JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

A computational view on normal forms of matrices of Ore polynomials

DISSERTATION

zur Erlangung des akademischen Grades

Doktor

im Doktoratsstudium der

Naturwissenschaften

Eingereicht von:
Johannes Middeke

Angefertigt am:
Research Institute for Symbolic Computation (RISC)

Beurteilung:
Univ.-Prof. DI. Dr. Franz Winkler (Betreuung)
Prof. Dr. George Labahn

Mitwirkung:
Dr. Günter Landsmann

Linz, Juli, 2011

Kurzfassung/Abstract

Kurzfassung

Diese Doktorarbeit behandelt Normalformen von Matrizen über Ringen von Ore-Polynomen. Sie ist in drei Teile geteilt: Zunächst werden Ore-Polynome vorgestellt und ihre grundlegenden Eigenschaften. Dieser Teil beinhaltet einen Exkurs über Integro-Differential-Operatoren. Zum zweiten werden im Hauptteil ein- und beidseitige Normalformen von Matrizen behandelt. Genauer legen wir unseren Fokus auf die Popov-, die Hermite- und die Jacobsonform. Der letzte Teil der Arbeit beschäftigt sich mit einer Anwendung von Normalformen auf ein Problem aus der Kontrolltheorie.

Im folgenden soll auf alle diese Teile noch ein mal genauer eingegangen werden.

Ore-Polynome, die von einigen Autoren auch als Schiefpolynome bezeichnet werden, wurden zuerst von Øystein Ore untersucht in [Ore32a, Ore32b]. Sie verallgemeinern die gewöhnlichen Polynome, wobei sie fast alle deren Eigenschaften erhalten mit der Ausnahme, dass die Multiplikation nicht kommutativ sein muss: Weder wird vorausgesetzt, dass die Koeffizienten miteinander kommutieren, noch muss die Unbestimmte mit diesen kommutieren. Ore-Polynome können verwendet werden, um Ringe von Differential- oder Differenzoperatoren zu modellieren. Unter anderem ist die bekannte Weyl-Algebra ein Ore-Polynomring.

Als eine Art ausführliches Beispiel benutzen wir Ore-Polynome, um Integro-Differential-Operatoren mit polynomiellen Koeffizienten darzustellen. Dieser Teil basiert auf unserem ISSAC 2009-Artikel [RRM09]. Wir erhalten eine Konstruktion, die große Ähnlichkeit zur Weyl-Algebra im rein differentiellen Fall aufweist.

Im Hauptteil der Doktorarbeit werden zunächst Normalformen von Matrizen betrachtet. Diese bieten eine Möglichkeit, Systeme von linearen Operatorgleichungen darzustellen und auf Lösbarkeit oder andere Eigenschaften hin zu untersuchen. Wir widmen uns zunächst Normalformen in Bezug auf Zeilenoperationen. Die Untersuchung erstreckt sich dabei auf Zeilenreduktion, Hermite-, Popov- und verschobene Popovformen. Wir stellen eine Verbindung dieser Normalformen zu Gröbnerbasen über Moduln her. Als eine mögliche Anwendung dieser Verbindung wird ein modifizierter FGLM-Algorithmus vorgestellt, der es erlaubt, von einer Normalform in eine andere zu wechseln. Teile dieser Arbeit wurden auf der ACA 2010 und in [Mid10] vorgestellt.

Weiterhin betrachten wir die Jacobsonform, die eine Normalform in Bezug auf simultane Zeilen- und Spaltenoperationen darstellt. In diesem Teil beschränken wir uns auf Differentialoperatoren mit kommutierenden Koeffizienten. Wir präsentieren einen modularen Algorithmus, der die Jacobsonform mit Hilfe von zyklischen Vektoren berechnet und der zumindest bei Körpern der Charak-

teristik Null immer ein Ergebnis liefert. Wir geben Bedingungen an, wann er auch bei positiver Charakteristik erfolgreich ist.

Der letzte Teil der Arbeit behandelt ein Thema aus der Kontrolltheorie. Wir untersuchen lineare, zeitvariante Systeme mit Totzeiten auf differentielle und auf π-Flachheit, wobei wir Ideen aus [MCL10] aufgreifen. Unsere Methode basiert auf den einseitigen Normalformen aus dem Hauptteil der Doktorarbeit anstelle der ursprünglich vorgeschlagenen Jacobsonform. Diese Arbeit wird auf der AMMCS 2011 vorgestellt und ist bei der CDC 2011 eingereicht. Erste Resultate wurden in [AM10] präsentiert.

Abstract

This thesis treats normal forms of matrices over rings of Ore polynomials. The whole thesis is divided in three parts: First, Ore polynomials are described and basic facts about them are recalled. This part also includes integro-differential operators as an extended example. Second, in the main part we present one- and two-sided normal forms of matrices. More precisely, we deal with the Popov normal form, Hermite normal form and the Jacobson normal form. In the last part, we explore an application of matrix normal forms to a problem in control theory.

Below, we describe each of the parts in more detail.

Ore polynomials, sometimes called skew polynomials, arise from the work of Øystein Ore in [Ore33]. They are a generalisation of the usual polynomials with almost all of their properties with the main exception being that the multiplication in not necessarily commutative: Neither need the coefficients commute with each other, nor does the indeterminate have to commute with them. Ore polynomials can be used to model differential or difference operators. For example, the famous Weyl algebra can be considered to be an Ore polynomial ring.

As an example, we model integro-differential operators with polynomial coefficients using Ore polynomials. This part is based on our ISSAC 2009 paper [RRM09]. We arrive at a construction which is similar to the Weyl algebra in the purely differential case.

In the main part, we consider normal forms of matrices. These make it possible to express systems of linear equations involving operators and to determine the properties of these systems such as, for example, solvability. We first consider normal forms with respect to row-operations. The coefficient domain here is a skew field. We treat row-reduction, the Hermite normal form, the Popov normal form and shifted Popov normal forms. We draw a connection between these normal forms to Gröbner bases over modules. As an application of this connection, we present a modified FGLM algorithm for converting matrices from one normal form into another. Parts of this were presented at ACA 2010 and in [Mid10].

We also consider the Jacobson normal form which is a normal form with respect to simultaneous row- and column-operations. Here, we restrict ourselves to differential operators over a commutative coefficient domain. We present a modular algorithm for computing a Jacobson normal form which is based on cyclic vectors and which is guaranteed to succeed in characteristic zero, but under certain conditions also yields a result in positive characteristic.

The last part deals with a topic from control theory. We examine linear time-varying differential systems with delays for differential flatness and π-flatness where we use an idea from [MCL10]. For this, we apply the one-sided normal forms from the main part instead of the originally proposed

Jacobson normal form. This will be presented at AMMCS 2011 and is also submitted to CDC 2011—initial results were presented at [AM10].

Curriculum vitæ

Personal data

Full Name	Johannes Middeke
Date of Birth	30th of November, 1979
Place of Birth	Oldenburg (Oldenburg), Germany
Home address	Aubrunnerweg 9, A-4040 Linz, Austria
Email address	jmiddeke@risc.jku.at
Citizenship	German

Career

2007–present	Ph. D. studies in Natural Sciences at the Research Institute for Symbolic Computation (RISC) in Hagenberg/Linz, Austria.
2000–2007	Diploma studies in Mathematics at Carl von Ossietzky University in Oldenburg (Oldenburg), Germany. Degree of Diplom-Mathematiker with distinction.

Career related activities

- Research visit at University of Innsbruck (Austria, 2009)
- Contributed talk at ISSAC 2009 (Seoul, Korea)
- Research visit at University of Waterloo (Canada, 2009)
- Contributed talk at ACA 2010 (Vlorë, Albania)
- Contributed talk at DEAM 2 (Linz, Austria)
- Organising committee of DEAM 2 (Linz, Austria)
- Research visit at University of Waterloo (Canada, 2011)
- Organising committee of CAI 2011 (Linz, Austria)
- Contributed talk at AMMCS 2011 (Waterloo, Canada)

Published papers

1. J. Middeke, *A polynomial-time algorithm for the Jacobson form for matrices of differential operators*, Tech. Report 08-13, RISC Report Series, University of Linz, Austria, July 2008.
2. G. Regensburger, M. Rosenkranz, and J. Middeke, *A skew polynomial approach to integro-differential operators*, Proceedings of ISSAC 2009 (J. R. Johnson, H. Park, and E. Kaltofen, eds.), ACM, 2009, pp. 287–294 (English).
3. J. Middeke, *Converting between the Popov and the Hermite form of matrices of differential operators using an FGLM-like algorithm*, Tech. report, RISC Report Series, University of Linz, Austria, June 2010.
4. J. Middeke, E. Shemyakova, F. Winkler. *Proceedings of DEAM (Workshop for Differential Equations by Algebraic Methods)*. Technical report no. 09-08 in RISC Report Series, University of Linz, Austria. 2009. Proceedings.
5. J. Middeke. *Conversion between Hermite and Popov normal forms using an FGLM-like approach*, Albanian Journal of Mathematics, Vol. 4, No. 4 (2010), Special Issue, Applications of Computer Algebra 2010.

Eidesstattliche Erklärung/Affidavit

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Hereby I declare in lieu of oath that I wrote the present thesis by my own and without any assistance from third parties and without sources other than those indicated in the thesis itself.

Johannes Middeke

Acknowledgements

First and foremost, many thanks to my adviser Prof. Franz Winkler for his support. He has allowed me great latitude in the choice of my topic and has always provided me with good suggestions in the many discussions in his seminar. I have benefited from his experience as a researcher and his sense for good mathematical writing.

Then, I want to give my thanks to Prof. George Labahn, my second adviser, for inviting me to the University of Waterloo and the discussions we had there about row-reduction and the Popov normal form. Besides the valuable scientific advise, he has also taken much efford to make my visits in Waterloo enjoyable.

I am grateful to Günter Landsmann who has given me many useful comments about my thesis and in general a lot of advise over the years. Also, his lectures were always a very pleasant way to spend my time.

I would like to thank my diploma thesis adviser Prof. Wiland Schmale. He has brought me to the subject of differential algebra and normal form computations. In addition, he has given me the idea of looking into cyclic vectors for the Jacobson normal form computation.

Many thanks to Markus Rosenkranz and Georg Regensburger. The lectures they gave at the University of Linz and the discussions we had about our joint paper have given me many insights into their topic.

I am thankful to Felix Antritter with whom I collaborated on the applications of normal forms in control theory.

I would like to thank Prof. Franz Pauer whom I visited at the University of Innsbruck. He has introduced me to the topic of Gröbner bases over rings.

I am grateful to Manuel Kauers whose lecture made me aquainted to the FGLM algorithm.

Many thanks go to Anja Korporal for kindly reading my thesis and spotting more typos than anybody else. Also, during my whole studies she has always been a big support and our scientific discussions over the years have given me many ideas.

I gratefully acknowledge the Austrian Science Foundation (FWF) whose funding under the project DIFFOP (P20 336–N18) enabled me to perfom my work on this theis.

Finally, I would like thank all my colleagues at RISC for providing such a pleasant and inspiring environment to work in.

Contents

Part I

Introduction

1 Overview

This thesis is devoted to the study of matrices over rings of non-commutative polynomials. It considers one- and two-sided normal forms of such matrices as well as an application. In this chapter we will give just a brief overview over the field. In the following, the individual chapters will contain more detailed information on the background of their respective topics.

As basic domain for investigations, we will consider *Ore polynomials* which first appeared in [Ore33]. Named after their inventor, Øystein Ore, they are a class of (univariate) non-commutative polynomials that may be characterised by the fact that the multiplication respects the usual degree rule $\deg(fg) \leq \deg f + \deg g$ which is taken from the usual polynomials. The latter are also an example of Ore polynomials and the only one where the multiplication is commutative. Two more prominent examples are *differential operators* and *difference operators* which are both generalised by the Ore construction. Other examples include q-difference operators or integro-differential operators. Confer also [CS98, Table 1] for a list of more operators that can be modelled using Ore polynomials.

The degree rule implies that Ore polynomials must fulfil the so-called *commutation rule* $\partial a = \sigma(a)\partial + \vartheta(a)$ where ∂ is the indeterminate, a is an element of the coefficient domain and σ and ϑ are maps of the coefficients into themselves. Setting for instance σ to the identity and ϑ to the derivation d/dt, the commutation rule models the composition of differential operators.

Of the many possible instances of Ore polynomials we chose to investigate integro-differential operators more closely. As in [RRM09] we define the *integro-differential Weyl algebra*. This is an extension of the famous differential Weyl algebra where in addition to the derivative an integral has been added. That is, the elements of the integro-differential Weyl algebra can be used to model operators from calculus like, for example,

$$f \mapsto xf + \int_0^x (x^3 f)' \, dx - f'.$$

Integro-differential operators provide an algebraic setting in which initial and boundary value problems may be studied. Confer, for example, [KRR11]. Since the addition of the integral introduces zero-divisors, the integro-differential Weyl algebra does not have all of the properties of its differential counterpart. For instance, it is not a simple ring.

The main focus of this thesis are matrices over Ore polynomial rings and their normal forms. As in the usual linear algebra, matrices of operators can be thought of as representing systems of equations involving these operators. For example, the system $f' + g = 0$ and $g - xg'' = 0$ may be represented in the following way

$$\begin{pmatrix} \frac{d}{dx} & 1 \\ 0 & 1 - x\frac{d^2}{dx^2} \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} = 0.$$

Like in the usual linear algebra over fields, elementary transformations of matrices do not alter the system. They may hence be utilised to compute *normal forms* which make reasoning about these systems easier. This includes, of course, solving these systems. Other applications of normal forms include the comparision of two different systems: The answer to the question whether one system includes another one may directly be translated to an inclusion of the corresponding solution spaces.

In this thesis we consider normal forms with respect to elementary row-operations and normal forms where additional column-operations are allowed. The first case, the one-sided normal forms, include the *Hermite normal form* and the *Popov normal form*—confer, for example, [BLV99]. While the first normal form is a generalisation of the row echelon form for matrices over fields; the latter, the Popov normal form, arising from the considerations in [Pop70], gives a minimal degree description of the row-space of the matrix.

For the special case of differential operators, we consider the *Jacobson normal form*. This is a diagonal matrix which includes at most one non-trivial diagonal element. Its interpretation in the setting of systems of differential equation is the translation of system to a single (usually high-order) equation. In the above example, the Jacobson normal form is

$$\begin{pmatrix} 1 & 0 \\ x\frac{d^2}{dx^2} - 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{d}{dx} & 1 \\ 0 & 1 - x\frac{d^2}{dx^2} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\frac{d}{dx} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & x\frac{d^3}{dx^3} - \frac{d}{dx} \end{pmatrix}$$

meaning that $f' + g = 0 = g - xg''$ it is equivalent to the single equation $xh''' = h'$. Thus, the Jacobson normal form may be used as an instrument for solving systems of differential equations—see, for example, also [CQ05].

Another prominent application of normal forms except for solving systems is the examination of their properties in more specialised fields of mathematics. For example, in *control theory*, matrix normal forms may be applied to determine the properties of control systems. In this thesis, we will treat the problem of *(differential) flatness* of such systems—see Chapter 8 for a definition. We describe an algorithm to solve the question whether a system is flat using the one-sided normal forms from earlier chapters.

2

Outline of the thesis

The whole thesis is divided into three parts. In the first part, we will introduce rings of so-called Ore polynomials; in the second part, we will consider matrices over those rings; and in the third part, we will present an application of the first two parts in the frame of control theory.

We start with a general overview over Ore polynomials in Chapter 3. After recalling the definition and the most basic properties in Section 3.1, we discuss as most prominent examples in Section 3.2 the commutative polynomials, the differential operators and the difference operators. The next section, Section 3.3, deals with the multiplication and (Euclidean) division of Ore polynomials. Section 3.4 list two less basic theorems: The universal property of Ore polynomials and one of its consequences. Chapter 3 is concluded with an overview of fractions over non-commutative domains.

As an extended example, Chapter 4 contains a treatise on the integro-differential Weyl algebra. This is an analogon to the famous differential Weyl algebra which includes, besides the derivation, also an integral operator. In Section 4.1 we give an overview over the previous work on integro-differential operators over general integro-differential algebras. Then, in Section 4.2, we restrict ourselves to (commutative) polynomials are coefficient domain for our operators—just as in the Weyl algebra. The resulting operator ring is then dubbed the integro-differential Weyl algebra. We investigate its ideal structure and prove that it is slightly more general than the integro-differential operators with respect to the definition in Section 4.1.

We also consider two important special cases: integro-differential operators with constant coefficients and integral operators with polynomial coefficients. The later we will call the integro Weyl algebra. For both special cases we will derive descriptions of the ideal structure and possible bases.

In Chapter 5 we start with the examination of matrices over Ore polynomial rings and their properties. The chapter begins in Section 5.1 with an overview over the notations for matrices that will be used in this thesis. The first main topic in the matrix part is then row-reduction which will be explained in Section 5.2. The section includes also a short review on Gröbner bases over rings which will be linked to row-reduction. Section 5.3 does a basic complexity analysis for the row-reduction algorithm which we be referenced in later chapters. At the end of Chapter 5, in Section 5.4, we explain how row-reduction may be used for the inversion of matrices and for computing greatest common divisors.

Chapter 6 is devoted to the study of one-sided normal forms of matrices. Objects of this study will be the Popov normal form, shifted Popov normal forms which are explained in Section 6.1 and the Hermite normal form which we define in Section 6.2. Both sections do also contain some basic properties of the respective normal forms. In Section 6.3, we will then recall Gröbner bases for free modules over Ore polynomial rings. They will be connected to the one-sided normal forms in Section 6.4 where we will prove that the Popov normal form, the shifted Popov normal forms and the Hermite normal form are indeed reduced Gröbner bases. We apply this result in Section 6.5 to derive a conversion algorithm for normal forms that is based on the famous FGLM algorithm.

We shift our focus from one-sided normal forms to a two-sided normal form in Chapter 7 where we consider the Jacobson normal form for matrices of differential operators. We present the definition of the Jacobson normal form in Section 7.1. In the next section, Section 7.2, we recall existing methods for the computation of the Jacobson normal form. In the remaining three sections of Chapter 7 we then derive a new method which is based modular computations. We start with pre-conditioning the matrix in Section 7.3 where we reach a decomposition of the quotient of the row-space into the torsion and free part. In Section 7.4 we will concentrate on the torsion part and derive conditions for it being a cyclic module. This is then be used in Section 7.5 where an algorithm is presented that allows to compute a Jacobson normal form with corresponding transformation matrices from a cyclic vector in the torsion part.

Finally, in Chapter 8, we provide an example on how normal forms may be applied to solve problems in the field of control theory. We start with a rough overview of control theory in Section 8.1. Then, in Section 8.2, we will concentrate on the notions of differential flatness and of π-flatness and will discuss an algorithm which checks whether a given system has one of these properties.

For illustrational purposes, this thesis includes MAPLE code for the conversion of one-sided normal forms into each other in the appendix. We did, however, decide to not develope this code into a complete package as the methods or at least parts of them are already included in MAPLE.

Part II

Ore polynomials

3

Definitions and basic facts

3.1 Definition

Ore polynomials originate from the works of Øystein Ore (see [Ore32a, Ore32b] or [Ore33]). The main idea was to study polynomials whose multiplication is non-commutative but which still fulfill the condition that the degree of a product does not exceed the sum of the degrees of the factors. Assume we are given two rings A and R such that $A \subseteq R$ and such that there exists an element ∂ whose powers generate R as a left A-module. That is, the elements of R are of the form

$$f = a_n\partial^n + a_{n-1}\partial^{n-1} + \ldots + a_2\partial^2 + a_1\partial + a_0$$

where $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in A$.[1] We assume further that this representation is unique, that is, that the powers of ∂ are A-linearly independent. If in the above representation $a_n \neq 0$, then we call n the *degree* of f denoted by $\deg f = n$ and we call a_n the *leading coefficient* of f for which we write $\mathrm{lc}(f) = a_n$. In order to avoid case distinctions we set $\deg 0 = -\infty$, while $\mathrm{lc}(0)$ remains undefined. Additionally, we define the s^{th} coefficient to be $\mathrm{coeff}(\partial^s, f) = a_s$ for $s \leq n$ and $\mathrm{coeff}(\partial^s, f) = 0$ otherwise.

The condition that we would like to impose on the elements of R can now be written down as

$$\deg(fg) \leq \deg f + \deg g \qquad \text{for all } f \text{ and } g \in R.$$

In particular, if $f = \partial$ and $g = a \in A$, then we obtain the *commutation rule*

$$\partial a = \sigma(a)\partial + \vartheta(a) \tag{3.1}$$

where $\sigma(a)$ and $\vartheta(a) \in A$ denote two elements that are uniquely determined by the condition that the powers of ∂ are linearly independent. Regarding σ and ϑ as functions $\sigma\colon A \to A$ and $\vartheta\colon A \to A$, the distributive law of R implies

$$\sigma(a+b)\partial + \vartheta(a+b) = \partial(a+b) = \partial a + \partial b = \big(\sigma(a) + \sigma(b)\big)\partial + \big(\vartheta(a) + \vartheta(b)\big)$$

[1] In this thesis, the natural numbers $\mathbb{N}$ always contain 0.

and thus $\sigma(a+b)=\sigma(a)+\sigma(b)$ and $\vartheta(a+b)=\vartheta(a)+\vartheta(b)$ for all a and $b \in A$ using again the uniqueness of the representation of the elements in R. Using the associativity and the unit in R, it is possible to prove that σ must be an endomorphism of A and that ϑ is a σ-derivation:

Definition 3.1 (σ-derivation)**.** Let A be a ring and let $\sigma: A \to A$ be an endomorphim. A *σ-derivation* is an additive map $\vartheta: A \to A$ satisfying the *σ-Leibniz rule*

$$\vartheta(ab) = \sigma(a)\vartheta(b) + \vartheta(a)b \tag{3.2}$$

for all a and $b \in A$.

