the Hermite form available for Ore rings, we used the standard way of calculating the Hermite form, i.e. by

repeated gcd computations. Since the Hermite form of a matrix is unique, the choice of algorithm is just a matter of calculation speed.

One problem with the preconditioning approach is that the diagonal entries become “ugly” (recall that they are only unique up to the weak notion of similarity). We illustrate this with an example as follows.

EXAMPLE 4.3. Consider the matrix

$$A := \begin{bmatrix} 1 + x\partial & x^2 + x\partial \\ x + (x + 1)\partial & 5 + 10\partial \end{bmatrix}.$$

Its Jacobson form, calculated by SINGULAR, has as its nontrivial entry:

$$(45x - 10 - 11x^2 - x^4 + 2x^5) + (2x^5 + 3x^4 - 12x^3 + 10x + 2x^2)\partial + (2x^4 - 19x^3 + 9x^2)\partial^2.$$

Calculating the Jacobson form with the approach of calculating a lot of gcds or gcds respectively results in the polynomial:

$$(-3x^3 + x^5 - 4x^2 + 3x + 10) + (-8x^3 + x^2 + x^5 + x^4 + 13x + 19)\partial + (-10x^3 + 8x^2 + x^4 + 9x)\partial^2.$$

If we precondition the matrix in the described way, the output of SINGULAR stays the same, but the output of the straightforward approach is the polynomial:

$$\begin{aligned} & 88360x^9 - 384554x^8 + 243285x^7 + 1104036x^6 - 4428356x^5 + 2474570x^4 + 3533537x^3 \\ & \quad - 3915039x^2 + 1431017x - 150930 \\ & + (88360x^9 - 31114x^8 - 948071x^7 + 5093247x^6 - 7538458x^5 + 5740077x^4 - 1935190x^3 \\ & \quad - 20353x^2 + 154797x + 10621)\partial \\ & + (-739659x^3 + 137249x^2 + 5031x + 1769774x^4 - 2553232 + x^5 + 2133343x^6 \\ & \quad - 1003074x^7 + 88360x^8)\partial^2. \end{aligned}$$

The calculation time was as expected similar to just calculating a Hermite form. Both answers are “correct”, but the Gröbner-based approach has the effect of reducing coefficient size and degree. An important future task could be to find a normal form for a polynomial in this notion of similarity. This normal form should have as simple coefficients as possible.

The demonstration here is simply that the algorithm works, not that we would beat previous heuristic algorithms in practice. The primary goal of this work is to demonstrate a polynomial-time algorithm, which we hope will ultimately lead to faster methods for computing and a better understanding of the Jacobson form.

4.2. Degree Bounds and Complexity. There are no clear bounds on complexity given in nowadays algorithms for computing the Jacobson normal form.

Viktor Levandovskyy’s and Kristina Schindelar’s algorithm does use Gröbner Bases, and one knows that in the worst case those algorithms have double exponential complexity.

Our approach is of Las Vegas Type and its complexity just relies on the complexity given by the algorithm used for calculating the Hermite form. M. Giesbrecht and M.S. Kim developed an algorithm for computing the Hermite form and in [GK09]. There was also a complexity theorem given.

THEOREM 4.4 (M. Giesbrecht, M.S. Kim, Theorem. 5.3). *Let $A \in R^{n \times n}$ with $\deg_{\partial}(A_{ij}) \leq d$ and $\deg_x(A_{ij}) \leq e$ for $1 \leq i, j \leq n$. Then we can compute the Hermite normal form $H \in R^{n \times n}$ of A , and a unimodular $U \in R^{n \times n}$ such that $UA = H$, with $O((n^{10}d^3 + n^7d^2e) \log(nd))$ operations in \mathbb{K} .*

The cost of the algorithm described for the Jacobson normal form is just the cost of a single preconditioning step (a matrix multiplication), plus the cost of computing a Hermite form (for which we use the algorithm of [GK09]). The growth in the degree of the input matrix after the precondition is an additive factor of $O(n^2d)$, which is largely dominated by the cost of computing the Hermite form. We thus obtain the following theorem.

THEOREM 4.5. *Let $A \in R^{n \times n}$ have full row rank, with $\deg_{\partial}(A_{ij}) \leq d$ for $1 \leq i, j \leq n$, and $\deg_x(A_{ij}) \leq e$.*

(a) *We can compute the Jacobson form J of A , and unimodular matrices U, V such that $J = UAV$, with an expected number of $O(n^9d^3e)$ operations in \mathbb{K} . The algorithm is probabilistic of the Las Vegas type, and always returns the correct solution.*

(b) *If $J = \text{diag}(1, \dots, 1, s_n)$, then*

$$\deg_{\partial}(s_n) \leq nd, \text{ and } \deg_{\partial}(U_{ij}), \deg_{\partial}(V_{ij}) \leq nd.$$

(c) *$\deg_x H_{ij} \in O(n^2de)$ and $\deg_x(U_{ij}) \in O(n^2de)$ for $1 \leq i, j \leq n$.*

PROOF. Part (a) follows directly from the algorithm and the preceding analysis. Part (b) and (c) follow from the degree bounds over on the Hermite form over Ore polynomial rings in [GK09, GK12]. \square

Of course a faster algorithm for computing the Hermite form would directly yield a faster algorithm for computing the Jacobson form of an input matrix.