If σ is the identity function id, then ϑ just satisfies the usual Leibniz rule from calculus. In that case we call ϑ simply a derivation.

Until now, we assumed that a ring R with the specified properties was given. But it is in fact possible for every ring A that is endowed with an endomorphim $\sigma: A \to A$ and a σ-derivation $\vartheta: A \to A$ to construct such a superring. See, for example, [Coh85, Theorem 0.10.1] where the construction is carried out analogously to the usual polynomials by embedding A into the (group) endomorphisms of $A^{\mathbb{N}}$ and defining $\partial: A^{\mathbb{N}} \to A^{\mathbb{N}}$ in a way such that its powers are A-linearly independent and such that the commutation rule (3.1) is fulfilled. The resulting ring is denoted by $A[\partial;\sigma,\vartheta]$ and is called the ring of *Ore polynomials* over A in the variable ∂ with respect to σ and ϑ. Some authors (including [Coh85]) prefer the name "skew polynomials"—but as this term is also used more specifically for certain subclasses of Ore polynomials (for example, [BCL06] reserves it for the case $\vartheta = 0$) we decided not to use it in this thesis.

There are generalisations of Ore polynomials. For example, in [CS98, Definition 1.2] so-called *Ore algebras* are defined. These are iterated Ore polynomial rings with the additional condition that the indeterminates commute. Even more general is the concept of so-called *Poincaré-Birkhoff-Witt rings* which are multivariate non-commutative polynomial rings with a slightly more complicated commutation rule than Ore algebras. See, for example, [BGTV03, Definition 2.2.5] for a definition. In [BGTV03, Corollary 2.3.3] it is shown that Ore algebras over skew fields are Poincaré-Birkhoff-Witt rings.

3.2 Examples

Commutative polynomials

First of all, the usual commutative polynomials are a special case of Ore polynomials. Indeed, if we take the identity function id and the zero-map 0, then in $A[\partial;\mathrm{id},0]$ the commutation rule (3.1) becomes just

$$\partial a = a\partial$$

for all $a \in A$. That means, that the ring $A[\partial;\mathrm{id},0]$ is isomorphic to the ring $A[X]$ of commutative polynomials over A.

Differential operators

Another important class of examples for Ore polynomials are *differential operators*. Here, we have $\sigma = \mathrm{id}$ and ϑ is a derivation in the ordinary sense. The commutation rule (3.1) becomes

$$\partial a = a\partial + \vartheta(a)$$

for all $a \in A$.

The connection to differential operators in the analytic sense can be drawn as follows. Let $\vartheta\colon A \to A$ be a derivation. We let A act on itself by left multiplication, that is, with each $a \in A$ we associate the function $a^* = x \mapsto ax$. The functions a^* with $a \in A$ and ϑ generate a subring in the group endomorphisms of A that can be identified with $A[\partial;\mathrm{id},\vartheta]$ if the powers of ϑ are A-linear independent. The reason is that using the Leibniz rule, we see that for every $b \in A$

$$\vartheta \circ a^*(b) = \vartheta(ab) = a\vartheta(b) + \vartheta(a)b = \left(a^* \circ \vartheta + \vartheta(a)^*\right)(b),$$

that is, we have the following identity of functions

$$\vartheta \circ a^* = a^* \circ \vartheta + \vartheta(a)^*$$

which is essentially the same as the commutation rule above.

A famous special case of differential operators is the *(first) Weyl algebra* $\mathrm{A}_1(\partial)$ which has a univariate polynomial ring $A = K[x]$ over a field K as coefficient domain and uses the standard derivation d/dx which maps x to 1. Note that fixing the derivative of x always yields unique derivation on $K[x]$ which extends the zero-derivation $a \mapsto 0$ on K. See, for example, [Kap76, I.2 Examples 4]. We refer the reader to [Cou95, Chapter 1] for a definition of and an extensive overview over the Weyl algebra. The introduction of [Cou95] contains a detailed historical overview.

Difference operators

The last major example that we are treating here are the *difference operators* which are sometimes also labelled shift or delay operators . The general case is that ϑ is simply the zero-map which makes the commutation rule (3.1) become

$$\partial a = \sigma(a)\partial.$$

The name “difference operator” comes from the case that A is a ring of functions in the real variable t and $\sigma\colon A \to A$ is the function $a(t) \mapsto a(t-\tau)$ that shifts the functions in A by a fixed amount $\tau \in \mathbb{R}$.

This class of Ore polynomials is also called “skew polynomials” by some authors (for example, [BCL06]).

3.3 Elementary properties

Multiplication

Let A be a ring, and let $\sigma\colon A \to A$ be an endomorphism and $\vartheta\colon A \to A$ be a σ-derivation. We abbreviate $A[\partial;\sigma,\vartheta]$ by R. If we take $f = f_m\partial^m + \ldots + f_1\partial + f_0 \in R$ where $f_0,\ldots,f_n \in A$, then

$$\partial f = \sum_{j=0}^{m} \partial f_j \partial^j = \sum_{j=0}^{m} \sigma(f_j)\partial^{j+1} + \sum_{j=0}^{m} \vartheta(f_j)\partial^j.$$

Letting σ and ϑ act on elements in R by coefficient-wise application, the above equation may be written more succinctly as

$$\partial f = \sigma(f)\partial + \vartheta(f). \tag{3.3}$$

Since multiplication by ∂ from the right is just a shift of the coefficients, we need m applications of σ and ϑ and $m-1$ additions in order to compute this product. That means to compute the product fg for $g \in R$, we could apply the following naïve method:

1. Compute iteratively $\partial^j g = \partial(\partial^{j-1} g) = \sigma(\partial^{j-1} g)\partial + \vartheta(\partial^j g)$ for $j = 1, \ldots, m$.
2. Compute the products $f_j \partial^j g$ for $j = 0, \ldots, m$.
3. Compute the sum $f_m \partial^m g + \ldots + f_1 \partial g + f_0 g$.

Let $\deg g = n$. Since computing $\partial^j g$ from $\partial^{j-1} g$ needs $(j-1)+n$ applications of σ and ϑ and $(j-1)+n-1$ additions, the first step needs

$$\sum_{j=1}^{m} \big((j-1)+n\big) = m(n-1) + \sum_{j=1}^{m} j = m(n-1) + \frac{m(m+1)}{2} = m\big(n - \frac{1}{2} + \frac{1}{2}m\big)$$

applications of σ and ϑ and $m(n - \frac{1}{2} - \frac{3}{2}m)$ additions. Computing the products in the second step needs

$$\sum_{j=0}^{m} (j+n) = (m+1)n + \frac{m(m+1)}{2} = (m+1)\big(n + \frac{1}{2}m\big)$$

multiplications in A, and the third step needs $m(n - \frac{1}{2} + \frac{1}{2}m)$ additions.

Remark 3.2. Counting applications of σ, ϑ, additions and multiplications in A all as atomic operations, we see that in order to compute the product fg of two elements f and $g \in R$ of degree $\deg f = m$ and degree $\deg g = n$, we need

$$\mathcal{O}(m \cdot \max\{m, n\})$$

operations in A.

It is also possible to derive direct formulæ for the coefficients of a product in means of the coefficients of the factors. See, for example, [Ore33, Equation (13)]. We repeat it here for the convenience of the reader.

Definition 3.3 (Diffnomial)**.** Let $k \le m$, and let $\sigma : A \to A$ and $\vartheta : A \to A$ be mappings for a ring A. By $\left\{ {m \atop k} \right\}$ we denote the sum of all compositions of σ and ϑ of length m where σ occurs exactly k times, that is,

$$\left\{ {m \atop k} \right\} : A \to A = \begin{cases} \mathrm{id} & \text{if } k = m = 0, \\ \sigma^m & \text{if } k = m, \\ \vartheta^m & \text{if } k = 0, \\ \left\{ {m-1 \atop k-1} \right\} \circ \sigma + \left\{ {m-1 \atop k} \right\} \circ \vartheta, & \text{otherwise.} \end{cases}$$

We call $\left\{ {m \atop k} \right\}$ a *diffnomial* for the pair σ and ϑ.

The diffnomials are also introduced—without a name though—in [Ore33]. We give explicit formulæ for two special cases.

Example 3.4. 1. If $\sigma = \mathrm{id}$ then for all $m \ge k$

$$\left\{ {m \atop k} \right\} = \binom{m}{m-k} \vartheta^{m-k} = \binom{m}{k} \vartheta^{m-k}$$

since there is a one-to-one correspondence between the summands of $\left\{ {m \atop k} \right\}$ and the $(m-k)$-element subsets of $\{1, \ldots, m\}$ given by the positions of where ϑ occurs in the compositions.

2. If $\vartheta = 0$ then

$$\left\{ {m \atop k} \right\} = \begin{cases} \sigma^m, & \text{if } m = k, \\ 0, & \text{otherwise.} \end{cases}$$

The diffnomials provide a short way to write down products with a skew variable using a notation that reminds a little bit of the general Leibniz rule.

Lemma 3.5 ([Ore33, Equation (13)])**.** *Let A be a ring with endomorphism $\sigma : A \to A$ and σ-derivation $\vartheta : A \to A$. For the (left) skew polynomial $f \in A[\partial; \sigma, \vartheta]$ and every $m \geq 0$ we have*

$$\partial^m f = \sum_{k=0}^{m} \left\{ {m \atop k} \right\} (f) \partial^k$$

where $\sigma(f)$ denotes f with σ applied to all its coeffcients and $\vartheta(f)$ means f with ϑ applied to its coefficients. That is, if $f = f_n \partial^n + \ldots + f_1 \partial + f_0$ with $f_0, \ldots, f_n \in A$ then $\sigma(f) = \sigma(f_n)\partial^n + \ldots + \sigma(f_1)\partial + \sigma(f_0)$ and $\vartheta(f) = \vartheta(f_n)\partial^n + \ldots + \vartheta(f_1)\partial + \vartheta(f_0)$.

Proof. We use induction on m. The formula is obviously true for $m = 0$ since both the left hand side and the right hand side will be just f. For $m = 1$ we obtain

$$\partial f = \sum_{k=0}^{n} \partial f_k \partial^k = \sum_{k=0}^{n} \big(\sigma(f_k)\partial + \vartheta(f_k)\big)\partial^k = \sum_{k=0}^{n} \sigma(f_k)\partial\partial^k + \sum_{k=0}^{n} \vartheta(f_k)\partial^k = \sigma(f)\partial + \vartheta(f)$$

where $f = f_n \partial^n + \ldots + f_1 \partial + f_0$ with $f_0, \ldots, f_n \in A$. Assume now that $m \geq 0$. Then

$$\begin{aligned} \partial^{m+1} f = \partial^m \big(\sigma(f)\partial + \vartheta(f)\big) &= \partial^m \sigma(f)\partial + \partial^m \vartheta(f) \\ &= \sum_{k=0}^{m} \left\{ {m \atop k} \right\} (\sigma(f)) \partial^k \partial + \sum_{k=0}^{m} \left\{ {m \atop k} \right\} (\vartheta(f)) \partial^k \\ &= \sum_{k=1}^{m+1} \left\{ {m \atop k-1} \right\} \circ \sigma(f) \partial^k + \sum_{k=0}^{m} \left\{ {m \atop k} \right\} \circ \vartheta(f) \partial^k \\ &= \sum_{k=1}^{m+1} \left(\left\{ {m \atop k-1} \right\} \circ \sigma + \left\{ {m \atop k} \right\} \circ \vartheta \right) (f) \partial^k = \sum_{k=1}^{m+1} \left\{ {m+1 \atop k} \right\} (f) \partial^k \end{aligned}$$

using the case $m = 1$ for the first and the induction hypothesis for the fourth identity. □

The formula $\partial g = \sigma(g)\partial + \vartheta(g)$ for non-zero $g \in R$ implies that $\operatorname{lc}(\partial g) = \sigma(\operatorname{lc}(g))$ unless $\sigma(\operatorname{lc}(g)) = 0$. Iterating this, we obtain for any non-zero $f \in R$ the identity

$$\operatorname{lc}(fg) = \operatorname{lc}(f)\, \sigma^{\deg f}\big(\operatorname{lc}(g)\big) \tag{3.4}$$

provided that neither $\operatorname{lc}(f)$ is a zero divisor nor $\sigma^{\deg f}\big(\operatorname{lc}(g)\big) = 0$. In particular, if A does not contain zero divisors and σ is injective, then the above formula always holds. Hence, in this case R will be a (non-commutative) domain.

Greatest common divisors

If A is a field and σ is an automorphism, then the leading coefficient formula (3.4) and the degree formula imply that for any non-zero f and $g \in R$ with $\deg g \leq \deg f$ the polynomial

$$\operatorname{lc}(f)\Big(\sigma^{\deg f - \deg g}(\operatorname{lc}(g))\Big)^{-1}\partial^{\deg f - \deg g} \cdot g$$

has the same degree and leading coefficient as f. Consequently, subtracting it from f yields a polynomial of degree strictly smaller than $\deg f$. Iterating this reduction we obtain polynomials $q \in R$ and $r \in R$ such that

$$f = qg + r$$

where $\deg r < \deg g$. We refer to this as *(Euclidean) right division*. It can be shown that q and r are uniquely determined by these conditions. Analogously, also

$$g \cdot \sigma^{-\deg g}\big(\operatorname{lc}(g)^{-1}\operatorname{lc}(f)\big)\partial^{\deg f - \deg g}$$

has the same leading coefficient and degree as f and we may compute $\tilde{q}$ and $\tilde{r} \in R$ such that

$$f = g\tilde{q} + \tilde{r}$$

and $\deg \tilde{r} < \deg g$. This will be called *(Euclidean) left division*.

It is also possible to do pseudo-division in a way analogous to the case of commutative polynomials. See, for example, [Li98].

Example 3.6. Consider the difference operators $\mathbb{Q}(X)[\partial; \mathfrak{s}, 0]$ where $\mathfrak{s}a(X) = a(X-1)$. Let $f = \partial^2 + X\partial + 1$ and $g = \frac{1}{X}\partial + 1$ then we have

$$f = \big((1+X)\partial - X\big)g + (X+1) \qquad \text{and} \qquad f = g\big((X-1)X + (X-1)\big) + (2-X)$$

illustrating that neither the quotient nor the remainder needs to be the same when going from left to right division.

The left and right division make R a left and right Euclidean ring. In particular R is a principal left and right ideal domain. Moreover, it is possible to compute greatest common left or right divisors as well as least common left or right multiples using a version of the *Euclidean algorithm*. This appeared already in [Ore33, Section 2]. Other presentations may be found, for example, in [BP96, Secion 3]. In [Li98, Proposition 6.1] an algorithm for greatest common divisors is presented which is based on subresulant methods, while [Li96] contains—at least for special coefficient domains—a modular method for the computation of greatest common right divisors.

Below in Lemma 5.16, we will present a method to compute greatest common divisors that is based on row-reduction. It will compute the greatest common divisor as well as the Bézout cofactors.

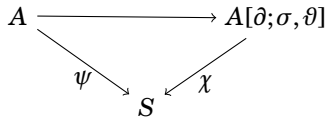
3.4 Further properties of Ore polynomial rings

Below we will need the following *universal property* of Ore polynomial rings which we cite from [MR01, § 1.2.5]. The homomorphism mentioned there corresponds to the substitution homomorphism in the commutative case—see, for example, [Wae03, Page 45] or [Jac85, Theorem 2.10]—where the condition on the element ξ is void since $\sigma = \mathrm{id}$, $\vartheta = 0$ and A as well as the image $\psi(A)$ of A in S are commutative.

Theorem 3.7 (Universal property/[MR01, § 1.2.5])**.** *Let A be a ring with endomorphism $\sigma\colon A \to A$ and σ-derivation $\vartheta\colon A \to A$. Let S be another ring, $\psi\colon A \to S$ and $\xi \in S$ such that*

$$\xi\psi(a) = \psi(\sigma(a))\xi + \psi(\vartheta(a))$$

for all $a \in A$. Then there exists a unique ring homomorphism $\chi\colon A[\partial;\sigma,\vartheta] \to S$ extending ψ such that $\chi(\partial) = \xi$ and the diagram



is commutative.

An ideal $I \trianglelefteq A$ of A is called an *σ-ϑ-ideal*—or just ϑ-ideal if $\sigma = \mathrm{id}$—if for all $a \in I$ we have $\sigma(a) \in I$ and $\vartheta(a) \in A$. Using the commutation rule (3.1), it is easy to see that the ideal which is generated by I in $A[\partial;\sigma,\vartheta]$ consists just of the set of all Ore polynomials with coefficients from I. This is analogous to the commutative case as the following result is—where again the conditions on I trivially hold. See, for example, [Vet02, Satz 7.10].

Corollary 3.8. *Let A be a ring with endomorphism $\sigma\colon A \to A$ and σ-derivation $\vartheta\colon A \to A$. Let $I \subseteq A$ be a (two-sided) σ-ϑ-ideal, that is, an ideal such that*

$$\sigma(I) \subseteq I \qquad \text{and} \qquad \vartheta(I) \subseteq I.$$

Then

$$(A/I)[\tilde{\partial};\tilde{\sigma},\tilde{\vartheta}] \cong A[\partial;\sigma,\vartheta]/(I)$$

where $\tilde{\sigma}$ and $\tilde{\vartheta}$ are the homomorphism and $\tilde{\sigma}$-derivation induced by σ and ϑ and (I) is the ideal generated by I in $A[\partial;\sigma,\vartheta]$.

Proof. Since I is two-sided, A/I is a ring. Let $\pi\colon A \to A/I$ be the canonical homomorphism. The induced homomorphism $\tilde{\sigma}\colon A/I \to A/I$ is defined as $\tilde{\sigma}(\pi(a)) = \pi(\sigma(a))$ for all $a \in A$. This is well-defined since $a - b \in I$ implies $\sigma(a-b) \in \sigma(I) \subseteq I$ and thus $0 = \pi(\sigma(a) - \sigma(b)) = \pi(\sigma(a)) - \pi(\sigma(b))$ for all $b \in A$. Analogously, we prove that $\tilde{\vartheta}(\pi(a)) = \pi(\vartheta(a))$ yields a well-defined map of A/I. We have

$$\begin{aligned}\tilde{\vartheta}(\pi(a)\pi(b)) = \tilde{\vartheta}(\pi(ab)) = \pi(\vartheta(ab)) &= \pi(\sigma(a)\vartheta(b) + \vartheta(a)b) \\ &= \pi(\sigma(a))\pi(\vartheta(b)) + \pi(\vartheta(a))\pi(b) = \tilde{\sigma}(\pi(a))\tilde{\vartheta}(\pi(b)) + \tilde{\vartheta}(\pi(a))\pi(b)\end{aligned}$$

for all a and $b \in A$ meaning that $\tilde{\vartheta}$ is a $\tilde{\sigma}$-derivation. Thus, the ring $(A/I)[\tilde{\delta};\tilde{\sigma},\tilde{\vartheta}]$ exists.

For all $a \in A$ is

$$\tilde{\partial}\pi(a) = \tilde{\sigma}(\pi(a))\tilde{\partial} + \tilde{\vartheta}(\pi(a)) = \pi(\sigma(a))\tilde{\partial} + \pi(\vartheta(a)).$$

Thus, by the universal property 3.7 there must be a ring homomorphism $\chi\colon A[\partial;\sigma,\vartheta] \to (A/I)[\tilde{\partial};\tilde{\sigma},\tilde{\vartheta}]$. Its kernel consists of all Ore polynomials in $A[\partial;\sigma,\vartheta]$ with all coefficients being in I. This is precisely the ideal (I) generated by I in $A[\partial;\sigma,\vartheta]$. Thus, by the homomorphism theorem for rings—confer, for example, [Coh00, Theorem 1.21]—the claim follows. □

3.5 Rings of fractions

In the application part we will need to consider localisations of Ore polynomial rings. A general theory for fractions in non-commutative domains was given by [Ore31]—see also [Coh61] or [Coh00, Section 5.1]. In this thesis, we are going to use the formulæ from [Jež96], which includes also a section about derivatives of fractions. This will be needed below in Section 8.2 in order to define iterated Ore polynomial extensions including fractions.

Just as in the commutative theory, localisations over a non-commutative ring A are represented as pairs of a denominator and a numerator, that is, the pair $(a,b) \in A \times A$ represents the element $b^{-1}a$ in the—yet to be defined—ring of fractions over A. Having the denominator on the left hand side is referred to as *left fractions*. Analogously, we could represent fraction with the denominators written on the right hand side instead, that is, we could consider *right fractions*. This is possible as well under similar conditions as in the left case. Below, we will only list the formulæ for left fractions, though. For the other case, we refer the reader to [Jež96].

Instead of considering merely multiplicative subsets for the denominators as in the commutative case, we need to be more restrictive in the non-commutative case. The problem is that to resolve products like $b^{-1}a \cdot d^{-1}c$ we need to commute a and c^{-1}, that is, we need a fraction $q^{-1}p$ such that $ac^{-1} = q^{-1}p$ or, denoted differently, we need a denominator q and an arbitrary element p such that

$$qa = pc.$$

This consideration motives the following definition: A subset $S \subseteq A$ is called a *left Ore set* if

1. $1 \in S$ and S is closed under multiplication,
2. S does not contain left or right zero divisors, and
3. for all $s \in S$ and $a \in A$ we have $Rs \cap Sa \neq \emptyset$.

See also [Jež96, Page 87] or [Coh00, Page 177] for the right Ore set case.

Using the algorithm for least common multiples from, for example, [BP96], we see that for every Ore polynomial ring $R = K[\partial;\sigma,\vartheta]$ over a field K and with automorphism $\sigma\colon K \to K$ and σ-derivation $\vartheta\colon K \to K$ the set $S = R \setminus \{0\}$ is a left Ore set. See also [Coh03, Proposition 7.3.4]. But not every multiplicative subset of R has this property, as the following example shows.

Example 3.9. Let $A = \mathbb{Q}(t)$, the field of rational functions in the indeterminate t, and let σ be the substitution $t \mapsto t-1$. Consider $R = A[\partial;\sigma,0]$ and $\pi = \partial + t$. We prove by induction, that the powers of π are not a left Ore set in R. That is, we have to prove that there is $a \in R$ such that there exists no $n \geq 0$ and no $f \in R$ with

$$\pi^n a = f\pi,$$

or, put differently, we have to prove that π is not a right divisor of $\pi^n a$ for all $n \geq 0$. We choose $a = t$ and proceed using induction. Obviously, π cannot divide t because of the degree. Assume that π does not divide $\pi^n t$ for some $n \geq 0$. Since

$$\pi^{n+1}t = \pi^n(\partial t + t^2) = \pi^n\big((t-1)\partial + t^2\big) = \pi^n\big((t-1)(\partial+t) + t\big) = \pi^n(t-1)\pi + \pi^n t,$$

we see that if π divided $\pi^{n+1}t$ from the right, then π also divided $\pi^n t$ from the right contradicting our assumption. Thus, $S = \{\pi^n \mid n \geq 0\}$ cannot be a left Ore set of R.

It can be proved that for any left Ore set $S \subseteq A$ we construct a ring $S^{-1}A$ such that every element in $S^{-1}A$ can be expressed as fraction $s^{-1}a$ with $s \in S$ and $a \in A$. Moreover, the map $a \mapsto 1^{-1}a$ from A to $S^{-1}A$ is an embedding, that is, an injective homomorphism and all images of elements in S are invertible. See, for example, [Jež96] of [Coh00, Theorem 5.2] for the dual case.

In particular doing for $R = K[\partial;\sigma,\vartheta]$ as above the *full ring of fractions* $(R \setminus \{0\})^{-1}R$ exist. We will usually denote it just by $K(\partial;\sigma,\vartheta)$. By [Coh00, Proposition 5.3]—which can be formulated and proved for left fractions as well—we can bring every finite set of fractions to a common denominator.

We will here just cite the formulæ for addition, multiplication and—in the case that A has a derivation $\vartheta\colon A \to A$—derivation of fractions. Let $b^{-1}a$ and $d^{-1}c \in S^{-1}A$ be given. Then by [Jež96, Equation (40)] we have

$$b^{-1}a + d^{-1}c = (\tilde{d}b)^{-1}(\tilde{d}a + \tilde{b}c)$$

where $\tilde{b}$ and $\tilde{d} \in S$ satisfy $\tilde{b}d = \tilde{d}b$, by [Jež96, Equation (41)]

$$b^{-1}a \cdot d^{-1}c = (\tilde{d}b)^{-1}(\tilde{a}c)$$

where $\tilde{d}a = \tilde{a}d$, and finally using [Jež96, Theorem 13] with $\tilde{\vartheta}\colon S^{-1}A \to S^{-1}A$ defined by

$$\tilde{\vartheta}(b^{-1}a) = (\tilde{b}b)^{-1}(\tilde{b}\vartheta(a) - xa)$$

where $\tilde{b}\vartheta(b) = xb$ we obtain a derivative on $S^{-1}A$ which extends ϑ.

4

Extended example: Integro-differential operators

4.1 Integro-differential operators

As an extended example we would like to show how integro-differential operators may be modelled by Ore polynomials. Integro-differential operators arise from the work in [RR08] based itself on [Ros05]. Just as we have argued that differential operators may be modelled algebraically in Section 3.2, integro-differential operators are a way to model operators that are build from a derviation as well as an antiderivation, commonly called an integral. They have applications in treating *boundary value problems* in a symbolic fashion. See [RRTB11, Section 5] for this, where integro-differential operators are used to achieve a factorization of boundary value problems into smaller parts which then can be attacked separately.

In this chapter, we will discuss our joint with Georg Regensburger and Markus Rosenkranz work in [RRM09] where we examined how to model integro-differential operators as Ore polynomials.[1]

In this whole chapter, all fields will be of characteristic zero. We start with the definition of an integro-differential algebra. This is the base point for our integro-differential operators as it will serve both as coefficient domain and also as target for possible actions of integro-differential operators.

Definition 4.1 (Integro-differential algebra, [RRM09, Definition 1])**.** Let $\mathscr{F}$ be a commutative algebra over a field K. Assume that there are two maps $\vartheta\colon \mathscr{F} \to \mathscr{F}$ and $\int\colon \mathscr{F} \to \mathscr{F}$ such that ϑ is a derivation, $\int$ is a K-linear right-inverse of ϑ, that is, $\vartheta\int = \mathrm{id}$, and the *differential Baxter axiom* holds, that is, for all f and $g \in \mathscr{F}$ it is

$$\int\big(\vartheta(f)\big)\int\big(\vartheta(g)\big) = \int\big(\vartheta(f)\big)g + f\int\big(\vartheta(g)\big) - \int\big(\vartheta(fg)\big).$$

Then, the triple $(\mathscr{F}, \vartheta, \int)$ is called a *integro-differential algebra*. The map $\int$ is called an *integral* for ϑ.

[1] In [RRM09] the term "skew polynomials" was used for Ore polynomials.

Usually the integral $\mathfrak{b}$ and derivation ϑ are denoted just by the symbols $\int$ and ∂ known from calculus. Denoting the derivation by the even more common prime, the differential Baxter axiom would be denoted as

$$\int f' \cdot \int g' = \int f' \cdot g + f \cdot \int g' - \int (fg)'.$$

We will here, however, refrain from this notation since we would like to reserve the symbols ∂ and $\int$ for the indeterminates of an integro-differential operator ring below. In this, we differ from [RRM09] and [RRTB11].

The most prominent example of an integro-differential algebra are the smooth functions $\mathscr{F} = \mathrm{C}^\infty(\mathbb{R})$ over the reals together with the usual derivation $\vartheta = d/dx$ and the corresponding integral $\mathfrak{b} = f \mapsto \int_0^x f(\xi)\,d\xi$. Here, the integral is indeed only a one-sided inverse of the derivation since in general

$$\mathfrak{b}\vartheta(f) = \int_0^x f'(\xi)\,d\xi = f(\xi)\Big|_{\xi=0}^{\xi=x} = f(x) - f(0) \neq f(x)$$

for a function $f \in \mathrm{C}^\infty(\mathbb{R})$. Thus, here we have $\mathfrak{b}\vartheta \neq \mathrm{id}$.

Another—more algebraic—example which we will consider below are the polynomials $K[x]$ over a commutative field K of characteristic zero together with the formal derivation $\vartheta = d/dx$ with respect to x and $\mathfrak{b}$ given by $x^n \mapsto \frac{1}{n+1}x^{n+1}$. This example shows also that $\mathfrak{b}$ needs not to be uniquely determined since for every $c \in K$ the map $\mathfrak{b}_c$ defined by $x^n \mapsto \frac{1}{n+1}(x^{n+1} - c^{n+1})$ yields a right-inverse of ϑ which fulfills the differential Baxter axiom.

Substituting $\mathfrak{b}(f)$ for f and $\mathfrak{b}(g)$ for g in the differential Baxter axiom and using that $\mathfrak{b}$ is a right-inverse of ϑ and the Leibniz rule as well as the linearity of $\mathfrak{b}$ yields

$$\begin{aligned}\mathfrak{b}(f)\mathfrak{b}(g) &= \mathfrak{b}\big(\vartheta(\mathfrak{b}(f))\big)\mathfrak{b}\big(\vartheta(\mathfrak{b}(g))\big) = \mathfrak{b}\big(\vartheta(\mathfrak{b}(f))\big)\mathfrak{b}(g) + \mathfrak{b}(f)\mathfrak{b}\big(\vartheta(\mathfrak{b}(g))\big) - \mathfrak{b}\big(\vartheta(\mathfrak{b}(f)\mathfrak{b}(g))\big)\\ &= \mathfrak{b}(f)\mathfrak{b}(g) + \mathfrak{b}(f)\mathfrak{b}(g) - \mathfrak{b}\big(\mathfrak{b}(f)\vartheta(\mathfrak{b}(g)) + \vartheta(\mathfrak{b}(f))\mathfrak{b}(g)\big) = 2\mathfrak{b}(f)\mathfrak{b}(g) - \mathfrak{b}\big(\mathfrak{b}(f)g\big) - \mathfrak{b}\big(f\mathfrak{b}(g)\big)\end{aligned}$$

which is equivalent to

$$\mathfrak{b}(f)\mathfrak{b}(g) = \mathfrak{b}\big(\mathfrak{b}(f)g\big) + \mathfrak{b}\big(f\mathfrak{b}(g)\big).$$

The last rule is generally known as *integration by parts*—as can be easily seen from the more familiar notation $F \cdot G = \int FG' + \int F'G$ where $F = \int f$ and $G = \int g$. The above equation is not in general equivalent to the differential Baxter axiom by itself. See [RRTB11, Proposition 7] for the conditions necessary in order to define an integro-differential algebra using integration by parts. A description of the properties of an integral purely by itself is the *pure Baxter axiom*

$$\mathfrak{b}(f)\mathfrak{b}(g) = \mathfrak{b}(f\mathfrak{b}(g)) + \mathfrak{b}(g\mathfrak{b}(f))$$

which can be found in [RRTB11, Definition 8]—in [RRTB11, Proposition 10] it is shown that it holds in an integro-differential algebra.

Since the integral is only a right inverse—also called a *section*—of the derivation, the map $\varepsilon = \mathfrak{b}\vartheta - \mathrm{id}$ is in general not zero. In [RRTB11, Section 3] it is proven that ε is a multiplicative projector. We call ε an *evaluation*. This name is justified by the facts that in the standard examples $\mathscr{F} = \mathrm{C}^\infty(\mathbb{R})$ and $\mathscr{F} = K[x]$ a function (or polynomial function) f is evaluated to $\varepsilon(f) = f(c)$ where $c \in K$ is the lower limit of the integration. Thus, ε is a K-linear map from $\mathscr{F}$ to K, a so-called *character*. It makes it possible to formulate *initial value problems*—see also the explanation just behind [RRTB11, Corollary 18].

In [RRTB11]—and also in the introductory part of [RRM09]—it is usually assumed that one is given other characters apart from ε. Since they do not occur in the integro-differential Weyl algebra we will be concentrating on below, we do not give any details here.

In [RRM09] integro-differential operators have been introduced in two different but equivalent ways. The first involves considering an integro-differential algebra $(\mathscr{F}, \vartheta, \rlap{\,/}\int)$ and considering the free algebra $\mathscr{F}\langle\partial, \int\rangle$ over $\mathscr{F}$ in the indeterminates ∂ and $\int$. Then, relations which model the compositions of integral operators and differential operators are identified and combined into a rewriting system which allows one to compute normal forms in $\mathscr{F}\langle\partial, \int\rangle$. This whole approach is described in great detail in [RRTB11]. The reference also outlines a THEOREM∀ implementation of this with the complete code being available online.

The other approach—which we will describe now—models the integro-differential operators in three separate parts: Differential operators, integral operators and boundary operators. This is motivated by [RRTB11, Proposition 26] where it is shown that every integro-differential operator—as defined there—can be written uniquely as a sum of these three types of operators.

In [RRM09, Section 3] we took this sum decomposition as a definition. We will outline this here for the convenience of the reader. See also [KRR11] for a more detailed description and an implementation of integro-differential operators in MAPLE using this approach. This reference contains applications of integro-differential operators to boundary value problems as well. Also here, the package is available online.

Let first $(\mathscr{F}, \vartheta, \rlap{\,/}\int)$ be an integro-differential algebra over K. We start by defining the *differential operators* by simply setting $\mathscr{F}[\partial] = \mathscr{F}[\partial; \mathrm{id}, \vartheta]$ as in Section 3.2.

Next, we define integral operators $\mathscr{F}[\int]$. For this we need to choose a basis $\mathfrak{B}$ of $\mathscr{F}$ as an K-space. The *integral operators* are then defined as the free $\mathscr{F}$-module over the elements $\int b$ where $b \in \mathfrak{B}$. Note that $\int b$ is considered as a purely symbolic value. We will also write non-basis elements v on the right hand side of $\int$. This is to be understood as $\int v = \sum_{b \in \mathfrak{B}} c_b \int b$ where $v = \sum_{b \in \mathfrak{B}} c_b b$. This models the K-linearity of the integral which is ultimately also the reason for choosing a basis here as right hand sides. The multiplication in $\mathscr{F}$ is based on the equation

$$\int b \cdot \int = \rlap{\,/}\int(b) \int - \int \rlap{\,/}\int(b) \tag{4.1}$$

where $b \in \mathfrak{B}$ and $\int \rlap{\,/}\int(b)$ has to be represented as described above. This models the integration by parts rule. The multiplication can be extended to all of $\mathscr{F}[\int]$ using associativity and distributivity.

Finally, we need to define the *boundary operators* $\mathscr{F}[\mathrm{E}]$ that represent those integro-differential operators containing the evaluation $\varepsilon = \rlap{\,/}\int\vartheta - 1$. The set $\mathscr{F}[\mathrm{E}]$ is defined to be the left $\mathscr{F}$-module spanned by the (again purely symbolic) elements $\mathrm{E}\partial^j$ for $j \geq 0$. They model evalutation of a derivative of a function. The product in $\mathscr{F}$ is obtained from

$$\mathrm{E}\partial^i \cdot f\,\mathrm{E}\partial^j = \varepsilon\big(\vartheta^i(f)\big)\mathrm{E}\partial^j$$

with i and $j \geq 0$—which is motivated by the Leibniz rule and the fact that ε is a projection. Again, distributivity and associativity are used to expand this to all of $\mathscr{F}[\mathrm{E}]$.

Now, we finally may define the *integro-differential operators* as the direct sum

$$\mathscr{F}[\partial, \textstyle\int] = \mathscr{F}[\partial] \oplus \mathscr{F}[\textstyle\int] \oplus \mathscr{F}[\mathrm{E}]. \tag{4.2}$$

It remains to define the products of basis elements from the different parts with each other. In the following let $b \in \mathfrak{B}$, $f \in \mathscr{F}$ and i and $j \geq 0$. Then we have for products of differential and integral

operators

$$\partial \cdot f \int b = fb + \vartheta(f)\int b \qquad \text{and} \qquad \int b \cdot f \partial = bf - \int \vartheta(bf) - \varepsilon(bf)\mathrm{E}.$$

In order to multiply differential and boundary operators we need the equations

$$\partial^i \cdot f \mathrm{E} \partial^j = \vartheta^i(f)\mathrm{E}\partial^j \qquad \text{and} \qquad \mathrm{E}\partial^i \cdot f \partial^j = \sum_{k=0}^{i} \varepsilon(f_k)\mathrm{E}\partial^{j+k}$$

where $f_0, \ldots, f_i \in \mathscr{F}$ are the coefficients of $\partial^i f = \sum_{k=0}^{i} f_k \partial^k$. Finally, to multiply integral and boundary operators we use

$$\int b \cdot f \mathrm{E} \partial^i = b(bf)\mathrm{E}\partial^i \qquad \text{and} \qquad \mathrm{E}\partial^i \cdot f \int b = \sum_{k=0}^{i-1} \varepsilon(g_k)\mathrm{E}\partial^k$$

where $\sum_{k=1}^{i} f_k \partial^{k-1} b = \sum_{k=0}^{i-1} g_k \partial^k$ in $\mathscr{F}[\partial]$ with $f_0, \ldots, f_k$ as before.

It is not difficult but tedious to prove that these rules make $\mathscr{F}[\partial, \int]$ into a ring. (The unit element 1 is contained in the first direct summand $\mathscr{F}[\partial]$.) It yields exactly the relations of the approach in [RRTB11].

The last two equations show that multiplying anything with a boundary operators from either side will result in a boundary operator again. Hence, boundary operators form a two-sided ideal in the ring $\mathscr{F}[\partial, \int]$ that we labeled *evaluation ideal* in [RRM09].

4.2 Modelling integro-differential operators with Ore polynomials

In this chapter, we will concentrate on the algebra $K[x]$ with the standard derivation given by $x \mapsto 1$ and the integration defined via $1 \mapsto x$. Note, that by [Kap76, I.2 Examples 4], prescribing a derivative for x will fix the derivation on all of $K[x]$ uniquely. Also, note fixing $b(1) = x$ actually fixes the integral of x^n to $b(x^n) = \frac{1}{n+1}x^{n+1}$ for every $n \geq 0$: Taking $b(1) = x$ as the base case, induction using the pure Baxter axiom yields

$$\frac{1}{n+1}x^{n+2} = b(1)b(x^n) = b\big(1b(x^n)\big) + b\big(x^n b(1)\big) = b\big(\tfrac{1}{n}x^{n+1}\big) + b(x^{n+1}) = \frac{n+2}{n+1}b(x^{n+1})$$

and thus $b(x^{n+1}) = \frac{1}{n+2}x^{n+2}$.

This setting will lead to an integro-differential algebra that is analogue to the Weyl algebra $\mathrm{A}_1(\partial)$ in the differential case.

For this ring we need only a small subset of the multiplication rules of the integro-differential operators defined in the last section that are sufficient generate all the others. This will be proven in Theorem 4.23. The initial multiplication rules are just

$$\partial x = x\partial + 1, \qquad \int^2 = x\int - \int x \qquad \text{and} \qquad \partial \int = 1.$$

Here, the first rule is the commutation rule in $K[x][\partial]$; the second rule is Equation (4.1) for $b = 1$; and the last rule follows from the cross multiplication of $K[x][\partial]$ and $K[x][\int]$. The boundary operators will in this setting be defined purely in terms of ∂ and $\int$.

The straight-forward approach to implement these rules in an Ore polynomial ring would be to start with the already known Weyl algebra $A_1(\partial) = K[x][\partial; \mathrm{id}, d/dx]$ and extend this by a second variable $\int$ with a corresponding derviation. This however fails since the Baxter axiom

$$\int x = -\int^2 + x\int$$

violates the degree rule: Considering the degree in $\int$, we have $\deg \int = 1$ and $\deg x = 0$ and are thus expecting $\deg \int x = 1$; but on the right hand side we encounter a polynomial of second degree in $\int$.

The way to overcome this problem is to note that while the degree in $\int$ in the above equation is different on the left and on the right hand side, the degree in x is the same. The same is true also for the Leibniz rule $\partial x = x\partial + 1$. This observation leads to the following attempt to define the integro-differential Weyl algebra: First, construct the ring of integro-differential operators $K[\partial, \int]$ with constant coefficients; and second, use this ring as the coefficient domain for an Ore extension $K[\partial, \int][x; \mathrm{id}, \vartheta]$ in the variable x with a fittingly chosen derivation ϑ of $K[\partial, \int]$.

Integro-differential operators with constant coefficients

We start by examining the ring of integro-differential operators with constant coefficients. This corresponds roughly to the fourth section of [RRM09]. Let K be a (commutative) field. We want to introduce two variables ∂ and $\int$ such that $\int$ is a right inverse of ∂. For this we consider the free algebra $K\langle D, L\rangle$. Let $(DL - 1) \trianglelefteq K\langle D, L\rangle$ denote the two-sided ideal that is generated by $DL - 1$.

Definition 4.2 ([RRM09, Definition 2])**.** The algebra $K\langle \partial, \int\rangle$ is the quotient $K\langle D, L\rangle/(DL - 1)$ where ∂ denotes the residue class of D and $\int$ denotes that of L.

When we will add x below, we need to fulfil the relations

$$x\partial = \partial x - 1 \qquad \text{and} \qquad x\int = \int x + \int^2.$$

If we are to regard these identities as instances of the commutation rule, then the derivation $\vartheta\colon K\langle \partial, \int\rangle \to K\langle \partial, \int\rangle$ must fulfil

$$\vartheta(\partial) = -1 \qquad \text{and} \qquad \vartheta(\int) = \int^2.$$

We can define a derivation $\tilde{\vartheta}\colon K\langle D, L\rangle \to K\langle D, L\rangle$ by $\tilde{\vartheta}(D) = -1$ and $\tilde{\vartheta}(L) = L^2$—see, for example, [Coh69] or [BD78]. Because of

$$\tilde{\vartheta}(DL - 1) = \tilde{\vartheta}(D)L + D\tilde{\vartheta}(L) = -L + DL^2 = (DL - 1)L$$

the ideal $(DL - 1)$ is a differential ideal and $\tilde{\vartheta}$ induces a well-defined derivation $\vartheta\colon K\langle \partial, \int\rangle \to K\langle \partial, \int\rangle$ with the relations we were looking for.

Algebras with one-sided inverses have already been studied in [Jac50], one consequence of this paper being that $K\langle \partial, \int\rangle$ is neither (left or right) Noetherian nor (left or right) Artinian. Later, [Ger00] extended this results describing the right modules and derivations over $K\langle \partial, \int\rangle$. In the notation of [Ger00], we have $\vartheta = -\partial_0$.