Given the complexity measure of the calculation steps for computing the Hermite form in Theorem 4.4, we see that in this case we can discard the last n^2 , and the complexity to compute a random polynomial of degree n^2d is also possible in $O(n^2d)$. Therefore, using this specific algorithm for computing the Hermite normal form, our algorithm has the same complexity as the calculation of the Hermite form.

5. Application to other Ore Domains

“Not the mama!” – Baby Sinclair, from the 80s TV-show “The Dinosaurs”.

For the last couple of sections, we assumed R to be the rational first Weyl algebra. It made some discussions easier, since it is a simple domain and the Jacobson form can be associated with the one nontrivial entry (as seen in Corollary 1.16).

But is it possible to state also some structure properties of a Jacobson form over other Ore domains? Fortunately, we can answer this question with yes. Let us start with the rational shift algebra, where we made our first observations.

5.1. Jacobson Normal Forms over the Rational Shift Algebra. For this subsection we denote by R the first rational shift algebra.

OBSERVATION 5.1. Let p be a polynomial in the rational first shift algebra. It has the form

$$p := \sum_{i=0}^n p_i S^i, \quad p_i \in \mathbb{K}(x).$$

Then, by two sided linear combinations with coefficients in $\mathbb{K}(x)$, we can transform p to the polynomial S^k , where $k := \min\{i = 0, \dots, n \mid p_i \neq 0\}$.

The transformation steps are very simple. Take the element $x \in R$. Then apply the following linear combination to p :

$$\hat{p} := (x + n)p - px.$$

This transformation step is chosen in the way that \hat{p} has a strictly lower degree in S than p . The terms of lower degree do not vanish after the application of this step, since we will have as coefficient of S^k for $k \in \{0, \dots, n-1\}$

$$\begin{aligned} & (x+n)p_k S^k - (x+k)p_k S^k \\ &= (x+n-x-k)p_k S^k \\ &= (n-k)p_k S^k \neq 0. \end{aligned}$$

Thus we obtain the desired form after a finite amount of steps.

EXAMPLE 5.2. Take the polynomial

$$p := S^2 + x^{-1}S + 1.$$

Then

$$\begin{aligned} & (x+2)p - px \\ &= (x+2)S^2 + \frac{x+2}{x}S + (x+2) - (x+2)S^2 - \frac{x+1}{x}S - x \\ &= \frac{x+2-x-1}{x}S + (x+2-x) \\ &= \frac{1}{x}S + 2, \end{aligned}$$

and the second transformation step results in

$$\begin{aligned} & (x+1)\frac{1}{x}S + 2(x+1) - \frac{1}{x}Sx - 2x \\ &= 2x + 2 - 2x \\ &= 2. \end{aligned}$$

Therefore the two-sided ideal generated by p is actually R itself.

COROLLARY 5.3. *All nontrivial two sided ideals in the rational first shift algebra are generated by a positive power of S .*

PROOF. The rational first shift algebra is a left principal ideal domain. Therefore we can transform every ideal at first in the form where we just have one generator. After that we apply the transformation steps as described in the observation above and obtain the desired result. \square

COROLLARY 5.4. *Let $a, b \in R$, and b be given by $b := \sum_{i=0}^n b_i S^i$, $b_i \in \mathbb{K}(x)$. Then a is a total divisor of b if and only if $a = \hat{a} S^k$, where $\hat{a} \in \mathbb{K}(x)$ and $k \leq \min\{i = 0, \dots, n | b_i \neq 0\}$.*

PROOF. Let us recall the definition of total divisibility. It means, that there exists a two-sided ideal I , such that $bR \subseteq I \subseteq aR$. That a is a total divisor of b if it has the form as given in the statement is trivial. The more interesting part is the other direction. As we know from Corollary 5.3 we have $I = \langle S^{\hat{k}} \rangle$ and $\hat{k} \leq \min\{i = 0, \dots, n | b_i \neq 0\}$ in order to obtain $bR \subseteq I$. Since we need $I \subseteq aR$, we see that $S^{\hat{k}} \in aR$. There is a grading on R defined by the weights 0 for x and 1 for S and we see now that a has to be homogenous in order to generate $S^{\hat{k}}$. Thus it has the desired form. \square

Now, as a byproduct of the results above, we obtain the strong Jacobson form for matrices over the rational shift algebra.

THEOREM 5.5. *Let $A \in R^{n \times n}$. Then there exist unimodular matrices $U, V \in R^{n \times n}$ such that*

$$J = UAV = \text{diag}(1, \dots, 1, S, \dots, S, \dots, S^k, \dots, S^k, fS^l, 0, \dots, 0),$$

where $f \in R$ and $l \geq k \in \mathbb{N}_0$.