As K-vector space, $K\langle \partial, \int\rangle$ is generated by all monomials of the form $\int^i \partial^j$ since every monomial reduces to this form using the relation $\partial\int = 1$. We follow [Jac50] and define for i and $j \geq 0$

$$\mathrm{E} = 1 - \int\partial \qquad \text{and} \qquad e_{ij} = \int^i \mathrm{E}\partial^j.$$

In particular, it is $\mathrm{E} = e_{00}$. As before, E corresponds to an evaluation. Thus, the equation

$$\mathrm{E}^2 = 1 - \int\partial + \int\partial - \int\partial\int\partial = 1 - \int\partial = \mathrm{E}$$

can be understood in such a way that evaluating a function twice is the same as evaluating it only once, since the result of the first evaluation will be a constant which always evaluates to itself. Since

$$\partial\mathrm{E} = \partial - \partial\int\partial = \partial - \partial = 0, \qquad \text{and} \qquad \mathrm{E}\int = \int - \int\partial\int = 0,$$

$K\langle\partial, \int\rangle$ has zero divisors. Confer also [Jac50] and [Ger00]. Note, that the first equation can be interpreted in a way that deriving a function that is evaluated to a constant yields zero; while the second equation means that the integral from c to c yields zero as well. Extending the equations derived above we obtain for all i, j, s and $t \geq 0$ that

$$e_{ij}e_{st} = \int^i \mathrm{E}\partial^j \int^s \mathrm{E}\partial^t = \begin{cases} \int^i \mathrm{E}\partial^{j-s}\mathrm{E}\partial^t, & \text{if } j > s \\ \int^i \mathrm{E}\int^{s-j}\mathrm{E}\partial^t, & \text{if } s > j \\ \int^i \mathrm{E}\mathrm{E}\partial^t, & \text{otherwise} \end{cases}.$$

Since for $j \neq s$ the term simplifies to 0 and $\mathrm{E}^2 = \mathrm{E}$, we are left with the equation

$$e_{ij}e_{st} = \delta_{js}e_{it}$$

where δ denotes the Kronecker symbol. This means that the e_{ij} behave like *matrix units*—see [Jac50] or [Coh85, Section 0.1]. Further identities involving the e_{ij} are

$$\int e_{ij} = e_{i+1,j} \qquad \text{and} \qquad \partial e_{ij} = \begin{cases} e_{i-1,j}, & \text{if } i \geq 1, \\ 0, & \text{if } i = 0 \end{cases} \tag{4.3}$$

as well as

$$e_{ij}\partial = e_{i,j+1} \qquad \text{and} \qquad e_{ij}\int = \begin{cases} e_{i,j-1}, & \text{if } j \geq 1, \\ 0, & \text{if } j = 0 \end{cases}. \tag{4.4}$$

The latter equations show that the two-sided ideal (E) generated by E has the e_{ij} as a K-basis. Hereby, the linear indepedence can be proven by expanding the equation

$$e_{ij} = \int^i \mathrm{E}\partial^j = \int^i (1 - \int\partial)\partial^j = \int^i \partial^j - \int^{i+1}\partial^{j+1}.$$

This allows to translate any relation of the e_{ij} into one of the K-basis $\int^s\partial^t$.

The last equation can be rewritten as

$$\int^{i+1}\partial^{j+1} = -e_{ij} + \int^i \partial^j.$$

Applying this recursively yields a way of expressing every polynomial $\int^i\partial^j$ in terms of the e_{st} and pure powers of either ∂ or $\int$. More precisely, we obtain

$$\int^i\partial^j = \begin{cases} \int^{i-j} - \sum_{k=1}^{j} e_{i-k,j-k}, & \text{if } i \geq j \\ \partial^{j-i} - \sum_{k=1}^{i} e_{i-k,j-k}, & \text{if } j \geq i \end{cases}$$

for the conversion between the standard basis and the e_{ij}.

Example 4.3. Consider the operator

$$f = \int\partial^2 + \int\partial + \partial^2.$$

Using the formula, we see that $\int\partial = 1 - \mathrm{E}$ and $\int\partial^2 = \partial - e_{0,1}$ and thus

$$f = 1 + \partial + \partial^2 - \mathrm{E} - e_{0,1}.$$

In total, this yields already half of the proof of the following theorem which will serve as a first step of unifying $K\langle\partial,\int\rangle$ with the integro-differential operators in Equation (4.2).

Theorem 4.4 ([RRM09, Proposition 3])**.** *We have the decomposition*

$$K\langle\partial,\int\rangle = K[\partial] \oplus K[\int]\int \oplus (\mathrm{E})$$

as direct sum of K-vector spaces where $K[\partial]$ is a differential subring of $K\langle\partial,\int\rangle$ with respect to ϑ, $K[\int]\int$ is a differential subring without unit and (E) is a differential ideal.

Proof. We have already seen that $K\langle\partial,\int\rangle$ may be decomposed as direct sum. It remains to prove the statements about the structure of the sumands. First, since ∂ commutes with the elements in K, we see that $K[\partial]$ is actually just a commutative polynomial ring. Since $\vartheta(\partial) = -1 \in K[\partial]$, we obtain $\vartheta(K[\partial]) \subseteq K[\partial]$. Analogously, since for $p\int \in K[\int]\int$ we have $\vartheta(p\int) = \vartheta(p)\int + p\int^2 \in K[\int]\int$ we see that also $K[\int]\int$ is closed under ϑ. Of course is $K[\int]\int$ as (two-sided) ideal of the commutative polynomial ring $K[\int]$ closed under addition, multiplication and additive inverses. Finally, we have

$$\vartheta(\mathrm{E}) = -\vartheta(\int\partial) = -\big(\int\vartheta(\partial) + \vartheta(\int)\partial\big) = -(-\int + \int^2\partial) = \int(1 - \int\partial) = \int\mathrm{E} \in (\mathrm{E}) \tag{4.5}$$

and thus $\vartheta(e_{ij}) = \vartheta(\int^i)\mathrm{E}\partial^j + \int^i\mathrm{E}\vartheta(\partial^j) + \int^i\mathrm{E}\vartheta(\partial^j) \in (\mathrm{E})$ for all i and $j \geq 0$. This implies that also (E) is closed under ϑ. □

The ideal (E) that has been mentioned in the preceeding theorem has an interesting property which can also be found in [Jac50].

Lemma 4.5 ([RRM09, Lemma 4])**.** *Every non-zero ideal in $K\langle\partial,\int\rangle$ contains (E).*

Proof. Let $I \trianglelefteq K\langle\partial,\int\rangle$ be any ideal in $K\langle\partial,\int\rangle$, and assume that there exists an element $f \neq 0$ such that $f \in I$. We want to prove that $\mathrm{E} \in I$. Using the decomposition of Theorem 4.4, we may write $f = p + q + e$, where $p \in K[\partial]$, $q \in K[\int]\int$ and $e \in (\mathrm{E})$.

Assume first, that $p + q \neq 0$. Multiplying f with a sufficiently high power ∂^k of ∂ we obtain an element $\partial^k f \in I \cap K[\partial]$ since because of $\partial\int = 1$ the terms of q get "shifted" into $\partial^k q \in K[\partial]$ and because of $\partial^{i+1}e_{ij} = 0$ the terms of $\partial^k e$ vanish. Denote now the degree of $\partial^k f$ in ∂ by μ. We may assume that $\partial^k f$ is monic. Then

$$\mathrm{E}\partial^k f\int^\mu = \mathrm{E} \in I$$

since all terms $\mathrm{E}c_j\partial^j$ in $\mathrm{E}\partial^k f$ with $c_j \in K$ and $j < \mu$ upon multiplication with $\int$ from the left become $c_j\mathrm{E}\int^{\mu-j} = 0$ since $\mu - j \geq 1$. We obtain $(\mathrm{E}) \subseteq I$.

If $p + q = 0$, then we must have $e \neq 0$. Choose i maximal such that e_{ij} appears in e with a non-zero coefficient. Then multiplying with ∂^i from the left yields $\partial^i e = c_0 e_{00} + \ldots + c_\nu e_{0\nu}$ for some $\nu \geq 0$ where $c_0, \ldots, c_\nu \in K$. Assume that $c_\nu \neq 0$. Then $\partial^i e\int^\nu = c_\nu\mathrm{E} \in I$ and thus $(\mathrm{E}) \subseteq I$ also in this case. □

The idea of the proof is illustrated by the following example.

Example 4.6. Consider the operator

$$f = \partial^2 + \int\partial + \int^2 = \partial^2 + 1 + \int^2 - \mathrm{E}.$$

Multiplying f by ∂^2 from the left yields

$$\partial^2 f = \partial^2(\partial^2 + 1 + \int^2 - \mathrm{E}) = \partial^4 + \partial^2 + 1.$$

Multiplication with E from the left leads to

$$\mathrm{E}(\partial^2 f) = \mathrm{E}(\partial^4 + \partial^2 + 1) = e_{0,4} + e_{0,2} + \mathrm{E},$$

and finally multiplying by $\int^4$ from the right yields

$$\mathrm{E}(\partial^2 f)\int^4 = (e_{0,4} + e_{0,2} + \mathrm{E})\int^4 = \mathrm{E}$$

using the identities in Equation 4.4.

Things get even more special if we consider ϑ-ideals. In fact, the choice of them in $K\langle\partial,\int\rangle$ is pretty limited.

Theorem 4.7 ([RRM09, Proposition 5])**.** *The only (two-sided) ϑ-ideals in $K\langle\partial,\int\rangle$ are $\{0\}$, (E) and $K\langle\partial,\int\rangle$ itself.*

Proof. We have seen in Lemma 4.5 that (E) is a ϑ-ideal and obviously the other two are ϑ-ideals as well.

Let now a ϑ-ideal I be given and assume that $I \neq \{0\}$ and $I \neq (\mathrm{E})$. By Theorem 4.4, this means that there is an element $f = p + q + e \in I$ with $p \in K[\partial]$, $q \in K[\int]\int$ and $e \in (\mathrm{E})$ where $p + q \neq 0$. Analogously to the proof of Lemma 4.5 we can find some $k \geq 0$ such that $\partial^k f \in K[\partial]$. We must have $\partial^k f \neq 0$—since $p + q \neq 0$—and thus $m = \deg \partial^k f \geq 0$. Because ϑ acts on $K[\partial]$ as $d/d\partial$, applying ϑ^m just yields $\vartheta^m(\partial^k f) = m!\operatorname{lc}(\partial^k f) \in K \setminus \{0\}$ which must also be in I since it is a ϑ-ideal. Thus, there is a unit in I and we obtain $I = K\langle\partial,\int\rangle$. □

In an integro-differential algebra the integral is only a right-inverse of the derivation. An interesting question is thus: What happens if we make it a two-sided inverse, that is, enforce the relation $\int\partial - 1 = \mathrm{E} = 0$? Intuitively this would turn $K\langle\partial,\int\rangle$ into some kind of Laurent polynomial ring. And indeed, this is just the result of the following theorem.

Theorem 4.8 ([RRM09, Proposition 6])**.** *The map*

$$\frac{K\langle\partial,\int\rangle}{(\mathrm{E})} \xrightarrow{\sim} K[Z,Z^{-1}]$$

defined by $\partial + (\mathrm{E}) \mapsto Z$ and $\int + (\mathrm{E}) \mapsto Z^{-1}$ is a differential ring isomorphism with respect to ϑ and $-d/dZ$.

Proof. We regard both $K\langle\partial,\int\rangle$ and $K[Z,Z^{-1}]$ as K-spaces. The linear map φ which maps the basis element $\int^i\partial^j$ with i and $j \geq 0$ of $K\langle\partial,\int\rangle$ to the basis element Z^{j-i} of $K[Z,Z^{-1}]$ is thus well defined. We prove first that φ is also a differential homomorphism. It is sufficient to check this for basis elements. Let i, j, m and $n \geq 0$. Assuming first $m \geq j$, we obtain

$$\varphi(\textstyle\int^i\partial^j \cdot \int^m\partial^n) = \varphi(\int^{i+m-j}\partial^n) = Z^{n-i-m+j} = Z^{j-i}Z^{n-m} = \varphi(\int^i\partial^j)\cdot\varphi(\int^m\partial^n);$$

and analogously for $m \leq j$ we have

$$\varphi(\textstyle\int^i \partial^j \cdot \int^m \partial^n) = \varphi(\int^i \partial^{j-m+n}) = Z^{j-m+n-i} = Z^{j-i} Z^{n-m} = \varphi(\int^i \partial^j) \cdot \varphi(\int^m \partial^n).$$

This proves that φ is a ring homomorphism. Because for all i and $j \geq 0$ we have

$$\begin{aligned}\varphi\big(\vartheta(\textstyle\int^i \partial^j)\big) = \varphi\big(\int^i \vartheta(\partial^j) + \vartheta(\int^i)\partial^j\big) &= \varphi(-j\textstyle\int^i \partial^{j-1} + i\int^{i+1}\partial^j) \\ &= -jZ^{j-1-i} + iZ^{j-i-1} = (i-j)Z^{j-i}\textstyle\int^i \partial^j - 1 = -\dfrac{d}{dZ}Z^{j-i} = -\dfrac{d}{dZ}\varphi(\int^i \partial^j),\end{aligned}$$

we see that φ is even a differential homomorphism.

By [Kap76, Theorem 1.2], this means that the kernel of φ must be a differential ideal which by Theorem 4.7 leaves only three choices. We can rule out $\ker\varphi = K$ since $\varphi(1) = 1 \neq 0$ and also $\ker\varphi = \{0\}$ since

$$\varphi(\mathrm{E}) = \varphi(\textstyle\int\partial - 1) = 1 - 1 = 0.$$

Thus, we conclude that $\ker\varphi = (\mathrm{E})$. Furthermore, φ is surjective since each Z^a is either the image of ∂^a if $a \geq 0$ or that of $\int^{-a}$ otherwise. Again from [Kap76, Theorem 1.2] we obtain that $K\langle\partial, \textstyle\int\rangle/(\mathrm{E})$ is differentially isomorphic to the image $K[Z, Z^{-1}]$ □

Using the previous theorem together with the third isomorphism theorem—confer, for example, [Coh00, Theorem 1.23]—we conclude that there is a one-to-one correspondence between the ideals of $K[Z, Z^{-1}]$ and the non-zero ideals of $K\langle\partial, \textstyle\int\rangle$. Theorem 4.8 leads thus to a complete description of the ideal structure of the integro-differential operators $K\langle\partial, \textstyle\int\rangle$ with constant coefficients. We remark, that the Laurent polynomials $K[Z, Z^{-1}]$ are a principal ideal domain by [BIV89, Theorem 2.18].

Remark 4.9 ([RRM09, Proposition 16])**.** Instead of modelling the derivation in Theorem 4.8 by setting the derivative of Z to -1 which mimicks the derivative of ∂ in $K\langle\partial, \textstyle\int\rangle$, we could also have set it to Z^2 thereby mimicking the derivative of $\int$. Not surprisingly, also this approaches yield a differential isomorphism of rings: It is easy to prove that $\varphi\colon K[Z, Z^{-1}] \to K[Y, Y^{-1}]$ defined by $Z \mapsto Y^{-1}$ is a differential isomomorphism with respect to $-d/dZ$ in $K[Z, Z^{-1}]$ and $Y^2 \cdot d/dY$ in $K[Y, Y^{-1}]$, since

$$Y^2 \frac{d}{dY}\varphi(Z) = Y^2 \frac{d}{dY} Y^{-1} = -\frac{Y^2}{Y^2} = -1 = \varphi(-1) = \varphi\Big(-\frac{d}{dZ}Z\Big).$$

Thus, composition of the isomomorphisms shows that $\partial + (\mathrm{E}) \mapsto Y^{-1}$ and $\textstyle\int + (\mathrm{E}) \mapsto Y$ would be a differential isomomorphism between $K\langle\partial, \textstyle\int\rangle$ and the Laurent polynomials, too.

Integro-differential operators with polynomial coefficients

After investigating the integro-differential operators with constant coefficients, we are now prepared to add the Ore indeterminate x. This leads to the integro-differential Weyl algebra which we study in this section.

Definition 4.10 (Integro-differential Weyl algebra/[RRM09, Definition 7])**.** The *integro-differential Weyl algebra* is defined to be the Ore polynomial ring

$$\mathrm{A}_1(\partial, \textstyle\int) = K\langle\partial, \int\rangle[x; \mathrm{id}, \vartheta]$$

where $K\langle\partial, \textstyle\int\rangle$ and $\vartheta\colon K\langle\partial, \textstyle\int\rangle \to K\langle\partial, \textstyle\int\rangle$ have been defined in the last section.

As promised, this ring fulfils the relations

$$x\partial = \partial x + \vartheta(\partial) = \partial x - 1, \qquad x\int = \int x + \vartheta(\int) = \int x + \int^2, \qquad \text{and} \qquad \partial\int = 1.$$

Hence it is exactly the ring we have been looking for.

Since $K\langle\partial,\int\rangle$ is not left Noetherian—as may be found in [Jac50]—there is an infinite ascending chain of left ideals in $K\langle\partial,\int\rangle$. This gives rise to an infinite ascending chain of left ideals in $\mathrm{A}_1(\partial,\int)$. Consequently, the integro-differential Weyl algebra is not left Noetherian, too. Analogously, we see that $\mathrm{A}_1(\partial,\int)$ is not right Noetherian and neither left nor right Artinian. This is a major difference to the differential Weyl algebra which is not only left and right Noetherian but by [Sta78, Corollary 3.2] all (one-sided) ideals are generated by only two elements.

The structure of two-sided ideals of the differential Weyl algebra is even more specific, namely, the differential Weyl algebra is a simple ring—confer, for example, [Cou95, Theorem 2.1]. This is another result which does not hold for $\mathrm{A}_1(\partial,\int)$.

Theorem 4.11 ([RRM09, Proposition 8])**.** *The ring* $\mathrm{A}_1(\partial,\int)$ *is not simple.*

Proof. We will use [Lam01, Theorem 3.15] which says that a ring of differential operators over a $\mathbb{Q}$-algebra is simple if and only if the coefficient algebra has no non-trivial differential ideals and the derivation is not inner. Since we required $\operatorname{char} K = 0$ in this section, the theorem is applicable to $K\langle\partial,\int\rangle$. We have already shown in Theorem 4.7 that $K\langle\partial,\int\rangle$ does have a non-trivial ϑ-ideal, namely (E). Thus, $\mathrm{A}_1(\partial,\int)$ is not simple. □

Remark 4.12. Additionally, we may prove that ϑ is not an inner derivation. For assume, it was. Then there was $p \in K\langle\partial,\int\rangle$ such that $[p,\partial] = \vartheta(p) = -1$. On the other hand, since by Theorem 4.8 $K\langle\partial,\int\rangle/(\mathrm{E})$ is commutative, we obtain $\overline{[p,\partial]} = 0$ in the quotient ring, that is, $[p,\partial] \in (\mathrm{E})$. This is a contradication to the fact that (E) is a proper ideal—see Theorem 4.4.

Integral operators

The (usual) differential Weyl algebra is a subring of the integro-differential Weyl algebra. The same is true if we consider only integral operators. This leads to the following definition

Definition 4.13 (Integro Weyl algebra/[RRM09, Definition 9])**.** The subring $\mathrm{A}_1(\int) = K[\int][x;\mathrm{id},\vartheta]$ of $\mathrm{A}_1(\partial,\int)$ is called the *integro Weyl algebra*.

In contrast to its differential counterpart, the integro Weyl algebra seems to have attracted less attention. In particular, they seem not to have been studied in an Ore polynomial setting before. We would, however, like to refer the reader to the original work about the similar *Rota-Baxter algebras* in [Bax60] and [Rot69].

Since $K[\int]$ as a commutative polynomial ring is an integral domain, $\mathrm{A}_1(\int)$ also does not have zero-divisors. This is different from $\mathrm{A}_1(\partial,\int)$ as we have shown earlier but analogue to the differential Weyl algebra. Another notable difference is that $\mathrm{A}_1(\int)$ does have a natural grading: In the equation $x\int = \int x + \int^2$ assigning both x and $\int$ a similar weight, we have the same weight sums on both sides. An immediate consequence of this together with the absence of zero divisors is that $\mathrm{A}_1(\int)$ cannot be simple because for instance the ideal generated by x contains only terms of weight 1 or higher and thus no units. We will come back to this below in Theorem 4.20 where we will present a proof that fits more into the Ore polynomial setting.

The basis elements of the integro Weyl algebra as a K space are the terms $\int^i x^j$ with i and $j \geq 0$. We will call this basis the *left basis* of $A_1(\int)$. We will discuss now how the identity $x\int = \int x + \int^2$ can be used to switch the sides of $\int$ and x. This leads to the *right basis* $x^i \int^j$ with i and $j \geq 0$. The following lemma describes how the bases map onto each other.

Lemma 4.14 ([RRM09, Lemma 10])**.** *We have the identities*

$$x^n \int^m = \sum_{k=0}^{n} (-1)^k \frac{(-m)^{\underline{k}} n^{\underline{k}}}{k!} \int^{m+k} x^{n-k} \qquad \text{and} \qquad \int^m x^n = \sum_{k=0}^{n} \frac{(-m)^{\underline{k}} n^{\underline{k}}}{k!} x^{n-k} \int^{m+k}$$

for changing between the left and right basis where $n^{\underline{k}} = n(n-1)\cdots(n-k+1)$ *denotes the falling factorial.*

Proof. Using Lemma 3.5 together with the formula for diffnomials from Example 3.4 part 1, we obtain that for every $f \in A_1(\int)$

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

Analogously, we may prove that for all $f \in A_1(\int)$

$$f x^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^{n-k} \vartheta^k(f)$$

using $fx = xf - \vartheta(f)$ in the induction step. (Using $x * f = fx$, the formula reads $x * f = f * x - \vartheta(f)$ and can thus be interpreted as a commutation rule in the opposite ring with $-\vartheta$ as derivation—then the second identity is again an instance of Lemma 3.5.)