PROOF. As the diagonal entries of the Jacobson normal form (we assume the diagonal entries to be normalized) are total divisors in an ascending order, all entries have to be a power of S according to Corollary 5.4, except for the last entry before the 0-sequence starts. The ascending degree of S on the diagonal results also from the total divisibility criterion. \square

The question that is now arising: Can we use the same techniques to calculate the Jacobson form that we used for the rational first Weyl algebra also for the rational first shift algebra? If we go back, our whole discussion based essentially on Lemma 3.2 and on the fact, that we basically always wanted to achieve the grcd to be 1.

Therefore, let us state Lemma 3.2 for the shift case.

LEMMA 5.6. *Given $h := \sum_{i=0}^n h_i S^i \in R$, nontrivial in S . Then there exists a $w \in \mathbb{K}[x]$ with $\deg_x(w) \leq \deg_S(h)$ such that*

$$\text{grcd}(h, hw) = S^k,$$

where $k := \min\{i = 0, \dots, n | h_i \neq 0\}$.

PROOF. Without loss of generality, we assume $h_0 \neq 0$, since we can always extract S and swap it bijectively with an element in $\mathbb{K}(x)$. Therefore, our goal will be the grcd 1.

Case 1: h is irreducible. Then we get from the reduction step

$$(x + n) \cdot h - hx$$

an element of strictly smaller degree, that is not equal to zero. Due to the irreducibility of h , further reduction steps will result in 1. So therefore just put $w = x$ in this case.

Case 2: h is reducible. Then h can be written as $\tilde{h}_1 \cdots \tilde{h}_n$. With analogue arguments as in Lemma 3.2, there are just finitely many monic w such that right multiplication with a unit results in another right factor. Therefore we have a lot possibilities for w such that

any rightmost factor is not a rightmost factor any more after the multiplication by w from the right. \square

REMARK 5.7. The main difference between the shift case and the Weyl case lies in the choice of the preconditioning element for the irreducible case. While the element had to suffice a certain degree in the Weyl algebra, in the shift case the element x is already suitable.

We could start over again here and build up the argumentation to get an analogous algorithm for matrices over the shift algebra as we already have for the Weyl algebra. The only interesting part will be that the choice of the precondition matrix might be more easy, because we do not have to choose our preconditioning elements to be of such a high degree. But we will dismiss this part here and leave it as practical exercise for the implementation to come.

In our experimental implementation mentioned before the algebra was also part of the input. Therefore we could also try the concept on matrices over the shift algebra, although the precondition matrix might be too big degree-wise for the shift case. Some empirical attempts were giving us the expected results. We put the output of the algorithm for one of them into the appendix.

What we want to deal with now is for which algebras we can use similar arguments as in the shift case to get similar structure properties for the Jacobson normal form.

5.2. What the Shift Case Has Shown Us. Let us go back to Observation 5.1 and look at it from a more general point of view. For this subsection, $R := \mathbb{K}(x)[\partial; \sigma]$, where σ is an automorphism on $\mathbb{K}(x)$. What was needed, such that the reduction steps did work as they did?

One of the things having a chance to fail is that after a reduction also lower order terms do vanish. Therefore we depend on the existence of an element $w \in K(x)$, such that for all $i < k \leq n$ the condition

$$\sigma^k(w) - \sigma^i(w) \neq 0$$

does hold. In order to have more freedom for the choice of this element w , we are choosing it dependent on the degree of the polynomial p .

THEOREM 5.8. *Let σ be an automorphism, such that for all $n \in \mathbb{N}$ and all $i < k \leq n$ there exists an element $w \in R$, such that*

$$\sigma^k(w) - \sigma^i(w) \neq 0.$$

Then the two sided ideals of R are either generated by a positive power of ∂ or they are trivial.

PROOF. Following [BGTVO3], Proposition 4.13, we know that R is a left principal ideal domain. Therefore we can assume that our two-sided ideal can be generated by one element after some left sided reduction. Let this element be denoted by $p := \sum_{i=0}^n p_i \partial^i$, $p_i \in \mathbb{K}(x)$. Let further $k := \min\{i = 1, \dots, n \mid p_i \neq 0\}$. Now we start the two sided reduction steps. Take the element w , which exists and fulfills the properties for n stated in the theorem. Then

$$\sigma^n(w)p - pw$$

is constructed in the way, that it has a strictly lower degree in ∂ than the original element. The coefficients of the terms with lower degree $i < n$ now have the form

$$\underbrace{(\sigma^n(w) - \sigma^i(w))}_{\neq 0} p_i \partial^i \neq 0.$$

After at most $n-k$ more steps we reach the last element ∂^k , which proves the statement. \square

COROLLARY 5.9. *Let the same assumptions on σ be true here as in Theorem 5.8. Let $a, b \in R$, and b be given by $b := \sum_{i=0}^n b_i \partial^i, b_i \in \mathbb{K}(x)$. Then a is a total divisor of b if and only if $a = \hat{a} \partial^k$, where $\hat{a} \in \mathbb{K}(x)$ and $k \leq \min\{i = 0, \dots, n \mid b_i \neq 0\}$.*

PROOF. The proof of this statement is analogue to the proof of the equivalent in the special case of the shift algebra (Corollary 5.4). An algebra like that of course also possesses a grading using the $[0, 1]$ weight vector. \square

Thus, if σ has the property as stated above, we also have the strong Jacobson normal form for that kind of algebra as we had it for the shift algebra.