We apply the formulæ to $f = \int^m$. We have to use

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} \qquad \text{and} \qquad \vartheta^k(\int^m) = (-1)^k (-m)^{\underline{k}} \int^{m+k}$$

where the last identity follows from iterating $\vartheta(\int^m) = m\int^{m+1}$—which holds since ϑ is a derivation. With these identities, the claim of the lemma follows. □

The identities in the previous lemma are written in such a way that their relation to the corresponding formulæ for the differential Weyl algebra becomes evident. In fact, they are very similar to [SST00, Equation (1.4)] if we regard $\int$ as a ∂^{-1} as sketched in Theorem 4.8.

In order to identify $A_1(\int)$ later with the summand $K[x][\int]$ in Equation (4.2) we will present now yet another basis which is more similar to the definition of $K[x][\int]$. More precisely, we will prove below that the terms x^m with $m \geq 0$ and $x^i \int x^j$ with i and $j \geq 0$ are a K-basis of $A_1(\int)$. This corresponds to the definition of $K[x][\int]$ since a K-basis of the polynomial ring $K[x]$ is given by just the powers of x. We will call this basis the *mid basis*. If we let the operators act on a function space, then the mid basis has the interesting interpretation that all iterated integrals can be replaced by just single integrals. It thus never necessary to integrate twice. This may be regarded as an algebraic analogue of the *Cauchy formula* for repeated integration—confer, for example, [OS74, Page 38].

Lemma 4.15 ([RRM09, Lemma 11])**.** *It is* $x^n \int - \int x^n = n \int x^{n-1} \int$ *for all* $n \geq 0$.

Proof. The identity obviously holds for $n = 0$. We will now prove it for $n+1$. Using the right to left basis formula from Lemma 4.14 in the case $m = 1$, we obtain

$$(n+1)\int \cdot x^n \int = \sum_{k=0}^{n} (n+1)^{\underline{k+1}} \int^{k+2} x^{n-k} = -\int x^{n+1} + \sum_{k=0}^{n+1} (n+1)^{\underline{k}} \int^{k+1} x^{n+1-k}$$

using $(-1)^{\underline{k}}/k! = (-1)^k$. Since the sum on the right hand side is just $x^{n+1}\int$ by the second identity in Lemma 4.14, the desired formula follows. □

From this lemma we obtain:

Corollary 4.16 ([RRM09, Corollary 12]). *The monomials of the form x^m for $m \geq 0$ and $x^i \int x^j$ with i and $j \geq 0$ form a K-basis of $\mathrm{A}_1(\int)$.*

Proof. Just as the differential Weyl algebra, also the integro Weyl algebra may be represented as a quotient of a free algebra. More precisely, we have

$$\mathrm{A}_1(\int) = \frac{K\langle L, X\rangle}{(XL - LX - L^2)}$$

identifying $x = \overline{X}$ and $\int = \overline{L}$. By Lemma 4.15, the expressions

$$LX^n L - \frac{1}{n+1}\left(X^{n+1}L - LX^{n+1}\right)$$

belong to the ideal $(XL - LX - L^2)$. They form a Gröbner basis with respect to to the following admissible ordering as described in [Ufn98, Page 268]: Words are compared first by L-degree, then in total degree, and finally lexicographically (with either $L < X$ or $X < L$). It is easy to check that the overlaps LX^nLX^mL are resolvable. Thus, do the residue classes of the monomials X^n and X^iLX^j form a K basis of the quotient by [Ufn98, Theorem 7]. □

We collect the identities that govern the transitions between the left, the right and the mid basis in the following lemma.

Lemma 4.17 ([RRM09, Lemma 13]). *The following equations hold in $\mathrm{A}_1(\int)$ for all m and $n \geq 0$:*

$$x^m \int x^n = \sum_{k=0}^{m} \frac{m!}{k!} \int^{m-k+1} x^{k+n}, \qquad x^m \int x^n = \sum_{k=0}^{m} (-1)^{n-k} \frac{n!}{k!} x^{m+k} \int^{n-k+1},$$

$$\text{and} \qquad \int^{m+1} = \sum_{k=0}^{m} \frac{(-1)^k}{k!(m-k)!} x^{m-k} \int x^k.$$

Proof. The first two identities may immediately be derived from Lemma 4.14 where we applied an index transformation to sort the terms with respect to x instead of with respect to $\int$. Note that using distributivity it is sufficient to consider $n = 0$ for the first formula and $m = 0$ for the second.

The third identity is proven by induction: It definitely holds for $m = 0$. Assume that it is true for $m \geq 0$. Then multiplying it from the left with $\int$ and applying Lemma 4.15 yields

$$\int^{m+1} = \sum_{k=0}^{m} \frac{(-1)^k}{k!(m-k)!} \int x^{m-k} \int x^k = \sum_{k=0}^{m} \frac{(-1)^k}{(k+1)!(m-k)!} \left(x^{m+1}\int - x^{m-k}\int x^{k+1}\right).$$

Using a well-known formula for binomial coefficients, we obtain

$$(m+1)!\sum_{k=0}^{m}\frac{(-1)^k}{(k+1)!(m-k)!}=\sum_{k=0}^{m}\frac{(-1)^k(m+1)!}{(k+1)!(m-k)!}=-\sum_{k=0}^{m}(-1)^{k+1}\binom{m+1}{k+1}=\binom{m+1}{0}=1$$

since the summation is only up to m. Using this in the calculation above, we see that

$$\begin{aligned}\sum_{k=0}^{m}\frac{(-1)^k}{(k+1)!(m-k)!}x^{m+1}\textstyle\int-\sum_{k=0}^{m}\frac{(-1)^k}{(k+1)!(m-k)!}x^{m-k}\textstyle\int x^{k+1}&\\ =x^{m+1}\textstyle\int+\sum_{k=1}^{m+1}\frac{(-1)^k}{k!(m+1-k)!}x^{m+1-k}\textstyle\int x^k=\sum_{k=0}^{m+1}\frac{(-1)^k}{k!(m+1-k)!}x^{m+1-k}\textstyle\int x^k&\end{aligned}$$

which is the promised identity for $m+1$. □

The previous lemma may also be used for an alternative proof that the mid basis is indeed a K-basis: By the last identity in the lemma, the mid basis is a generating set for $\mathrm{A}_1(\int)$. The linear independence may be obtained by the first formula: Assume that

$$\sum_{\mu=0}^{m}\sum_{\nu=0}^{n}\alpha_{\mu,\nu}x^\mu\textstyle\int x^\nu+\sum_{k=0}^{p}\beta_k x^k=0 \tag{4.6}$$

for some $\alpha_{\mu,\nu}$ and $\beta_k\in K$. We compute first the coefficient of x^0. Using the first identity of Lemma 4.17, this must be

$$\beta_0+\sum_{\mu=0}^{m}\mu!\textstyle\int^{\mu+1}\alpha_{\mu,0}$$

since x^0 can occur in the sum only for terms of the form $x^\mu\int x^0$ and only where the summation index in the formula of the lemma k is zero. By assumption the coefficient of x^0 must vanish, which implies that the above sum vanishes. Since the powers of $\int$ in the sum are all different, this means that $\beta_0=\alpha_{0,0}=\ldots=\alpha_{m,0}=0$. In particular, no term of the form $x^\mu\int$ with $\mu\geq 0$ occurs in the sum in Equation (4.6). Dividing it by x from the right—remember here that $\mathrm{A}_1(\int)$ is integral—we can iterate this argument eventually proving that all $\alpha_{\mu,\nu}$ and β_ℓ with μ, ν and $\ell\geq 0$ must vanish. This shows that the mid basis elements are K-linearly independent and hence really a basis.

Example 4.18. Changing from the left to the mid basis we may compute

$$\textstyle\int^3+\int^2x=\frac{1}{2}x^2\int-x\int x+\frac{1}{2}\int x^2+(x\int-\int x)x=\frac{1}{2}x^2\int-\frac{1}{2}\int x^2$$

using the last formula from Lemma 4.17.

Since in $K[\int]$ we have $\vartheta(q\int)=\vartheta(q)\int+q\int^2\in(\int)$, we see that $(\int)$ is a ϑ-ideal. Thus, the set of all operators with coefficients in $(\int)$ is an ideal in $\mathrm{A}_1(\int)$. Denote this set by $\mathrm{A}_1(\int)\int$.[2] Using the left basis, $\mathrm{A}_1(\int)\int$ is generated by all terms of the form $\int^{m+1}x^n$ with m and $n\geq 0$. Using the third identity in the lemma, such a term corresponds to a sum of mid basis terms in which an $\int$ occurs. Conversely, by the first identity does every mid basis term with an $\int$ expand to a sum of terms of the form $\int^{m+1}x^n$

[2] Although this notation is usually reserved to one-sided ideals in the remainder of the thesis, we use it here in a purely symbolical way since it has been used in [RRM09], too.

with m and $n \geq 0$ in the left basis. Thus, the mid basis terms $x^i \int x^j$ with i and $j \geq 0$ form a basis of $A_1(\int)\int$.

Since $A_1(\int)\int$ is a two-sided ideal of $A_1(\int)$ which does contain no units because all terms have at least weight 1, we may conclude that the integro Weyl algebra in contrast to its differential counterpart is not simple. This fact will also be proven differently below in Theorem 4.20.

We can establish a homomorphism between $A_1(\int)\int$ and the direct summand $K[x][\int]$ in Equation (4.2) mapping the mid basis terms to the corresponding terms in $K[x][\int]$. Using Lemma 4.15 it is easy to check that the multiplication in $A_1(\int)\int$ corresponds to the multiplication in $K[x][\int]$ as defined in Equation (4.1). That means that the mapping is not only K-linear but also multiplicative.[3]

We will end this section with the promised alternative proof that $A_1(\int)$ is not simple. For this we will need a lemma first which generalises our reasoning about $(\int)$ above.

Lemma 4.19. *[RRM09, Lemma 14]. An ideal $I \trianglelefteq K[\int]$ is a non-trivial ϑ-ideal if and only if $I = (\int^m)$ with $m > 0$*

Proof. Since for $m > 0$ we have $\vartheta(\int^m) = m\int^{m+1}$ the ideal generated by $\int^m$ is obviously a ϑ-ideal.

Conversely, let $I \trianglelefteq K[\int]$ be a ϑ-ideal which is different from K and $\{0\}$ but otherwise arbitrary. Since $K[\int]$ is just a commutative polynomial ring, there exists an element $q \in K[\int]$ with $\deg q = m > 0$ such that $I = (q)$. Assume that $q = \sum_{i=k}^{m} a_i \int^i$ for some $m \geq k \geq 0$ with $a_k, \ldots, a_m \in K$ and with $a_k \neq 0$. Because we assumed I to be an ϑ-ideal, we have $\vartheta(q) \in I$ and thus $\vartheta(q) = rq$ for some $r \in K[\int]$. Since

$$\vartheta(q) = \sum_{i=k}^{m} a_i i \int^{i+1} = \sum_{i=k+1}^{m+1} a_{i-1}(i-1)\int^i$$

has degree $m+1$, we must have $\deg r = 1$ and thus $r = b_1\int + b_0$. Equating the coefficients of $\int^{m+1}$ and $\int^k$ in $\vartheta(q)$ and rq we obtain $a_m b_1 = m a_m$ and $a_k b_0 = 0$. This implies $b_1 = m$ and $b_0 = 0$. If we had $k < m$ then the coefficients of $\int^{k+1}$ were $k a_k$ in $\vartheta(q)$ and $m a_k$ in rq which implied $(m-k)a_k = 0$ contradicting our assumptions. Thus, we must have $k = m$ and hence $q = a_m \int^m$. Consequently, we obtain $I = (\int^m)$. □

The lemma does not only give a complete description of the ϑ-ideals of $K[\int]$, but analogously to Theorem 4.11 we may use it to prove that $A_1(\int)$ must have non-trivial ideals.

Theorem 4.20. *[RRM09, Proposition 15]. The integro Weyl algebra $A_1(\int)$ is not simple.*

Proof. Since there exist non-trivial ϑ-ideals in $K[\int]$, by [Lam01, Theorem 3.15] $A_1(\int)$ cannot be simple. □

Connection to integro-differential operators

This section is dedicated to the comparision of the integro-differential Weyl algebra with the integro-differential operators as defined in Section 4.1. While in the latter we always worked with a fixed integral, in the construction of the integro-differential Weyl algebra we required the symbol $\int$ to merely be any one-sided inverse of ∂. This lets us expect that the integral in $A_1(\partial, \int)$ is more versatile than its counterpart from Section 4.1. That this intuition is correct will be proven in Theorem 4.23.

[3] It is not a homomorphism, though, since neither $K[x][\int]$ nor $A_1(\int)$ contain an unit element and they are not rings.

But first, we will once more examine the consequences of making $\int$ a two-sided inverse as for constant coefficients we already did in Theorem 4.8. There, we proved that $K\langle\partial,\int\rangle$ and the Laurent polynomial ring $K[Z,Z^{-1}]$ are differentially isomorphic if we interpret Z as ∂, that is, if we set the derivative of Z to -1. In Remark 4.9 we proved that also the dual approach of interpreting Z as $\int$ by setting its derivative to Z^2 yields a differential isomorphism. By the universal property of Ore polynomials (see Theorem 3.7), this isomorphism lifts to the Ore polynomial rings. That is, we have

$$K[Z,Z^{-1}][x;\mathrm{id},-d/dZ] \cong K[Z,Z^{-1}][x;\mathrm{id},Z^2\cdot d/dZ]$$

as rings.

If we extend the isomorphism of Theorem 4.8 using the universal property in Theorem 3.7, then we obtain the following result. This is the connection between integro-differential Ore polynomials in rings with integrals that are one-sided inverses to those where they are two-sided inverses.

Theorem 4.21 ([RRM09, Theorem 18])**.** *We have*

$$\frac{\mathrm{A}_1(\partial,\int)}{(\mathtt{E})} \cong K[Z,Z^{-1}][x;\mathrm{id},-d/dZ]$$

as rings.

As last result in this chapter we finally want to connect the integro-differential Weyl algebra to the integro-differential operators. Using the direct sum decomposition of $K\langle\partial,\int\rangle$ in Theorem 4.4 coefficient-wise, we obtain a direct sum decomposition

$$\mathrm{A}_1(\partial,\int) = \mathrm{A}_1(\partial)\oplus\mathrm{A}_1(\int)\int\oplus(\mathtt{E})$$

where $(\mathtt{E})$ denotes the ideal generated by $\mathtt{E}$ in $\mathrm{A}_1(\partial,\int)$. Since $(\mathtt{E})$ is a ϑ-ideal, it consists of all those Ore polynomials whose coefficients are in $(\mathtt{E}) \trianglelefteq K\langle\partial,\int\rangle$. This corresponds directly to the decomposition of $K[x][\partial,\int]$ in its defining Equation (4.2). It remains to map each summand to its counterpart.

The important step for this will be to fix the constant of integration $c \in K$. For this we have to investigate the last summand in the above decomposition more closely. First, we consider analogously to the boundary operators $K[x][\mathtt{E}]$ the subspace B of $\mathrm{A}_1(\partial,\int)$ with basis $x^k\mathtt{E}\partial^j$ with k and $j \geq i$. Here, it is important to note, that the identities

$$\partial x = x\partial + 1, \qquad \int x = x\int - \int^2 \qquad \text{and} \qquad \mathtt{E}x = x\mathtt{E} - \int\mathtt{E}$$

which come from the commutation rule—where we used $\vartheta(\mathtt{E}) = \int\mathtt{E}$ as computed in Equation (4.5)—may be used to convert the *left basis* $\partial^i x^r$, $\int^j x^s$ and $e_{m,n}x^t$ with i, j, m, n, r, s and $t \geq 0$ to a corresponding *right basis* $x^r\partial^i$, $x^s\int^j$ and $x^t e_{m,n}$. Confer also Lemma 4.14 where we gave the concrete formula for the integro case and its proof from which conversion formulæ for the other cases may be derived.

Lemma 4.22 ([RRM09, Lemma 19])**.** *In* $\mathrm{A}_1(\partial,\int)$ *we have for every* $c \in K$ *a decomposition*

$$(\mathtt{E}) = B \oplus (\eta)$$

where $B = \langle x^k\mathtt{E}\partial^j \mid k,j \geq 0\rangle$ *and* $\eta = \mathtt{E}x - c\mathtt{E}$*. Furthermore, a basis for the ideal* $(\eta) \trianglelefteq \mathrm{A}_1(\partial,\int)$ *is given by the terms* $x^k\int^i\eta\partial^j$ *with* i*,* j *and* $k \geq 0$*.*

Proof. We have $\mathrm{E}x = (x - \int)\mathrm{E}$ and $\int^{i-1} x = x\int^{i-1} - \vartheta(\int^{i-1}) = x\int^{i-1} - (i-1)\int^i$ for $i \geq 1$ by the commutation rule. This implies

$$\int^{i-1}\eta = \int^{i-1}(\mathrm{E}x - c\mathrm{E}) = \int^{i-1}x\mathrm{E} - \int^i\mathrm{E} - c\int^{i-1}\mathrm{E} = x\int^{i-1}\mathrm{E} - i\int^i\mathrm{E} - c\int^{i-1}\mathrm{E} \in (\eta).$$

Thus, multiplying by x^k from the left and by ∂^j from the right, we obtain

$$x^k e_{i,j} + \frac{c}{i}x^k e_{i-1,j} - \frac{1}{i}x^{k+1}e_{i-1,j} \in (\eta)$$

for $i \geq 1$. This allows to replace terms $x^k e_{i,j}$ of the right basis of (E) by terms with smaller powers of $\int$ plus some term in (η). Iterating this, we eventually see that all elements in (E) may be represented as linear combinations of terms $x^k e_{0,j} = x^k\mathrm{E}\int^j$ and some term in (η).

Analogously to the e_{ij}, we write $\eta_{i,j}$ for $\int^i\eta\partial^j$ where i and $j \geq 0$. Furthermore, we denote the K-space generated by the terms $x^k\eta_{ij}$ as $H = \langle x^k\eta_{i,j} \mid i,j,k \geq 0\rangle$. Since H is generated by terms in (η), it is obviously a subspace of (η). For all i, j and $k \geq 0$, we have

$$\int\eta_{i,j} = \int\eta_{i+1,j} \qquad \text{and} \qquad \partial\eta_{i,j} = \begin{cases}\eta_{i-1,j}, & \text{if } i \geq 1\\ 0, & \text{if } i = 0\end{cases}$$

as well as

$$\eta_{i,j}\partial = \eta_{i,j+1} \qquad \text{and} \qquad \eta_{i,j}\int = \begin{cases}\eta_{i,j-1}, & \text{if } j \geq 1\\ 0, & \text{if } j = 0.\end{cases}$$

using the Equations (4.3) and (4.4) on Page 24 as well as the commutation rule $x\int = \int x + \int^2$ for $\eta\int = \mathrm{E}(\int x + \int^2 - \int c) = 0$. Using Lemma 4.14 and the similarly proven equation $\partial x^k = x^k\partial + kx^{k-1}$, we see that products of ∂ and $\int$ with $\eta_{i,j}$ on either side stay in H. Since we also have $\eta x = (x - \int)\mathrm{E}x - c(x - \int)\mathrm{E}x = (x - \int)\eta$ we see that H is an ideal of $\mathrm{A}_1(\partial, \int)$. Thus, since $\eta \in H$ and $H \subseteq (\eta)$ we obtain $H = (\eta)$.

It remains to prove that the sum $B + (\eta)$ is direct. We have the identity

$$\begin{aligned}x^k\eta_{i,j} &= x^k\int^i\eta\partial^j = x^k\int^i\mathrm{E}x\partial^j - x^k c\int^i\mathrm{E}\partial^j = x^k\int^i(x - \int)\mathrm{E}\partial^j - x^k c\int^i\mathrm{E}\partial^j\\ &= x^k\int^i x\mathrm{E}\partial^j - x^k\int^{i+1}\mathrm{E}\partial^j - cx^k\int^i\mathrm{E}\partial^j = x^k(x\int^i - i\int^{i+1})\mathrm{E}\partial^j - x^k\int^{i+1}\mathrm{E}\partial^j - cx^k\int^i\mathrm{E}\partial^j\\ &= x^{k+1}\int^i\mathrm{E}\partial^j - ix^k\int^{i+1}\mathrm{E}\partial^j - x^k\int^{i+1}\mathrm{E}\partial^j - cx^k\int^i\mathrm{E}\partial^j = x^{k+1}e_{i,j} - (i+1)x^k e_{i+1,j} - cx^k e_{i,j}\end{aligned}$$

which allows to convert the generating elements $x^k\eta_{i,j}$ of H into the right basis $x^t e_{m,n}$ of (E). Assume now that

$$\sum_{m,n\geq 0}\alpha_{m,n}x^m e_{0,n} = \sum_{i,j,k\geq 0}\beta_{i,j,k}x^k\eta_{i,j}$$

for $\alpha_{m,n}$ and $\beta_{i,j,k} \in K$ with only finitely many of them non-zero and where i, j, k, m and $n \geq 0$. Choosing i maximal such that $\beta_{i,j,k} \neq 0$ and converting to the right basis, we see that the terms $\beta_{i,j,k}$ must vanish for all j and $k \geq 0$ since the basis elements $x^k e_{i+1,j}$ coming from the conversion do not appear on the left hand side. Since this contradicts the choice of i, we conclude that all coefficients must be zero thus implying the directness of the sum.

The same argument—repeated with 0 as the left hand side—also proves that the terms $x^k\eta_{i,j}$ with i, j and $k \geq 0$ are indeed K-linearly independent and thus a basis for (η). □

With this lemma the connection of $\mathrm{A}_1(\partial, \int)$ to $K[x][\partial, \int]$ from Section 4.1 is almost immediate.

Theorem 4.23 ([RRM09, Theorem 20]). *If $\int$ is an integral of the standard derivation d/dx on $K[x]$, then we have*

$$\frac{\mathrm{A}_1(\partial, \int)}{(\mathtt{E}x - c\mathtt{E})} \cong K[x][\partial, \int]$$

where $c = \int(1) - x \in K$ is the constant of integration.