THEOREM 5.10. *Let $A \in R^{n \times n}$, and σ has the properties as stated in Theorem 5.8. Then there exist unimodular matrices $U, V \in R^{n \times n}$ such that*

$$J = UAV = \text{diag}(1, \dots, 1, \partial, \dots, \partial, \dots, \partial^k, \dots, \partial^k, f \partial^l, 0, \dots, 0),$$

where $f \in R$ and $l \geq k \in \mathbb{N}_0$.

Of course, there are various algebras with that property. One famous example – besides the shift algebra of course – is the ring of quantum polynomials, where the parameter q is either an element transcendent over \mathbb{K} , or one uses an element $q \in \mathbb{K}$ that has infinite order in the multiplicative group of \mathbb{K} .

Let us state a counterexample for an algebra, where σ does not have the useful property.

EXAMPLE 5.11. Let $R := \mathbb{K}(x)[\partial; \sigma]$, where

$$\sigma\left(\sum_{i=0}^n a_i x^i\right) = \sum_{i=0}^n a_i (-x)^i, a_i \in \mathbb{K}.$$

Then σ is clearly an automorphism as an affine transformation of x .

Let p be given by

$$p := \partial^2 + \partial + 1.$$

If we now perform the step

$$\sigma^2(x)p - px,$$

we obtain $2x\partial$. We still have a generator that is a power of ∂ , but the condition on its degree does not hold any longer. This observation does hold for any element $w \in \mathbb{K}[x]$ that we choose for that step, that has at least one term that has an odd degree in x . If all degrees are even, then $pw = wp$, and we cannot reduce further. But the two sided ideal generated by p is actually R itself. One can find that out using SINGULAR:

```
> ring R = 0, (x,d), dp;
> def r = nc_algebra(-1,0);
> setring(r);
> poly p = d^2+d+1;
```



```
> twostd(ideal(p));  
_[1]=x  
_[2]=d2+d+1
```

Therefore, as a conclusion we can see, that it is possible to use those techniques for calculating the Jacobson form not only for the Weyl algebra, but we can generalize them to other algebras, too. The preconditioning element might differ from algebra to algebra and that should be examined as a future work. And, as we have seen in this section, also other algebras than the Weyl algebra do have further structure to their Jacobson form. On this topic there should also be made some investigations in the future.

Conclusion and Future Work

Let us draw a conclusion what we saw in this thesis and where we can see tasks for the future.

In the first chapter, there were two main topics. The first one is the new approach for factoring inhomogeneous polynomials in the first Weyl algebra.

Even though it seem to return good results for all the examples we feed to it, there is still some work to do; mainly some proofs why our resulting set is always finite respectively how we can derive our answer from it if the resulting set is not finite. Furthermore, we can also think about the question how to simplify the equations in advance, so that the calculation of the result becomes more easy.

Another bottleneck is still finding all valid combinations of the highest and the lowest homogeneous summand of the polynomial-to-factor. This problem occurs when they have a lot of different homogeneous factorizations. Maybe some more heuristics would result in a tremendous speedup.

One can also think about using those techniques for factoring inhomogeneous polynomials in the first q -Weyl algebra, which was a combinatorial explosion using the old way of factoring.

The second main topic in the first chapter was the one about localizations in noncommutative rings. We provided an overview on what we have to take care of and the main result was the generalization of the Lemma of Gauss. This tells us, that it suffices to deal with the factorization in the polynomial case, if one is just interested in classes of different factorizations. If one is also interested in the maybe infinite solution space, we recommend to use the techniques of Tsarev on the factorization we get after factoring in the polynomial case. For the future we also have to think about how we can use these facts for current problems involving factorizations of differential operators, as for example the approach of Hrushovski to determine the differential Galois group of a given operator.

For the second chapter I am deeply apologizing at this point; it was a huge run through a lot of cases trying to answer a question that is not rigorously stated – namely the one why the coefficients of two similar polynomials have such exploding coefficient behavior in the underlying field \mathbb{K} .

But it was a fruitful accounting, as we gained new necessary conditions for polynomials being similar or not in addition to having clues for the coefficient growth – namely shifts in the zero homogeneous parts. Furthermore we discovered some structural properties our multiples $a, b \in A_1$ must have in $af = gb$. And we discussed how the concept of being homogeneous relates to the similarity question. The result was that it is possible for an inhomogeneous polynomial to be similar to a homogeneous one. An interesting task for the future would be to characterize families of inhomogeneous polynomials that are similar to homogeneous ones. The motivation for that comes from the fact that homogeneous

polynomials are very nice to handle and by now we have a lot of intuition dealing with them. Additionally, using the new techniques, one can think about developing an algorithm to decide whether two polynomials are similar – even though there are a lot of existing ones, but just for the interest.

Another point on the TODO-list could be to examine similarity also for other graded noncommutative algebras and see, what properties we do find there.

Moreover, now that we have seen that the coefficient growth comes et al. from shifts of zero homogeneous factors of two similar polynomials, we can ask the question about the existence of a normal form of an element in the polynomial first Weyl algebra with respect to similarity, i.e. if we can simplify a given element to a certain extend. This would be very useful for our algorithm that computes the Jacobson normal form. Here, we can directly draw the connection to the last chapter.

The last chapter contributed a polynomial time algorithm of Las Vegas type for computing the Jacobson normal form. We generalized the techniques known for the Smith normal form in the commutative case to the noncommutative case. The reader got an overview on how linear algebra over Ore domains does work and what problems we are facing there, too. The conclusion is that in practice it does not beat current implementations like the one in SINGULAR, but it is the first one that calculates the Jacobson normal form of a given matrix provable in polynomial time using random parameters. But the coefficient growth does not make it applicable yet.

Another contribution in the last chapter was the strong Jacobson form for matrices over the rational first shift algebra and the generalization to a class of algebras that have the same property. We have seen that the root for it comes from the notion of total divisibility. One can examine this concept also for other algebras to find further structural properties there.

For the TODO-list in this chapter we have also one more point. The preconditioning in the Jacobson algorithm right now uses polynomials that are fairly huge. For the future it would be interesting to have some heuristics when we can choose them to be of smaller degree.

Summa summarum: There is a lot of work to do and some intuition to be gained about how we can use and extend the results here for dealing with other problems related either to factorization, similarity or matrix normal forms. Or to answer if it is worth the effort. One never knows. We can just try and either succeed or fail. On that note let us conclude this thesis.

Bibliography

- [AB99] M. Agrawal and S. Biswas, *Primality and identity testing via chinese remaindering*, 40th annual symposium on foundations of computer science. Proceedings of the symposium (FOCS'99) (1999), no. 40, 202–208.
- [BGTV03] J. Bueso, J. Gómez-Torrecillas, and A. Verschoren, *Algorithmic methods in non-commutative algebra. Applications to quantum groups.*, Dordrecht: Kluwer Academic Publishers, 2003 (English).
- [Buc97] B. Buchberger, *Introduction to Groebner bases.*, Berlin: Springer, 1997 (English).
- [Cha91] M. Chardin, *Differential resultants and subresultants.*, Budach, Lothar (ed.), Fundamentals of computation theory. 8th international conference, FCT '91, Gosen, Germany, September 9-13, 1991. Proceedings, Berlin etc.: Springer-Verlag, 1991 (English).
- [CK02] R. C. Churchill and J. J. Kovacic, *Cyclic vectors.*, Singapore: World Scientific, 2002 (English).
- [Coh85] P.M. Cohn, *Free rings and their relations. 2nd ed.*, , 1985 (English).
- [Die43] J. Dieudonné, *Les déterminants sur un corps non commutatif.*, Bull. Soc. Math. Fr. **71** (1943), 27–45 (French).
- [FGLM93] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering.*, J. Symb. Comput. **16** (1993), no. 4, 329–344 (English).
- [GK09] M. Giesbrecht and M. S. Kim, *On computing the Hermite form of a matrix of differential polynomials.*, Berlin: Springer, 2009 (English).
- [GK12] M. Giesbrecht and M.S. Kim, *On computing the Hermite form of a matrix of differential polynomials*, Submitted Publication. ArXiv: 0906.4121. (2012).
- [GLMS10] G.-M. Greuel, V. Levandovskyy, A. Motsak, and H. Schönemann, PLURAL. A SINGULAR 3.1 Subsystem for Computations with Non-commutative Polynomial Algebras. Centre for Computer Algebra, TU Kaiserslautern, 2010.
- [GP07] G.-M. Greuel and G. Pfister, *A Singular introduction to commutative algebra. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann. 2nd extended ed.*, Berlin: Springer, 2007 (English).
- [GR91] I.M. Gel'fand and V.S. Retakh, *Determinants of matrices over noncommutative rings.*, Funct. Anal. Appl. **25** (1991), no. 2, 91–102 (English).
- [Hei10] A. Heinle, *Factorization of polynomials in a class of noncommutative algebras*, Bachelor Thesis at RWTH Aachen University, April 2010.
- [Her08] Ch. Hermite, *Oeuvres de Charles Hermite publiées sous les auspices de l'Académie des Sciences par Émile Picard, Membre de l'Institut. Tome II.*, , 1908 (French).
- [Hru02] E. Hrushovski, *Computing the Galois group of a linear differential equation.*, Warsaw: Polish Academy of Sciences, Institute of Mathematics, 2002 (English).
- [Jac43] N. Jacobson, *The theory of Rings.*, 1943 (English).
- [KC02] Victor Kac and Pokman Cheung, *Quantum calculus.*, New York, NY: Springer, 2002 (English).
- [KKS87] E. Kaltofen, M. S. Krishnamoorthy, and B. D. Saunders, *Fast parallel computation of Hermite and Smith forms of polynomial matrices.*, SIAM J. Algebraic Discrete Methods **8** (1987), 683–690 (English).
- [Koe98] W. Koepf, *Hypergeometric summation. An algorithmic approach to summation and special function identities.*, Wiesbaden: Vieweg, 1998 (English).