Proof. By Lemma 4.22 and the direct sum decomposition of $\mathrm{A}_1(\partial, \int)$ we obtain

$$\frac{\mathrm{A}_1(\partial, \int)}{(\mathtt{E}x - c\mathtt{E})} = \mathrm{A}_1(\partial) \oplus \mathrm{A}_1(\int)\int \oplus B$$

where B is defined in the lemma. As hinted before identifying the right basis elements $x^i\partial^j$ where i and $j \geq 0$ of $\mathrm{A}_1(\partial)$, the mid basis elements $x^m \int x^n$ where m and $n \geq 0$ of $\mathrm{A}_1(\int)$ from Corollary 4.16 and the basis elements $x^s\mathtt{E}\partial^t$ where s and $t \geq 0$ of B from Lemma 4.22 with the corresponding basis elements of $K[x][\partial]$, $K[x][\int]$ and $K[x][\mathtt{E}]$ from Section 4.1, we establish a K-linear bijection $\varphi\mathrm{A}_1(\partial, \int)/(\mathtt{E}x - c\mathtt{E}) \to K[x][\partial, \int]$.

It remains to prove that φ is multiplicative as well. By the linearity of φ, it is sufficient to verify this for basis elements. First of all note, that $\mathrm{A}_1(\partial)$ and $K[x][\partial]$ are isomorphic as rings since $\varphi(\partial)\varphi(x) = \partial x = x\partial + 1 = \varphi(x)\varphi(\partial) + 1$ yields the same commutation rule. Similarly, we can show that $\mathrm{A}_1(\int)\int$ and $K[x][\int]$ are isomorphic: We compute for $n \geq 0$ in $\mathrm{A}_1(\int)$

$$\int x^n \int = \frac{1}{n+1} x^{n+1} \int - \frac{1}{n+1} \int x^{n+1} = \frac{1}{n+1}(x^{n+1} + c^{n+1}) \int - \int \frac{1}{n}(x^{n+1} + c^{n+1}) = \int(x^n) \int - \int \int(x^n).$$

For the isomorphism between B and $K[x][\mathtt{E}]$ we note that by Lemma 3.5 using the commutation $\partial x = x\partial + 1$ in $\mathrm{A}_1(\partial)$ we can prove

$$\partial^i x^k = \sum_{\substack{j=0 \\ j-i \geq k}}^{i} \binom{i}{j} k^{\underline{i-j}} x^{k+j-i} \partial^j.$$

This yields in $(\mathtt{E})$ for i, k, m and $n \geq 0$

$$x^n\mathtt{E}\partial^i x^k \mathtt{E}\partial^m = x^n\mathtt{E} \sum_{\substack{j=0 \\ j-i \geq k}}^{i} \binom{i}{j} k^{\underline{i-j}} x^{k+j-i} \partial^j \mathtt{E}\partial^m = \begin{cases} x^n\mathtt{E}k^{\underline{i}} x^{k-i}\mathtt{E}\partial^m, & \text{if } i \geq k \\ 0, & \text{otherwise} \end{cases}$$

since $\partial^j\mathtt{E} = 0$ for $j \geq 1$ which is exactly the formula for multiplication in $K[x][\mathtt{E}]$.

The formulæ for the multiplication between the other direct summands are proven similarly using the fact that in $K[x][\partial, \int]$ the identities $\partial x = x\partial + 1$, $\int^2 = x\int - \int x$ and $\partial \int = 1$ hold and using the identity $\mathtt{E}x = c\mathtt{E}$ which is enforced by taking the quotient with $(\mathtt{E}x - c\mathtt{E})$ and which yields $\mathtt{E}p(x) = p(c)\mathtt{E}$, that is, $\mathtt{E}p = \varepsilon(p)\mathtt{E}$ in $\mathrm{A}_1(\partial, \int)/(\mathtt{E}x - c\mathtt{E})$ for every $p \in K[x]$. □

The last theorem shows that Ore polynomials are indeed well suited to model integro-differential operators with polynomial coefficients. They provide new insight and a framework for computation which might be utilized by implementations of integro-differential operators in computer algebra systems.

It is interesting, that the integro-differential Weyl algebra is a slightly more general structure than the integro-differential operators alone. It allows to abstract from a given integral of d/dx to a general integral which does not fix the constant of integration.

Part III

Normal forms

5

Row-reduction, column-reduction and Gröbner bases over rings

5.1 General definitions for matrices

In this whole chapter, K will always be a skew field. Let $\sigma: K \to K$ be an automorphism and $\vartheta: K \to K$ a σ-derivation. We set $R = K[\partial;\sigma,\vartheta]$. This section contains definitions and notations for matrices over R. The set of all $s \times t$-matrices with entries in R will be denoted by ${}^sR^t$. If $s = 1$, then we simply write ${}^1R^t = R^t$ for the set of row vectors of length t. If $t = 1$, we write ${}^sR^1 = {}^sR$ for the set of column vectors of length s.

A square matrix $M \in {}^sR^s$ will be called *unimodular* if it possesses a two-sided inverse $M^{-1} \in {}^sR^s$. We will denote the set of unimodular $s \times s$-matrices over R by $\mathrm{Gl}_s(R)$. We denote the $s \times s$ identity matrix by $\mathbf{1}_s$. The $s \times t$ zero matrix is written as ${}_s\mathbf{0}_t$. A *diagonal matrix* will be denoted by $\mathrm{diag}(a_1,\ldots,a_n) \in {}^sR^t$ for $a_1,\ldots,a_n \in R$ where $n \leq \min\{s,t\}$. We like to point out, that in this thesis diagonal matrices need not to be square but may be rectangular. The precise size will always be visible from the context though.

For $M \in {}^sR^t$, we denote the i^{th} row by $M_{i,*}$ where $1 \leq i \leq s$ and the j^{th} column by $M_{*,j}$ for $1 \leq j \leq t$. More general, for a subset $I = \{i_1,\ldots,i_r\} \subseteq \{1,\ldots,s\}$ with $i_1 < \ldots < i_r$ by $M_{I,*}$ we denote the matrix in ${}^{|I|}R^t$ consisting of the rows $M_{i_1,*},\ldots,M_{i_r,*}$ of M. We will use the abbreviations $M_{\bar{I},*} = M_{\{1,\ldots,s\}\setminus I,*}$.We will write just $M_{\bar{i},*}$ if $I = \{i\}$. Similar notations will be used for matrices consisting of columns of M.

We extend the notion of degree to matrices by defining

$$\deg M = \max\{\deg M_{ij} \mid 1 \leq i \leq s \text{ and } 1 \leq j \leq t\}$$

where $M = (M_{ij}) \in {}^sR^t$. With this definition we obtain the identity $\deg MN \leq \deg M + \deg N$ for all matrices $N \in {}^tR^u$. Let $M \in {}^sR^t$ be an arbitrary matrix. We may write M as a formal sum

$$M = M_k\partial^k + \ldots + M_1\partial + M_0$$

where $M_0,\ldots,M_k \in {}^sK^t$ do not contain ∂. If $M_k \neq 0$, then we call $M_k = \mathrm{lv}(M)$ the *leading vector* of M.[1] If we apply σ and ϑ to matrices componentwise, then we we obtain the familiar looking rules

[1] The name was chosen since we apply the function mostly in the case $s = 1$, that is, to (row) vectors.

$\sigma(MN) = \sigma(M)\sigma(N)$ and $\vartheta(MN) = \sigma(M)\vartheta(N) + \vartheta(M)N$ as well as $\partial M = \sigma(M)\partial + \vartheta(M)$ for all $M \in {}^sR^t$ and $N \in {}^tR^u$. Thus, we can translate the formula for the leading coefficient (3.4) to matrices yielding

$$\operatorname{lv}(MN) = \operatorname{lv}(M)\,\sigma^{\deg M}\big(\operatorname{lv}(N)\big) \tag{5.1}$$

unless this product is zero; and $\operatorname{lv}(fM) = \operatorname{lc}(f)\,\sigma^{\deg f}\big(\operatorname{lv}(M)\big)$ for any non-zero $f \in R$. A possible MAPLE implementation for the leading vector can be found in Section 9.1 in the appendix.

It is possible to show that

$${}^s(K[\partial;\sigma,\vartheta])^s \cong ({}^sK^s)[\partial;\sigma,\vartheta].$$

In the latter ring, we can define left and right Euclidean division by any matrix $N \in {}^sR^s$ whose leading vector is invertible, that is, where $\operatorname{lv}(N) \in \mathrm{Gl}_s(K)$. Since we can embed every row vector $\mathfrak{v} \in R^s$ into an $s \times s$-matrix by simply adding $s-1$ zero rows, we conclude that in this case we may represent $\mathfrak{v} = \mathfrak{x}N + \mathfrak{u}$ where $\mathfrak{x}$ and $\mathfrak{u} \in R^s$ and $\deg\mathfrak{u} < \deg\mathfrak{v}$. This is a special case of a more general result which will be explained below in Theorem 5.2. It should not be confused, though, with the division that is presented in Theorem 6.22.

5.2 Row reduction & Gröbner bases over rings

Given a matrix $M \in {}^sR^t$ we would like to derive a nice description of its *row space* R^sM. A possible goal is to look for a set of generators of R^sM of minimal degree. This idea has first been pursued in [For75] for commutative polynomials under the name of *minimal bases*. The method to compute such a minimal basis was later dubbed row-reduction—for example, in [Kai80, Page 385]—and has been extended to Ore polynomials—see, for example, [BCL06].

We will present here a naïve algorithm for row-reduction that can be deduced from [For75, Main Theorem] or be found in the proof of [BCL06, Theorem 2.2]. We will, however, change the context of the method by relating it to a different field of research: Gröbner bases over rings as described, for example, in [Pau07]. This will yield a different view on row-reduction. Towards the end of the section we will prove that our approach—which we will call row bases in order to distinguish them from the Gröbner bases considered in the next section—and the traditional one do indeed lead to the same results. See Corollary 5.9.

The main idea is to try to lower the degrees of the rows of M by applying elementary row operations which may be interpretated as multiplication by unimodular matrices from the left. The degree of a row in M can be lowered if its leading vector is a linear combination of leading vectors of rows of lower degree.

For $k \geq 0$, we define the *k^{th} leading row coefficient matrix* $\mathrm{LC}^k_{\mathrm{row}}(M)$ of M row-wise by

$$\mathrm{LC}^k_{\mathrm{row}}(M)_{i,*} = \begin{cases} \sigma^{k-\deg M_{i,*}}\big(\operatorname{lv}(M_{i,*})\big), & \text{if } k \geq \deg M_{i,*} \geq 0 \\ 0, & \text{otherwise.} \end{cases}$$

(An alternative way of defining $\mathrm{LC}^k_{\mathrm{row}}(M)$ following [BCL06] is: Letting $\delta_i = \partial^{k-\deg M_{i,*}}$ if $k \geq \deg M_{i,*} \geq 0$ and $\delta_i = 0$ otherwise, we obtain $\mathrm{LC}^k_{\mathrm{row}}(M) = \operatorname{lv}\big(\operatorname{diag}(\delta_1,\ldots,\delta_m)M\big)$ unless $\delta_1 = \ldots = \delta_s = 0$ and $\mathrm{LC}^k_{\mathrm{row}}(M) = {}_s\mathbf{0}_t$ otherwise.) We will sometimes use the abbreviation $\mathrm{LC}_{\mathrm{row}}(M) = \mathrm{LC}^{\deg M}_{\mathrm{row}}(M)$ and call this just the leading row coefficient matrix of M. Again, an illustrating implementation can be found in Section 9.1.

Example 5.1. We consider the field $K = \mathbb{Q}(x)$ of rational functions. Let $\sigma: K \to K$ be the automorphism that substitutes x by $x+1$. Since the zero map $\vartheta = 0$ is a σ-derivation, we may form the Ore polynomial ring $R = \mathbb{Q}(x)[\mathfrak{S}; \sigma, 0]$. Let

$$M = \begin{pmatrix} \mathfrak{S}^2 + x\mathfrak{S} & \frac{1}{x}\mathfrak{S} & 1 - x\mathfrak{S}^2 \\ \mathfrak{S} - x^2 & x\mathfrak{S} - 1 & 2 \\ x & 0 & \mathfrak{S} \end{pmatrix} \in {}^3R^3$$

be given. Then we obtain

$$\mathrm{LC}^0_{\mathrm{row}}(M) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \mathrm{LC}^1_{\mathrm{row}}(M) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & x & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \text{and,} \qquad \mathrm{LC}^2_{\mathrm{row}}(M) = \begin{pmatrix} 1 & 0 & -x \\ 1 & x+1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We will say that a row-vector $\mathfrak{v} \in R^t$ is *reducible* by M if and only if $\mathfrak{v} \neq 0$ and there is a vector $\mathfrak{u} \in K^s$ such that

$$\mathfrak{u}\,\mathrm{LC}^{\deg \mathfrak{v}}_{\mathrm{row}}(M) = \mathrm{lv}(\mathfrak{v}).$$

If for $j = 1, \ldots, s$ we define $\tilde{\mathfrak{u}} \in R^s$ by $\tilde{\mathfrak{u}}_j = \mathfrak{u}_j \partial^{\deg v - \deg M_{j,*}}$ if $\deg v \geq \deg M_{j,*}$ and by $\tilde{\mathfrak{u}}_j = 0$ otherwise, then we obtain $\mathrm{lv}(\mathfrak{v}) = \mathrm{lv}\big(\tilde{\mathfrak{u}}M\big)$ since $\mathrm{LC}^{\deg \mathfrak{v}}_{\mathrm{row}}(M)_{j,*} = 0$ whenever $\deg v < \deg M_{j,*}$ and thus

$$\deg(\mathfrak{v} - \tilde{\mathfrak{u}}M) < \deg \mathfrak{v}.$$

We will say that $\mathfrak{v}$ *reduces* to $\mathfrak{v} - \tilde{\mathfrak{u}}M$ in one step. Iterating this as long as possible, we arrive at a vector of the form $\mathfrak{v} - \mathfrak{w}M$ with $\mathfrak{w} \in R^s$ that is not reducible by M any longer. In that case we call $\mathfrak{v} - \mathfrak{w}M$ a *remainder* of $\mathfrak{v}$ by reduction with M.

If we—a little sloppily—identify matrices with sets of row vectors, then we can draw an analogy between the reduction just defined and the reduction used in [Pau07] for Gröbner bases of rings. For this, we will call vectors of the form $\mathfrak{v}\partial^k$ with $\mathfrak{v} \in K^t$ *terms*. That means, that our coefficient domain are the vectors in K^t in analogy to taking coefficients from a ring as in [Pau07]. This domain allows solving linear equations—the computation of syzygies—just as demanded in [Pau07, Section 2]. There is only one possible term order since we are considering univariate Ore polynomials. This corresponds to several possible term orders as in [Pau07, Definition 1]. Hence, the degree function in our case is just the usual degree while the leading coefficient corresponds to our leading vector. The division algorithm explained in [Pau07, Proposition 2] is then just the reduction which we have defined above.

Theorem 5.2 ([Pau07, Proposition 2])**.** *Let K be a ring with an automorphism $\sigma: K \to K$ and a σ-derivation $\vartheta: K \to K$. Let $R = K[\partial; \sigma, \vartheta]$. Then for all $M \in {}^sR^t$ and $\mathfrak{v} \in R^t$ exist $\mathfrak{q} \in R^s$ and $\mathfrak{r} \in R^t$ such that*

$$\mathfrak{v} = \mathfrak{q}M + \mathfrak{r}$$

where

1. $\deg \mathfrak{r} \leq \deg \mathfrak{v}$,
2. $M_{j,*} = 0$, $\mathfrak{q}_j = 0$ *or* $\deg \mathfrak{q}_j + \deg M_{j,*} \leq \deg \mathfrak{v}$ *for* $j = 1, \ldots, s$, *and*
3. $\mathfrak{r} = 0$ *or* $\mathrm{lv}(\mathfrak{r}) \notin K^s\,\mathrm{LC}^{\deg \mathfrak{r}}_{row}(M)$.

Proof. The proof can be easily obtained from the proof of [Pau07, Proposition 2]. □

Example 5.3. We consider the ring of commutative polynomials over the rational numbers. That is, with $K = \mathbb{Q}$, $\sigma = \mathrm{id}$ and $\vartheta = 0$ we consider $R = \mathbb{Q}[X;\mathrm{id},0] \cong \mathbb{Q}[X]$. Let

$$M = \begin{pmatrix} X^2 & 1-X & X-X^2 \\ X & -1 & 1 \\ X+3 & 1 & X^2-1 \end{pmatrix} \in {}^3R^3 \qquad \text{and} \qquad \mathfrak{v} = \begin{pmatrix} X^2+X+3, & 2-X, & X-1 \end{pmatrix} \in R^3.$$

We have $\deg \mathfrak{v} = 2$ and

$$\mathrm{LC}^0_{\mathrm{row}}(M) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \mathrm{LC}^1_{\mathrm{row}}(M) = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \text{and,} \qquad \mathrm{LC}^2_{\mathrm{row}}(M) = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since, for example,

$$\mathrm{lv}(\mathfrak{v}) = \begin{pmatrix} 1, & 0, & 0 \end{pmatrix} = \begin{pmatrix} 0, & 1, & 0 \end{pmatrix} \cdot \mathrm{LC}^{\deg \mathfrak{v}}_{\mathrm{row}}(M)$$

we can reduce one step obtaining

$$\mathfrak{v}_1 = \mathfrak{v} - \begin{pmatrix} 0, & X, & 0 \end{pmatrix} \cdot M = \mathfrak{v} - \begin{pmatrix} X^2, & -X, & X \end{pmatrix} = \begin{pmatrix} X+3, & 2, & -1 \end{pmatrix}.$$

Since $\mathrm{lv}(\mathfrak{v}_1) \in K^3\,\mathrm{LC}^{\deg \mathfrak{v}_1}_{\mathrm{row}}(M)$, we are allowed to reduce another step obtaining the remainder

$$\mathfrak{v}_1 - \begin{pmatrix} 0, & 1, & 0 \end{pmatrix} \cdot M = \mathfrak{v}_1 - \begin{pmatrix} X, & -1, & 1 \end{pmatrix} = \begin{pmatrix} 3, & 3, & -2 \end{pmatrix}$$

which can not be reduced any longer.

If we had instead chosen to explore the relation

$$\mathrm{lv}(\mathfrak{v}) = \begin{pmatrix} 1, & 0, & 1 \end{pmatrix} \cdot \mathrm{LC}^{\deg \mathfrak{v}}_{\mathrm{row}}(M),$$

then the reduction would yield

$$\mathfrak{v} - \begin{pmatrix} 1, & 0, & 1 \end{pmatrix} \cdot M = 0.$$

This shows that the result of a reduction is not uniquely determined and that reduction in general gives no decision about the membership of a vector to the row space of a matrix.

We are now in the position to give a counterpart to [Pau07, Definition 4].

Definition 5.4 (Row basis)**.** Let $\mathfrak{M} \subseteq R^t$ be a submodule. For $d \geq 0$, we call

$$\mathrm{LV}_d(\mathfrak{M}) = \{\mathrm{lv}(v) \mid v \in \mathfrak{M} \text{ and } \deg v = d\} \cup \{0\}$$

the d^{th} *leading vector space* of $\mathfrak{M}$.

A matrix $M \in {}^sR^t$ is called a *row basis* for $\mathfrak{M}$, if $R^sM \subseteq \mathfrak{M}$ and the rows of $\mathrm{LC}^d_{\mathrm{row}}(M)$ generate $\mathrm{LV}_d(\mathfrak{M})$, that is,

$$\mathrm{LV}_d(\mathfrak{M}) = K^s\,\mathrm{LC}^d_{\mathrm{row}}(M)$$

for all $d \geq 0$.

Note, that $\mathrm{LV}_d(\mathfrak{M})$ is for any submodule $\mathfrak{M} \subseteq R^t$ indeed a vector space since scalar multiplication by non-zero elements from K does not change the degree of vectors of $\mathfrak{M}$ and addition can lower the degree only if the leading vectors are additive inverses of each other.

Also note that the condition $\mathrm{LV}_d(\mathfrak{M}) = K^s\,\mathrm{LC}^d_{\mathrm{row}}(M)$ for all $d \geq 0$ only means, that every non-zero vector in $\mathfrak{M}$ is reducible by M.

Example 5.5. In Example 5.3 the matrix M was not a row basis since the leading vector of

$$\begin{pmatrix}3, & 3, & -2\end{pmatrix} = \begin{pmatrix}1, & -X-1, & 1\end{pmatrix} M$$

is not contained in $K^3 \operatorname{LC}^0_{\text{row}}(M) = \{0\}$.

Analogously to Gröbner bases, row bases can be used to decide the membership problem:

Theorem 5.6 ([Pau07, Proposition 7])**.** *Let $M \in {}^sR^t$ be a row basis for the submodule $\mathfrak{M} \subseteq R^t$. Then, the remainder of $\mathfrak{v} \in R^t$ by division with M is zero if and only if $\mathfrak{v} \in \mathfrak{M}$.*

Proof. If the remainder is zero, then clearly $\mathfrak{v}$ must be in $\mathfrak{M}$.