- [Lev05] V. Levandovskyy, *Non-commutative computer algebra for polynomial algebras: Gröbner bases, applications and implementation*, Ph.D. thesis, Technische Universität Kaiserslautern, <https://kluedo.ub.uni-kl.de/frontdoor/index/index/docId/1670>, 2005.
- [Li98] Z. Li, *A subresultant theory for Ore polynomials with applications.*, Proceedings of the 1998 international symposium on symbolic and algebraic computation, ISSAC '98, Rostock, Germany, (Oliver (ed.) Gloor, ed.), New York, NY: ACM Press, August 1998, pp. 132–139 (English).
- [LKM11] V. Levandovskyy, C. Koutschan, and O. Motsak, *On two-generated non-commutative algebras subject to the affine relation.*, Berlin: Springer, 2011 (English).
- [Loe03] A. Loewy, *Über reduzible lineare homogene Differentialgleichungen.*, Math. Ann. **56** (1903), 549–584 (German).
- [Loe06] A. Loewy, *Über vollständig reduzible lineare homogene Differentialgleichungen.*, Math. Ann. **62** (1906), 89–117 (German).
- [LS11] V. Levandovskyy and K. Schindelar, *Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases.*, J. Symb. Comput. **46** (2011), no. 5, 595–608 (English).
- [LS12] V. Levandovskyy and K. Schindelar, *Fraction-free algorithm for the computation of diagonal forms matrices over Ore domains using Gröbner bases*, J. Symb. Comput. **47** (2012), no. 10, 1214 – 1232.
- [MA94] H. Melenk and J. Apel, *Reduce package ncpoly: Computation in non-commutative polynomial ideals.*, Konrad-Zuse-Zentrum Berlin (ZIB), 1994.
- [Mid08] J. Middeke, *A polynomial-time algorithm for the Jacobson form for matrices of differential operators*, Tech. Report 08-13, Research Institute for Symbolic Computation (RISC), Linz, Austria, 2008.
- [Mid11] J. Middeke, *A computational view on normal forms of matrices of Ore polynomials*, Ph.D. thesis, Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, 2011.
- [MM82] E. W. Mayr and A. R. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals.*, Adv. Math. **46** (1982), 305–329 (English).
- [MR10] R. Motwani and P. Raghavan, *Algorithms and theory of computation handbook*, Chapman & Hall/CRC, 2010, pp. 12–12.
- [Sch80] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities.*, J. Assoc. Comput. Mach. **27** (1980), 701–717 (English).
- [SL97] A. Storjohann and G. Labahn, *A fast Las Vegas algorithm for computing the Smith normal form of a polynomial matrix.*, Linear Algebra Appl. **253** (1997), 155–173 (English).
- [Smi61] H.J.S. Smith, *On systems of linear indeterminate equations and congruences*, Philosophical Transactions of the Royal Society of London **151** (1861), pp. 293–326.
- [SST00] M. Saito, B. Sturmfels, and N. Takayama, *Gröbner deformations of hypergeometric differential equations.*, Berlin: Springer, 2000 (English).
- [TL11] S.P. Tsarev and S.V. Larin, *Structure of the lattice of right divisors of a linear ordinary differential operator*, Differential Equations by Algebraic Methods (Deam2) Conference, proceedings not yet published, RISC, Linz, February 2011.
- [Tsa96] S.P. Tsarev, *An algorithm for complete enumeration of all factorizations of a linear ordinary differential operator*, New York, NY: ACM Press, 1996 (English).
- [Tsa00] H. Tsai, *Weyl closure of a linear differential operator.*, J. Symb. Comput. **29** (2000), no. 4-5, 747–775 (English).
- [vdPS03] M. van der Put and M. F. Singer, *Galois theory of linear differential equations.*, Berlin: Springer, 2003 (English).
- [vH97] M. van Hoeij, *Factorization of differential operators with rational functions coefficients.*, J. Symb. Comput. **24** (1997), no. 5, 537–561 (English).
- [vHY10] M. van Hoeij and Q. Yuan, *Finding all Bessel type solutions for linear differential equations with rational function coefficients*, Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation (New York, NY, USA), ISSAC '10, ACM, 2010, pp. 37–44.
- [Zer06] E. Zerz, *Algebraic Systems Theory*, Lecture Notes, RWTH Aachen University, February 2006.

Appendix

From Chapter 1

In Subsection 2.2.5. The output of SINGULAR for h_1 with our new algorithm is the following.

```
ring R = 0, (x,d), dp;
def r = nc_algebra(1,1);
setring(r);
LIB "ncfactor.lib";
poly h = (1+x^2*d)^4;
facFirstWeyl(h);
[
  [1, x2d+1, x2d-x+1, x2d-x+1, x2d+2x+1],          [1]
  [1, x2d+1, x2d-x+1, x2d+x+1, x2d+1],            [2]
  [1, x2d+1, x2d-2x+1, x2d+x+1, x2d+x+1],        [3]
  [1, x2d+1, x2d-2x+1, x2d+1, x2d+2x+1],         [4]
  [1, x2d+1, x2d+1, x2d-x+1, x2d+x+1],           [5]
  [1, x2d+1, x2d+1, x2d+1, x2d+1],               [6]
  [1, x2d-x+1, x2d-2x+1, x2d+2x+1, x2d+x+1],    [7]
  [1, x2d-x+1, x2d-2x+1, x2d+1, x2d+3x+1],      [8]
  [1, x2d-x+1, x2d-x+1, x2d+2x+1, x2d+1],       [9]
  [1, x2d-x+1, x2d-x+1, x2d-x+1, x2d+3x+1],     [10]
  [1, x2d-x+1, x2d+x+1, x2d-x+1, x2d+x+1],      [11]
  [1, x2d-x+1, x2d+x+1, x2d+1, x2d+1],          [12]
  [1, x2d-3x+1, x2d-x+1, x2d+2x+1, x2d+2x+1],   [13]
  [1, x2d-3x+1, x2d-x+1, x2d+x+1, x2d+3x+1],   [14]
  [1, x2d-3x+1, x2d+1, x2d+2x+1, x2d+x+1],      [15]
  [1, x2d-3x+1, x2d+1, x2d+1, x2d+3x+1],        [16]
  [1, x2d-3x+1, x2d+x+1, x2d+x+1, x2d+x+1],     [17]
  [1, x2d-3x+1, x2d+x+1, x2d+1, x2d+2x+1],     [18]
  [1, x2d-2x+1, x2d+x+1, x2d-x+1, x2d+2x+1],    [19]
  [1, x2d-2x+1, x2d+x+1, x2d+x+1, x2d+1],       [20]
  [1, x2d-2x+1, x2d-2x+1, x2d+2x+1, x2d+2x+1], [21]
  [1, x2d-2x+1, x2d-2x+1, x2d+x+1, x2d+3x+1],  [22]
  [1, x2d-2x+1, x2d+1, x2d+2x+1, x2d+1],       [23]
  [1, x2d-2x+1, x2d+1, x2d-x+1, x2d+3x+1]      [24]
]
```

For h_3 , the corresponding code and the output do look like the following.

```
ring R = 0, (x,d), dp;
def r = nc_algebra(1,1);
setring(r);
LIB "ncfactor.lib";
poly h = (x^4-1)*x*d^2+(1+7*x^4)*d+8*x^3;
facFirstWeyl(h);
```

```
[
  [1,d,xd-2,x+1,x2+1,x-1],          [1]
  [1,d,xd-2,x-1,x2+1,x+1],          [2]
  [1,d,xd-2,x2+1,x+1,x-1],          [3]
  [1,d,xd-2,x2+1,x-1,x+1],          [4]
  [1,d,xd-2,x+1,x-1,x2+1],          [5]
  [1,d,xd-2,x-1,x+1,x2+1],          [6]
  [1,xd-1,d,x+1,x2+1,x-1],          [7]
  [1,xd-1,d,x-1,x2+1,x+1],          [8]
  [1,xd-1,d,x2+1,x+1,x-1],          [9]
  [1,xd-1,d,x2+1,x-1,x+1],          [10]
  [1,xd-1,d,x+1,x-1,x2+1],          [11]
  [1,xd-1,d,x-1,x+1,x2+1]           [12]
]
```

And last but not least the output for the polynomial h_4 .

```
ring R = 0,(x,d),dp;
def r = nc_algebra(1,1);
setring(r);
LIB "ncfactor.lib";
poly h = 10x5d4+26x4d5+47x5d2-97x4d3;
facFirstWeyl(h);
[
  [1,10x4d2+26x3d3+47x4-117x3d-78x2d2+117x2+156xd-156,x,d,d],          [1]
  [1,10x4d2+26x3d3+47x4-117x3d-78x2d2+117x2+156xd-156,d,xd-1],          [2]
  [1,x,x,x,x,10xd2+26d3+47x-97d,d,d],          [3]
  [1,xd-3,x,x,x,10xd3+26d4+47xd-107d2-47],          [4]
  [1,x,xd-2,x,x,10xd3+26d4+47xd-107d2-47],          [5]
  [1,x,x,xd-1,x,10xd3+26d4+47xd-107d2-47],          [6]
  [1,x,x,x,x,d,10xd3+26d4+47xd-107d2-47],          [7]
  [1,,xd-3,10x3d2+26x2d3+47x3-117x2d-52xd2+52d,xd-1]          [8]
]
```

From Chapter 2

5.3. In Subsection 1.3. Here, we use all notations and definitions given in Subsection 1.3. As announced before in Remark 1.22, we are now going to look closer at an approach to solve for b having a trivial gcd with f and $f \mid gb$ under the given conditions there.

One general assumption that we can make here is that we already have candidates (sometimes multiple ones) for b_{m_1} and b_{m_2} given. One can see that within the different steps above.

Dependent on m_2 (which for system solving reasons we assume to be $m_2 = m_1 - 1$) and n_2 , the second highest homogeneous part of gb is either given by

- $g_{n_1}b_{m_2}$,
- $g_{n_2}b_{m_1}$ OR
- $g_{n_1}b_{m_2} + g_{n_2}b_{m_1}$.