Contrarily, assume that $\mathfrak{v} \in \mathfrak{M}$ and let $\mathfrak{r} = \mathfrak{v} - \mathfrak{q}M$ be the remainder of division by M. Hence, by Theorem 5.2 we must have $\mathfrak{r} = 0$ or $\operatorname{lv}(\mathfrak{r}) \notin K^s \operatorname{LC}^{\deg \mathfrak{r}}_{\text{row}}(M) = \operatorname{LV}_{\deg \mathfrak{r}}(\mathfrak{M})$ where the last identity holds since M is a row basis. The second alternative cannot hold since $R^s M \subseteq \mathfrak{M}$ by the definition of row bases implies $\mathfrak{r} \in \mathfrak{M}$. Thus, we obtain $\mathfrak{r} = 0$. □

It is possible to test whether a given matrix is a row basis using a generalised S-polynomial criterion. The version presented here is taken from [Pau07, Proposition 9]. It should be noted that the proof also gives kind of a generalised predictable degree property which we will treat in Corollary 5.8.

Theorem 5.7 ([Pau07, Proposition 9])**.** *Let $M \in {}^sR^t$. Then the following are equivalent:*

1. *M is a row basis for R^sM.*
2. *For every subset $J = \{j_1, \ldots, j_r\} \subseteq \{1, \ldots, s\}$ with $j_1 < \ldots < j_r$ and all $\mathfrak{u} \in B_J$ a remainder of*

$$\sum_{i=1}^{r} \mathfrak{u}_i \partial^{\deg M_{J,*} - \deg M_{j_i,*}} M_{j_i,*}$$

by division with M is zero where B_J is a basis of the nullspace of $\operatorname{LC}_{row}(M_{J,*})$.

Proof. The proof follows closely the one of [Pau07, Proposition 9]. We may assume without loss of generality that M does not contain any zero rows as they do not disturb condition 2.

We only have to prove that condition 2 implies condition 1 as the other direction follows from Theorem 5.6. Let $\mathfrak{v} = \mathfrak{x}M \in R^sM$ and $\mathfrak{v} \neq 0$. By Definition 5.4, we have to show that $\operatorname{lv}(\mathfrak{v}) \in K^s \operatorname{LC}^{\deg \mathfrak{v}}_{\text{row}}(M)$. Let $\delta = \max\{\deg \mathfrak{x}_i + \deg M_{i,*} \mid 1 \leq i \leq s\}$. We may assume that $\mathfrak{x}$ is chosen in such a way that δ is minimial. Let $J = \{j_1, \ldots, j_r\} = \{1 \leq i \leq s \mid \deg \mathfrak{x}_i + \deg M_{i,*} = \delta\}$ with $j_1 < \ldots < j_r$ be the set of indices of the summands of maximal degree in $\mathfrak{x}M$.

We need to distinguish two cases. If $\deg \mathfrak{v} = \delta$, then there exists a subset $J' \subseteq J$ such that

$$\operatorname{lv}(\mathfrak{v}) = \sum_{j \in J'} \mathfrak{x}_j M_{j,*}.$$

Since $\deg M_{J',*} = \deg \mathfrak{v}$ and thus $K^{|J'|} \operatorname{LC}_{\text{row}}(M_{J',*}) \subseteq K^s \operatorname{LC}^{\deg \mathfrak{v}}_{\text{row}}(M)$, we immediately obtain $\operatorname{lv}(\mathfrak{v}) \in K^s \operatorname{LC}^{\deg \mathfrak{v}}_{\text{row}}(M)$ in this case.

The second case is that $\delta > \deg \mathfrak{v}$. This can only happen if cancelation occurs in the higher order terms of $\mathfrak{x}M$, that is, if

$$\mathfrak{y} \cdot \sigma^{\delta - \deg M_{J,*}}\left(\operatorname{LC}_{\text{row}}(M_{J,*})\right) = 0, \qquad \text{or, equivalently,} \qquad \sigma^{\deg M_{J,*} - \delta}(\mathfrak{y}) \cdot \operatorname{LC}_{\text{row}}(M_{J,*}) = 0$$

where $\mathfrak{y} = \left(\operatorname{lc}(\mathfrak{x}_{j_1}), \ldots, \operatorname{lc}(\mathfrak{x}_{j_r})\right) \in K^r$ and where we used the fact that $\delta = \deg \mathfrak{x}_j + \deg M_{j,*}$ for all $j \in J$ and thus

$$\begin{aligned}\operatorname{lv}(\mathfrak{x}_j M_{j,*}) &= \operatorname{lc}(\mathfrak{x}_j) \cdot \sigma^{\deg \mathfrak{x}_j}\left(\operatorname{lv}(M_{j,*})\right) \\ &= \operatorname{lc}(\mathfrak{x}_j) \cdot \sigma^{\delta - \deg M_{J,*}} \circ \sigma^{\deg M_{J,*} - \deg M_{j,*}}\left(\operatorname{lv}(M_{j,*})\right) = \operatorname{lc}(\mathfrak{x}_j) \cdot \sigma^{\delta - \deg M_{J,*}}\left(\operatorname{LC}_{\text{row}}(M_{J,*})_{j,*}\right).\end{aligned}$$

We abbreviate $\delta - \deg M_{J,*}$ by μ which must be non-negative.

We will now try to construct a representation $\mathfrak{v} = \tilde{\mathfrak{x}} M$ with $\tilde{\mathfrak{x}} \in R^s$ for $\mathfrak{v}$ such that $\deg \tilde{\mathfrak{x}}_i + \deg M_{i,*} < \delta$ for all $1 \leq i \leq s$ in order to derive a contradication to the minimality of $\mathfrak{x}$. Let $B_J = (\mathfrak{b}_1, \ldots, \mathfrak{b}_\nu)$. Since we have shown above that $\sigma^{-\mu}(\mathfrak{y})$ is in the nullspace of $\operatorname{LC}_{\text{row}}(M_{J,*})$, there exist $\alpha_1, \ldots, \alpha_\nu \in K$ such that $\sigma^{-\mu}(\mathfrak{y}) = \alpha_1 \mathfrak{b}_1 + \ldots + \alpha_\nu \mathfrak{b}_\nu$. We obtain

$$\begin{aligned}\mathfrak{v} = \mathfrak{x} M &= \sum_{j \in J} \mathfrak{x}_j M_{j,*} + \sum_{j \notin J} \mathfrak{x}_j M_{j,*} \\ &= \sum_{j \in J} \Big(\mathfrak{x}_j - \sum_{k=1}^{\nu} \sigma^{\mu}\left(\alpha_k (\mathfrak{b}_k)_j\right) \partial^{\deg \mathfrak{x}_j} \Big) M_{j,*} + \sum_{j \in J} \sum_{k=1}^{\nu} \sigma^{\mu}\left(\alpha_k (\mathfrak{b}_k)_j\right) \partial^{\deg \mathfrak{x}_j} M_{j,*} + \sum_{j \notin J} \mathfrak{x}_j M_{j,*}.\end{aligned}$$

For $j \notin J$ we have $\deg \mathfrak{x}_j + \deg M_{j,*} < \delta$. Also, it is $\deg \mathfrak{x}_j - \sum_{k=1}^{\nu} \sigma^{\mu}\left(\alpha_k (\mathfrak{b}_k)_j\right) + \deg M_{j,*} < \delta$ for $j \in J$ since the leading term of $\mathfrak{x}_j$ is cancelled. We thus have to concentrate only on the middle summand. Thus we may rewrite the middle summand above as

$$\begin{aligned}\sum_{j \in J} \sum_{k=1}^{\nu} \sigma^{\mu}\left(\alpha_k (\mathfrak{b}_k)_j\right) \partial^{\deg \mathfrak{x}_j} M_{j,*} &= \sum_{k=1}^{\nu} \sigma^{\mu}(\alpha_k) \partial^{\mu} \sum_{j \in J} (\mathfrak{b}_k)_j \partial^{\deg M_{J,*} - \deg M_{j,*}} M_{j,*} \\ &\quad + \sum_{k=1}^{\nu} \sigma^{\mu}(\alpha_k) \sum_{j \in J} \Big(\sigma^{\mu}\left((\mathfrak{b}_k)_j\right) \partial^{\deg \mathfrak{x}_j} - \partial^{\mu} (\mathfrak{b}_k)_j \partial^{\deg M_{J,*} - \deg M_{j,*}} \Big) M_{j,*}.\end{aligned}$$

Since for all $j \in J$ we have $\delta = \deg \mathfrak{x}_j + \deg M_{j,*} = \deg M_{J,*} + \mu$ and thus $\deg \mathfrak{x}_j = \mu + \deg M_{J,*} - \deg M_{j,*}$, the leading terms in the second summand cancel. Thus, we have to concentrate only on the first summand. Using condition 2, for each $k = 1, \ldots, \nu$ we can find $\mathfrak{z}_k \in R^s$ such that

$$\sum_{j \in J} (\mathfrak{b}_k)_j \partial^{\deg M_{J,*} - \deg M_{j,*}} M_{j,*} = \mathfrak{z}_k M.$$

Since $\mathfrak{b}_k$ is in the nullspace of $\operatorname{LC}_{\text{row}}(M_{J,*})$, the sum on the left hand side has a degree strictly less than $\deg M_{J,*} = \delta - \mu$. This implies by Theorem 5.2 that $\deg (\mathfrak{z}_k)_j M_{j,*} < \deg M_{J,*} \leq \delta - \mu$ for all $j \in J$. Thus, replacing for all $1 \leq k \leq \nu$ the sums $\sum_{j \in J} (\mathfrak{b}_k)_j \partial^{\deg M_{J,*} - \deg M_{j,*}} M_{j,*}$ by the corresponding $\mathfrak{z}_k$, we obtain a representation of $\mathfrak{v}$ as R-linear combination $\tilde{\mathfrak{x}} M$ of the rows of M with $\deg \mathfrak{x}_i + \deg M_{i,*} < \delta$ for all i, contradicting the minimality of $\mathfrak{x}$. Thus, the case $\deg \mathfrak{v} < \delta$ cannot occur. □

Since the second alternative of the case distinction in the proof of the theorem was shown to never occur, we obtain the following corollary which represents a kind of generalised predictable degree property. See Lemma 5.11 for the original predictable degree property.

Corollary 5.8. *Let $M \in {}^sR^t$ be a row basis, and let $\mathfrak{v} \in R^s M$. Assume that $\mathfrak{x}$ is given such that $\mathfrak{x} M = \mathfrak{v}$ and such that $\delta = \max\{\deg \mathfrak{x}_i + \deg M_{i,*} \mid 1 \leq i \leq s\}$ is minimal among all vectors with that property. Then $\deg \mathfrak{v} = \delta$.*

Furthermore, we can identify a class of matrices that are guaranteed to be row bases for their respective row spaces.

Corollary 5.9. *A matrix $M \in {}^sR^t$ is a row basis for R^sM if $\mathrm{LC}_{row}(M)$ has maximal (left) row-rank.*

Proof. The maximality of the rank of $\mathrm{LC}_{\mathrm{row}}(M)$ implies that for every subset $J = \{j_1, \ldots, j_r\} \subseteq \{1, \ldots, s\}$ with $j_1 < \ldots < j_r$ the nullspace of $\mathrm{LC}_{\mathrm{row}}(M_{J,*})$ is $\{0\}$: Assume that $\mathfrak{u}M_{J,*} = 0$ for $\mathfrak{u} \in K^r$. Define $\tilde{\mathfrak{u}}$ entry-wise with the $k_i{}^{\text{th}}$ entry being $\tilde{\mathfrak{u}}_{k_i} = \sigma^{\deg M - \deg M_{J,*}}(\mathfrak{u}_i)$ and all other entries being zero. Then $\tilde{\mathfrak{u}}$ is in the nullspace of $\mathrm{LC}_{\mathrm{row}}(M)$. This implies $\tilde{\mathfrak{u}} = 0$ since the rank of $\mathrm{LC}_{\mathrm{row}}(M)$ is maximal. Hence, also $\mathfrak{u} = 0$ since σ is an automorphism. Thus, condition 2 of the previous theorem is trivially fulfilled and M must be a row basis. □

Matrices whose leading row coefficient matrices have maximal row rank have been studied before which earned them a special name in the literature.

Definition 5.10 ([BCL06, Definition 2.1])**.** A matrix $M \in {}^sR^t$ is called *row-reduced* if $\mathrm{LC}_{\mathrm{row}}(M)$ has maximal (left) row rank.

Some authors call row-reduced matrices *row-proper*, for example, in [Zer07, Section 2.2].

Using the idea from the proof of Theorem 5.7, we can easily prove that the rows of a row-reduced matrix $M \in {}^sR^t$ must be R-linearly independent: Otherwise there was a minimal vector $\mathfrak{x} \setminus \{0\} \in R^s$ such that $\mathfrak{x}M = 0$. Considering again $\delta = \max\{\deg \mathfrak{x}_i + \deg M_{i,*} \mid 1 \le i \le s\}$ and the set $J = \{1 \le i \le s \mid \deg \mathfrak{x}_i + \deg M_{i,*} = \delta\}$. Since M does not have zero-rows and $\mathfrak{x} \neq 0$, there must be at least one $k \in J$ such that $\mathfrak{x}_k \neq 0$ and such that $\deg M_{k,*} \le \delta$. We obtain

$$\sum_{j \in J} \mathrm{lc}(\mathfrak{x}_j)\sigma^{\deg \mathfrak{x}_j}\left(\mathrm{lv}(M_{j,*})\right) = \sum_{j \in J} \mathrm{lc}(\mathfrak{x}_j)\sigma^{\delta - \deg M_{j,*}}\left(\mathrm{lv}(M_{j,*})\right) = \sum_{j \in J} \mathrm{lc}(\mathfrak{x}_j)\mathrm{LC}^{\delta}_{\mathrm{row}}(M)_{j,*}$$

contradicting the independence of the non-zero rows of $\mathrm{LC}^{\delta}_{\mathrm{row}}(M)$. Together with Corollary 5.8 this gives the proof of the so-called *predictable degree property* which was first mentioned in [For75, Main Theorem]. It is interesting that—though the approach of this proof was motivated by row bases—the proof presented here is almost identical to that of [For75, Main Theorem] and of [BCL06, Lemma A.1 (a)] for the Ore case.

Lemma 5.11 (Predictable degree property)**.** *If $M \in {}^sR^t$ is row-reduced then for all $\mathfrak{x} \in R^s$ we have*

$$\deg \mathfrak{x}M = \max\{\deg \mathfrak{x}_i + \deg M_{i,*} \mid 1 \le i \le s\}.$$

In particular the rows of M are linearly independent over R.

Although Theorem 5.7 leads to a kind of *Buchberger's algorithm* for row bases (with the termination being easily provable since the considered vector spaces are finite dimensional), Corollary 5.9 hints of an easier way of computing row bases. For this, the following remark is useful.

Remark 5.12. A matrix $M \in {}^sR^t$ is *auto-reduced* if $M_{k,*}$ is not reducible by $M_{\bar{k},*}$ for all $1 \le k \le s$ and if none of its rows are zero. A matrix can only be auto-reduced if the row rank of its leading row coefficient matrix is maximal, or equivalently if it is row-reduced.

This can be proven analogously to [For75, Main Theorem] and [BCL06, Theorem 2.2]: Assume there was a relation $\mathfrak{u}\mathrm{LC}_{\mathrm{row}}(M) = 0$ with $\mathfrak{u} \in K^s$ such that $\mathfrak{u}_k \neq 0$ and $M_{k,*} \neq 0$ for some $1 \le k \le s$.

We may further assume that $M_{k,*}$ has maximal degree among all those rows $M_{j,*}$ for which $\mathrm{u}_j \neq 0$. Then, we obtain

$$\sigma^{\deg M_{k,*}-\deg M}(\mathrm{u})\,\mathrm{LC}_{\mathrm{row}}^{\deg M_{k,*}}(M) = 0$$

since σ is an automorphism and since those rows that are missing in $\mathrm{LC}_{\mathrm{row}}^{\deg M_{k,*}}(M)$ only correspond to zero entries of u. Noting that $\mathrm{lv}(M_{k,*})$ is just the k^{th} row of $\mathrm{LC}_{\mathrm{row}}^{\deg M_{k,*}}(M)$, we may rewrite this as

$$\mathrm{lv}(M_{k,*}) = \sigma^{\deg M_{k,*}-\deg M}(\mathrm{u}_k^{-1}\mathrm{u}_{\overline{k}}) \cdot \mathrm{LC}_{\mathrm{row}}^{\deg M_{k,*}}(M_{\overline{k},*})$$

where $\mathrm{u}_{\overline{k}}$ denotes u with the k^{th} entry removed. Thus, we see that $M_{k,*}$ is reducible by $M_{\overline{k},*}$.

The previous paragraph yields a naïve algorithm for the row-reduction of a matrix by auto-reduction which is presented, for example, in the proof of [BCL06, Theorem 2.2]. We list it here completely because we want to reason about its complexity below.

Algorithm 5.13 (Row-reduction)**.**

Input A matrix $M \in {}^sR^t$.

Output A row-reduced matrix $N \in {}^sR^t$ and a unimodular transformation matrix $Q \in \mathrm{Gl}_s(R)$ such that $QM = N$.

Procedure

1. Compute $\mathrm{LC}_{\mathrm{row}}(M)$.
2. If there exists $\mathrm{u} \in K^s$ such that $\mathrm{u}\,\mathrm{LC}_{\mathrm{row}}(M) = 0$ and $\mathrm{u}_j \neq 0$ for some j such that $M_{j,*} \neq 0$ then:
   (a) Choose $1 \leq k \leq s$ such that $\mathrm{u}_k \neq 0$ and $\deg M_{k,*}$ is maximal.
   (b) Define $\tilde{\mathrm{u}} \in R^s$ by

$$\tilde{\mathrm{u}}_j = \begin{cases} \sigma^{\deg M_{k,*}-\deg M}(\mathrm{u}_j) \cdot \partial^{\deg M_{k,*}-\deg M_{j,*}}, & \text{if } 0 \leq \deg M_{j,*} \leq \deg M_{k,*} \\ 0, & \text{otherwise.} \end{cases}$$

   (c) Define $P \in \mathrm{Gl}_s(R)$ by

$$P = \begin{pmatrix} 1 & 0 & & & & & 0 \\ 0 & \ddots & & & & & \vdots \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ \tilde{\mathrm{u}}_1 & \cdots & & \tilde{\mathrm{u}}_k & & \cdots & \tilde{\mathrm{u}}_s \\ 0 & \cdots & & 0 & 1 & 0 \cdots & 0 \\ \vdots & & & & \ddots & & 0 \\ 0 & & & & & 0 & 1 \end{pmatrix} \longleftarrow k^{\mathrm{th}} \text{ row}$$

   which is invertible since $\tilde{\mathrm{u}}_k = \sigma^{\deg M_{k,*}-\deg M}(\mathrm{u}_k) \neq 0$. Multiplying this matrix to M from the left will replace the k^{th} row of M by

$$\sum_{\substack{j=1 \\ 0 \leq \deg M_{j,*} \leq \deg M_{k,*}}}^{s} \sigma^{\deg M_{k,*}-\deg M}(\mathrm{u}_j) \cdot \partial^{\deg M_{k,*}-\deg M_{j,*}} M_{j,*}$$

   where the highest order terms cancel.

(d) Apply the algorithm recursively to PM in order to obtain N and Q.
(e) Return N and QP.

3. else return M and $\mathbf{1}_s$.

Of course, the matrix multiplications in the algorithm need not to be carried out as multiplications but can instead be replaced by elementary row operations.

Though we concentrated on the naïve row-reduction algorithm in this chapter, we would like to point out that there are other and more efficient methods. For instance, in [BCL06] the authors present a method for *fraction-free* row-reduction. Another example is [CL07] where *modular* methods are discussed.

5.3 Complexity of (naïve) row reduction

The main step of the naïve row-reduction algorithm is to add a multiple of one row of $M \in {}^sR^t$ to another row. Let $\deg M_{i,*} = m$ and $\deg M_{j,*} = n$. Assume that $f \in R$ has $\deg f = x$. Then by remark (3.2) we need $\mathcal{O}\big(t(x\max\{x,n\} + \max\{m,n\}))\big)$ operations in A in order to compute $M_{i,*} + fM_{j,*}$. In the case of row-reduction we will always have $n \le m$ and $x = m - n$. That yields

$$\mathcal{O}\big(t((m-n)\cdot\max\{m-n,n\} + m)\big)$$

operations. We claim that the term $(m-n)\cdot\max\{m-n,n\}$ is maximized by $n = 0$. Indeed, if $m - n \ge n$ then we have

$$(m-n)^2 = m^2 - 2mn + n^2 \le m^2 - 2mn + mn = m^2 - mn \le m^2$$

and if $m - n \le n$ then $(m-n)n = mn - n^2 \le mn \le m^2$ since $n \le m$. Thus, in the worst case, one elementary row-operation will need

$$\mathcal{O}(tm^2)$$

operations.

Solving a $s \times t$ linear system needs at most $\mathcal{O}(s^2t)$ additions and multiplications in K by [KS89, Bemerkung 2.19 (2)]. That means, that the complete row-reduction process needs at most

$$\mathcal{O}\big(sd\max\{s^2t, td^2\}\big)$$

operations in K where $d = \deg M$ since we need at most most sd iterations of the algorithm.

We state this a a lemma for future reference

Lemma 5.14 (Complexity of naïve row-reduction)**.** *Algorithm 5.13 applied to $M \in {}^sR^t$ needs at most*

$$\mathcal{O}\big(std(\max\{s,d\})^2\big)$$

operations in K where $d = \deg M$. If $Q \in \mathrm{Gl}_s(R)$ and $N \in {}^sR^t$ are the result, then we have $\deg N \le d$ and $\deg Q \le (s+1)d$.