On the other hand, the second highest homogeneous part of af is also either given by

- $a_{\mu_1}f_{\nu_2}$,
- $a_{\mu_2}f_{\nu_1}$ OR
- $a_{\mu_1}f_{\nu_2} + a_{\mu_2}f_{\nu_1}$.

Both of them must coincide.

As we fixed our choice of b_{m_1} , also on the other side a_{μ_1} is uniquely determined by that, because we must have

$$a_{\mu_1} f_{\nu_1} = g_{n_1} b_{m_1},$$

and f_{ν_1}, g_{n_1} and b_{m_1} are given. Therefore, when we are solving for b_{m_2} , we have in the equation at most b_{m_2} and a_{μ_2} as indeterminates. This becomes clear when we look at the possible equations to solve for the second most highest homogeneous summand:

$$(5.1) \quad g_{n_1} \underline{b_{m_2}} = a_{\mu_1} f_{\nu_2}$$

$$(5.2) \quad g_{n_1} \underline{b_{m_2}} = \underline{a_{\mu_2}} f_{\nu_1}$$

$$(5.3) \quad g_{n_1} \underline{b_{m_2}} = a_{\mu_1} f_{\nu_2} + \underline{a_{\mu_2}} f_{\nu_1}$$

$$(5.4) \quad g_{n_2} b_{m_1} = a_{\mu_1} f_{\nu_2}$$

$$(5.5) \quad g_{n_2} b_{m_1} = \underline{a_{\mu_2}} f_{\nu_1}$$

$$(5.6) \quad g_{n_2} b_{m_1} = a_{\mu_1} f_{\nu_2} + \underline{a_{\mu_2}} f_{\nu_1}$$

$$(5.7) \quad g_{n_1} \underline{b_{m_2}} + g_{n_2} b_{m_1} = a_{\mu_1} f_{\nu_2}$$

$$(5.8) \quad g_{n_1} \underline{b_{m_2}} + g_{n_2} b_{m_1} = \underline{a_{\mu_2}} f_{\nu_1}$$

$$(5.9) \quad g_{n_1} \underline{b_{m_2}} + g_{n_2} b_{m_1} = a_{\mu_1} f_{\nu_2} + \underline{a_{\mu_2}} f_{\nu_1}$$

The indeterminates in each equation are underlined. If there is just one, it is of course uniquely solvable. If both are there, as for example in equation (5.9), you can bring them on one side. In the example of (5.9), this means

$$g_{n_1} b_{m_2} - a_{\mu_2} f_{\nu_1} = a_{\mu_1} f_{\nu_2} - g_{n_2} b_{m_1}.$$

Here you can see that the element $a_{\mu_1} f_{\nu_2} - g_{n_2} b_{m_1}$ has to be contained in the set ${}_R\langle f_{\nu_1} \rangle + \langle g_{n_1} \rangle_R$. The indeterminate a_{μ_2} is then the cofactor of f_{ν_1} , and b_{m_2} is the cofactor of g_{n_1} in this sum. Here, one might have some freedom in the choice of those elements. Moreover, as appeared in the chapter about factorization, we can even put the finding of the solution down to solve it for elements in $\mathbb{K}[\theta]$. This also tells us, that finding an element in this sum that coincides with the right hand side of the equation is possible with high probability. That means that we should not put much hope in not being able to find it and return FALSE early.

After the determination of b_{m_2} and a_{μ_2} we go step by step down the homogeneous parts of gb and af . For every further step, we will have at most two new indeterminates that we have to solve for. This can be handled in the same way. Of course, in the end, they also have to fulfill the equations starting at $g_{n_k} b_{m_l} = a_{\mu_c} f_{\nu_d}$. Finding the solution spaces for them can be started in a parallel fashion. One also can try to eliminate candidates in between if it would become clear that for example b would have a nontrivial greatest common right divisor with f or a a nontrivial greatest common left divisor with g .

The part that makes all of this very hard is: The coefficients of a and b might come out of infinite sets. It appears to be very hard to proof whether all possibilities would be violating our left respectively right ideal condition. We will leave that part out here, since our aim in the first place was not to contribute an algorithm for determining whether

two polynomials are similar, but having some statements about relations they have. A complete development of an algorithm dealing with that problem would be worth a whole master thesis on its own.

From Chapter 3

In Subsection 5.1. We took as an example the matrix

$$A := \begin{bmatrix} S & x \\ x & S \end{bmatrix}$$

And we use it as in input in our experimental implementation.

```
printf("%a",hermiteToGetJacobson(A, MyShiftAlgebra));
==>Matrix(2, 2,
[
  [OrePoly(1)      OrePoly(0)],
  [OrePoly(0)      f          ]
])
```

Here, f is the polynomial

$$f = S^2 + \frac{-4(148x + 73x^2 + 75)}{13279 + 18339x^2 + 13090x + 5329x^4 + 11242x^3}S - x \frac{61279 + 188849x^2 + 166089x + 37887x^4 + 116597x^3 + 5329x^5}{13279 + 18339x^2 + 13090x + 5329x^4 + 11242x^3}.$$

As we see, we obtain the Jacobson form.