Proof. It remains only to prove the degree bounds. By [BCL06, Theorem 2.2], for each row of Q the degree is

$$\deg Q_{i,*} \le \nu_i + \Big(\sum_{j=1}^{s}(\mu_j - \nu_j) - \min\{\mu_k \mid 1 \le k \le s\}\Big) \le (s+1)d \tag{5.2}$$

where $\nu_j = \max\{\deg N_{j,*}, 0\} \le \mu_j = \max\{\deg M_{j,*}, 0\} \le d$. □

5.4 Some applications of row-reduction

Parallel to our row basis approach, a motivation for studying row-reduced matrices comes from the wish to reduce the degrees of the generators of a submodule as low as possible. This was the original idea in [For75] where row-reduced matrices are labelled *minimal bases*. Decreasing the degrees almost automatically leads to auto-reduction as we have described it above. It is possible to show that the result is indeed minimal in a certain sense. See for example [BCL06, Lemma A.1 (d)] where it is shown that the row-degrees of two row-reduced matrices generating the same row-space coincide up to row permutation.

This leads to an algorithm for inversion of matrices.

Lemma 5.15. *A matrix $M \in {}^sR^s$ is unimodular, if and only if row-reduction of M yields a matrix $N \in {}^sK^s$ of maximal rank.*

In particular, if for $Q \in \mathrm{Gl}_s(R)$ computed by Algorithm 5.13 we have $\deg QM = 0$, that is, $QM \in {}^sK^s$ and the rank of QM is s, then the inverse of M is $M^{-1} = (QM)^{-1}Q$. We can compute the inverse of M—if it exists—using at most $\mathcal{O}\left(s^2 d(\max\{s,d\})^2\right)$ operations where $d = \deg M$. We have $\deg M^{-1} \leq (s+1)\deg M$.

Proof. One direction follows immediately from the minimality: Let M be unimodular. Then $R^sM = R^s$. Since the same space is generated by the identity matrix $\mathbf{1}_s$, [BCL06, Lemma A.1 (d)] implies that the row-degrees of a row-reduced form $N = QM$ with $Q \in \mathrm{Gl}_s(R)$ of M must be all 0. Since $N = \mathrm{LC}_{\mathrm{row}}(N)$ is invertible by the row-reducedness of N, the claim follows.

Contrarily, assume that there exists $Q \in \mathrm{Gl}_s(Q)$ such that $N = QM$ is row-reduced with $\deg N = 0$ and such that the rank of N is maximal. Since N is invertible, we obtain $\mathbf{1}_s = (N^{-1}Q)M$. That means, that M is unimodular and $M^{-1} = N^{-1}Q = (QM)^{-1}M$.

The complexity of row-reduction is discussed in Lemma 5.14. □

Another application for row-reduction is to compute greatest common divisors. In principle, the computation is very similar to the Euclidean algorithm with the main difference being that reduction of a single polynomial may be by several polynomials.

Compare this result also to the computation of matrix greatest common divisors in [BCL06] or [CL07]. See also [BLV06, Example 5.4] where a similar method was used to derived degree bounds on the Bézout cofactors of the extended Euclidean algorithm.

Lemma 5.16. *Let $\mathfrak{v} = {}^t(v_1,\ldots,v_s) \in {}^sR$. If $Q\mathfrak{v}$ is row-reduced for $Q \in \mathrm{Gl}_s(R)$ then*

$$Q\mathfrak{v} = \begin{pmatrix} \mathrm{gcrd}(v_1,\ldots,v_s) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

A similar statement holds for column-reduction and left divisors.

The computations needs at most $\mathcal{O}(sd\max\{s^2,d^2\})$ operations in K and the degree of Q and its inverse—which can be computed in parallel—are at most $(s+1)d$ where $d = \max\{\deg v_j \mid 1 \leq j \leq s\}$.

Proof. If more than two entries of $Q\mathfrak{v}$ were different from zero, then $\mathrm{LC}_{\mathrm{row}}(Q\mathfrak{v}) \in {}^sK$ had a non-trivial left-kernel. Consequently, if $Q\mathfrak{v}$ is row-reduced, then $Q\mathfrak{v} = {}^t(d,0,\ldots,0)$ for some $d \in R$. Since the right

ideal generated by $v_1,\ldots,v_s$ is by the invertibility of Q just

$$Rv_1+\ldots+Rv_s = R^s\mathfrak{v} = R^sQ\mathfrak{v} = Rd$$

and R is a right principal ideal domain, we conclude that d is indeed a greatest common right divisor of $v_1,\ldots,v_s$.

The complexity analysis is done in Lemma 5.14. Since the computation of the inverse Q^{-1} is done using the same row-operations with negative sign, we obtain the same degree bound here. □

6

Hermite normal form, Popov normal form and their connection to Gröbner bases

6.1 The Popov normal form and the shifted Popov normal form

Just as in the previous chapter let K be again a skew field. Furthermore, assume that we are given an automorphism $\sigma: K \to K$ and a σ-derivative $\vartheta: K \to K$. As before, we will abbreviate the Ore polynomial ring $K[\partial;\sigma,\vartheta]$ by R. We use the notations for matrices that were explained in Section 5.1.

This section introduces normal forms of matrices with respect to row-equivalence. Two matrices M and $N \in {}^sR^t$ of same dimensions are *row-equivalent* if there exists a unimodular matrix $Q \in \mathrm{Gl}_s(R)$ such that $M = QN$. Since by Lemma 5.15 matrices may be inverted by row-reduction, that is, by elementary row operations, an equivalent definition of row-equivalence is that N may be transformed into M using elementary row-operations. It is readily seen, that row-equivalence is indeed an equivalence relation on the set of all $s \times t$ matrices over R.

The first normal form which we introduce here is the Popov normal form. This normal form is characterised by the fact that it is row-reduced. Actually, it may be regarded as a way to pick a unique representative among the set of all row-reduced matrices which are row-equivalent to a given matrix. The Popov normal form is called "polynomial-echelon form" by some authors such as in [Kai80, Page 481] or [KRT07].

Definition 6.1 (Popov normal form)**.** A matrix $M \in {}^sR^t$ is in *Popov normal form* if its leading row coefficient matrix (see Section 5.2) $\mathrm{LC}_{\mathrm{row}}(M)$ is of maximal rank, in row echelon form and the entries of M corresponding to the pivots of $\mathrm{LC}_{\mathrm{row}}(M)$ are monic and have the largest degree in their column.

Formally, the last condition can expressed as follows: Let for $1 \le i \le s$ the pivot of the i^{th} row of $\mathrm{LC}_{\mathrm{row}}(M)$ be in column j_i. Then for all $1 \le k \le s$ with $k \neq i$ we must have $\deg M_{i,j_i} > \deg M_{k,j_i}$ in order for M to be in Popov normal form. In this case, we will a little sloppily refer to the entries M_{i,j_i} corresponding to the pivots of $\mathrm{LC}_{\mathrm{row}}(M)$ as the *pivots* of M.

Some authors label a matrix whose leading row coefficient matrix is in row echelon form but which does not necessarily fulfill the other two conditions of the previous definition to be in *weak Popov normal form*. See for example [Che03, Definition 2.7].

Example 6.2. We consider $\mathbb{Q}[X]$. Here, the matrix

$$M = \begin{pmatrix} X & 1-X & X \\ 1 & 1 & X^2-1 \end{pmatrix} \in {}^2\mathbb{Q}[X]^3 \qquad \text{with} \qquad \mathrm{LC}_{\mathrm{row}}(M) = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \in {}^2\mathbb{Q}^3$$

is in Popov normal form, while the matrix

$$B = \begin{pmatrix} 1 & 0 \\ 1 & X \end{pmatrix} \in {}^2\mathbb{Q}[X]^2 \qquad \text{with} \qquad \mathrm{LC}_{\mathrm{row}}(M) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in {}^2\mathbb{Q}^2$$

is not in Popov normal form since $\deg B_{11} = \deg B_{21}$ violates the degree constraint.

In [KRT07, Definition 2] a Popov normal form—called polynomial-echelon form there—is defined in the following way: A matrix $M \in {}^sR^t$ is in Popov normal form if M is row-reduced (see Definition 5.10) with the rows sorted with respect to their degrees and for all rows $M_{i,*}$ there is a column index j_i (called the *pivot index*) such that

1. M_{i,j_i} is monic and $\deg M_{i,j_i} = \deg M_{i,*}$;
2. $\deg M_{i,k} < \deg M_{i,*}$ if $k < j_i$;
3. $\deg M_{k,j_i} < \deg M_{i,*}$ if $k \neq i$; and
4. if $\deg M_{i,*} = \deg M_{k,*}$ and $i < k$, then $j_i < j_k$ (meaning the pivot indices are increasing).

We will take a moment to show that this definition is actually the same as ours—except that we chose to order the rows in a different way. The requirement in [KRT07] that the matrix must be row-reduced corresponds to the condition that the leading row coefficient matrix has full rank in our definition. We are now going to argue that the pivot indices of [KRT07] are nothing else than the column indices of the pivot elements in the leading row coefficient matrix. By point 1 above, the pivots elements of [KRT07] have maximal degree in their respective rows, while point 2 implies that they are the left-most entries with this property. That means, that in the i^{th} row of $\mathrm{LC}_{\mathrm{row}}(M)$ we must have $\mathrm{LC}_{\mathrm{row}}(M)_{i,1} = \ldots = \mathrm{LC}_{\mathrm{row}}(M)_{i,j_i-1} = 0$ and $\mathrm{LC}_{\mathrm{row}}(M)_{i,j_i} = 1$ where the latter equation follows from the requirement that M_{i,j_i} is monic in point 1. We do still have to argue that no two pivot indices of [KRT07] are equal. Otherwise, if j_i and j_k were equal, then by point 3 for the i^{th} row implied that $\deg M_{k,i_j} = \deg M_{k,*} < \deg M_{i,*}$, while the same condition for the k^{th} implied that $\deg M_{i,*} < \deg M_{k,*}$—a contradition. Thus, reordering the rows with respect to their pivot indices we see that $\mathrm{LC}_{\mathrm{row}}(M)$ must be in row echelon form. Finally, by point 3 the pivots of [KRT07] possess the largest degree in their respective column. This is just the same requirement as in our definition.

Completely analogously one proves that a matrix which is in Popov normal form according to Definition 6.1 must be in Popov normal form according to [KRT07].

Just another definition for the Popov normal form is found in [BLV06, Definition 2.1] for square matrices of commutative polynomials. Translating their definition of a column Popov normal form to row Popov normal forms, a matrix $A \in {}^sK[X]^s$ is said to be in Popov normal form if its leading row coefficient matrix $\mathrm{LC}_{\mathrm{row}}(A)$ is upper triangular and its leading column coefficient matrix is the unit matrix. Note that [BLV06] used the alternative way of computing the leading row coefficient matrix

which we already briefly mentioned in Section 5.2: Let $M \in {}^sK[X]^s$. For every row index $1 \le i \le s$, we set $\delta_i = \partial^{\deg M - \deg M_{i,*}}$ if $\deg M_{i,*} \ge 0$ and $\delta_i = 0$ otherwise. With $Z = \operatorname{diag}(\delta_1, \dots, \delta_s)$ we then obtain $\mathrm{LC}_{\mathrm{row}}(M) = \mathrm{lv}(ZM)$. Analogously, the leading column coefficient matrix is computed.

The equivalence of [BLV06, Definition 2.1] to Definition 6.1 is easily seen: If $\mathrm{LC}_{\mathrm{row}}(A)$ is upper triangular, then it is in row echelon form where the pivots are exactly the diagonal entries. If the leading column coefficient matrix of A is $\mathbf{1}_s$, then this means just that the diagonal entries, that is, the pivots are monic and have the largest degree in their column. Again, the other direction is completely analogous.

The Popov normal form definition in [BLV06, Definition 2.1] is a special case of the more general definition of a shifted Popov normal form which we take from [BLV99, Definition 2.1] or, similarly, from [BLV06, Definition 2.3]. Note, that in the refences the definitions are described for column Popov normal forms, while we give them for row Popov normal forms. The definition below is not exactly the definition from these papers, but a characterisation which may be found just below [BLV06, Definition 2.3]. The original definition is very similar to [BLV06, Definition 2.1] which we have explained above.

Definition 6.3 (Shifted Popov normal form)**.** Let $\xi = (\xi_1, \dots, \xi_t) \in \mathbb{N}^t$. We define $\max \xi = \max\{\xi_1, \dots, \xi_t\}$ and $D_\xi = \operatorname{diag}(\partial^{\max\xi - \xi_1}, \dots, \partial^{\max\xi - \xi_t}) \in {}^tR^t$. A matrix $M \in {}^sR^t$ is said to be *ξ-row reduced* if MD_ξ is row-reduced.

We say that M is in *(shifted) ξ-Popov normal form* if MD_ξ is in Popov normal form.

The vector ξ in the definition allows to weight the columns of the matrix in order to make certain columns more important than others. If M is in ξ-Popov normal form, then we will—analogously to the usual Popov normal form—refer to the pivots of MD_ξ as the (ξ-) pivots of M. It is obvious that a 0-Popov normal form is just a Popov normal form in the usual sense.

In [BLV06, Definition 2.3], commutative polynomials in $K[X]$ were treated and the shift ξ was applied with negative weight, that is, in the form $\tilde{D}_\xi = \operatorname{diag}(X^{-\xi_1}, \dots, X^{-\xi_t})$. This allows negative powers of X to occur in the entries of $M\tilde{D}_\xi$. Due to the complications of fractions in non-commutative domains—see Section 3.5—we decided to take a different approach which keeps all terms occuring in the matrix in $R = K[\partial; \sigma, \vartheta]$.

Example 6.4. Consider a commutative polynomial ring $\mathbb{Q}[X]$. Consider the matrix

$$M = \begin{pmatrix} 3X & -3X & 2 & 1 \\ 4 + X + 2X^2 & -2 - X - 2X^2 & 0 & 1 \end{pmatrix} \in {}^2\mathbb{Q}[X]^4$$

which is similar to the one in [BLV06, Example 2.4]. Since

$$\mathrm{LC}_{\mathrm{row}}(M) = \begin{pmatrix} 3 & -3 & 0 & 0 \\ 2 & -2 & 0 & 0 \end{pmatrix}$$

the matrix M is not row-reduced.

Let now $\xi = (2, 2, 0, 0)$. Then we have $\max \xi = 2$ and $D_\xi = \operatorname{diag}(1, 1, X^2, X^2)$. Thus, it is

$$MD_\xi = \begin{pmatrix} 3X & -3X & 2X^2 & X^2 \\ 4 + X + 2X^2 & -2 - X - 2X^2 & 0 & X^2 \end{pmatrix}$$

and hence

$$\mathrm{LC}_{\mathrm{row}}(MD_\xi) = \begin{pmatrix} 0 & 0 & 2 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

We see that M is ξ-row reduced, but not in ξ-Popov normal form.

A Popov normal form may be computed analogously to row-reduction in Algorithm 5.13. First, the matrix $M \in {}^sR^t$ is brought into row-reduced form. For simplicity, we assume that no zero-rows occur here. Then elementary row-operations are used to bring the leading row coefficient matrix into row echelon form. Here it is important to always choose the pivots in such a way that they are of lowest possible degree. We emphasize that these operations cannot change the degrees of the rows, since that would mean that there has been a relation $\mathfrak{v} \in K^s$ with $\mathfrak{v}\,\mathrm{LC}_{\mathrm{row}}(M) = 0$. Alternatively, this follows from [BCL06, Lemma A.1 (d)] as well. Now, make the pivots monic. The last step is to ensure the degree condition. We are now going to prove that this does not disturb the fact that the leading row coefficient matrix is in row echelon form. Assume that $1 \leq i < k \leq s$ and that $M_{i,*}$ has its pivot in column j_i and that that of $M_{k,*}$ is in column j_k. Since $\mathrm{LC}_{\mathrm{row}}(M)$ is in row echelon form we must have $j_i > j_k$. Assume further that $\deg M_{i,j_k} \geq \deg M_{k,j_k}$. Euclidean division yields $M_{i,j_k} = qM_{k,j_k} + r$ with $q, r \in R$ and $\deg r < \deg M_{k,j_k}$. We claim that $M_{i,*} - qM_{k,*}$ still has its pivot in column j_i. Since $\deg M_{i,j_k} \leq \deg M_{i,*} = \deg M_{i,j_i}$, we see that $\deg q \leq \deg M_{i,*} - \deg M_{k,j_k}$. Since $\deg M_{k,\nu} < \deg M_{k,j_k}$ for $\nu < j_k$ and thus in particular for $\nu \leq j_i$, we have $\deg qM_{k,\nu} < \deg M_{i,*}$ for those ν. Thus can the first $j_i - 1$ entries of $M_{i,*} - qM_{k,*}$ have degree at most $\deg M_{i,*} - 1$ and the pivot in column j_i remains undisturbed. Thus, any matrix can be transformed into Popov normal form.

Transformation to ξ-Popov normal form can be done similarly by bringing MD_ξ into Popov normal form. Since R is integral, we may then cancel D_ξ and remain with the ξ-Popov normal form.

Another way to prove that any matrix can be brought into Popov normal form or ξ-Popov normal form for arbitrary $\xi \in \mathbb{N}^t$ will be shown in Corollary 6.31.

In Section 5.3, we have already argued, that an elementary row-operation needs at most $\mathcal{O}(td^2)$ operations in K where $d = \deg M$. Bringing the leading row coefficient matrix into row echelon form needs thus at most $\mathcal{O}(s^2td^2)$ operations where we use that $s \leq t$ since the matrix M was assumed to have full row-rank. Enforcing the degree condition needs again at most $\mathcal{O}(s^2td^2)$ operations since there are exactly s pivots. These transformations are less expensive than the row-reduction itself.

Confer also [Che03, Section 2.5.1] or [MS03] where similar algorithms are discussed. Another method may be found in [DCL08, Theorem 5.5] where computing the Popov normal form of A is reduced to computing a (left) nullspace. The latter can be carried out, for example, by the method described in [BCL06]. The authors do the complexity analysis in terms of the bit complexity.

Since the Popov normal form is in particular row-reduced, by Lemma 5.14 (using again [BCL06, Lemma A.2 (d)] if necessary), we see that the degree of a Popov normal form cannot be higher than the degree of the original matrix. We label this statement for future reference.

Remark 6.5. Let $M \in {}^sR^t$ and $U \in \mathrm{Gl}_s(R)$ be given such that UM is in Popov normal form. Then $\deg M \geq \deg UM$.

This gives us also a rough degree bound for the ξ-Popov normal form: Let for $M \in {}^sR^t$ and $Q \in \mathrm{Gl}_s(R)$ the non-zero rows of QMD_ξ be in Popov normal form. As we have argued above, this implies that QM is in ξ-Popov normal form. Since multiplication by D_ξ can at most enlarge the degree, we have $\deg QM \leq \deg QMD_\xi \leq \deg MD_\xi \leq \deg M + \deg D_\xi \leq \deg M + \max \xi$ by the previous remark and by the definition of D_ξ.

In the case of commutative polynomials, degree bounds can be derived for the degree of the ξ-Popov normal form which are independent on ξ. See for example [BLV06, Theorem 5.1 (b)] and the remark in front of [BLV06, Corollary 6.3].

Also for latter use, we state the following lemma.

Lemma 6.6. *If for $\xi \in \mathbb{N}^t$ the matrix $M \in {}^sR^t$ is in ξ-Popov normal form, then the rows of M are R-linearly independent. In particular matrices in Popov normal form have linearly independent rows.*

Proof. Let D_ξ be the matrix from Definition 6.3. Then M being in ξ-Popov normal form means that $\mathrm{LC}_{\mathrm{row}}(MD_\xi)$ has maximal rank and is in row echelon form. In other words, MD_ξ is row-reduced. By the predictable degree property (Lemma 5.11) the rows of MD_ξ are R-linearly independent. Assume now, that $\mathfrak{v}M = 0$ for $\mathfrak{v} \in R^s$. Then $\mathfrak{v}MD_\xi = 0$ and thus $\mathfrak{v} = 0$ by the independence of the rows of MD_ξ. Thus, the rows of M are R-linearly independent as well. □

6.2 The Hermite normal form

The other normal form we want to treat in this chapter it the Hermite normal form. Roughly speaking, this is a kind of reduced row echelon form with some additional restrictions on the degrees of the entries which serve to make the Hermite normal form uniquely determined. The definition wich we present here is a simplified version of [KRT07, Definition 2][1]. Confer also [GK09, Definition 3.2]. We will show below just before Remark 6.12 that every matrix can be transformed into a matrix with the non-zero rows being in Hermite normal form. Another possible way of computation is given through Gröbner bases—see Corollary 6.31.

Definition 6.7 (Hermite normal form)**.** A matrix $M \in {}^sR^t$ is in *Hermite normal form* if it is in row echelon form with the pivot entries being monic and of largest degree in their respective columns.

More formally, $M \in {}^sR^t$ is in Hermite normal form if there exist column indices $j_1 > j_2 > \ldots > j_s$ which we call *pivot indices* such that

1. $M_{i,k} = 0$ if $k < j_i$;
2. M_{i,j_i} is monic; and
3. $\deg M_{i,j_i} > \deg M_{k,j_i}$ for $k \neq i$.

Also for Hermite normal forms, we will refer to the entries M_{i,j_i} as the *pivots* of M. The context will always make it clear in which sense the word "pivot" is used. Later on, in Remark 6.27, the similar naming will be justified by the fact that the pivots in both cases translate to the same concept in Gröbner basis theory.

Example 6.8. The matrix

$$M = \begin{pmatrix} 1 & 1 & X^2 \\ 0 & X & X^2-1 \end{pmatrix} \in {}^2\mathbb{Q}[X]^3$$

is in Hermite normal form with the pivot indices being 1 and 2. As $\mathrm{LC}_{\mathrm{row}}(M)$ has linearly dependent rows, this example shows that a matrix in Hermite normal form needs not to be row-reduced.

The first property which we like to point out is the independence of the rows of a Hermite normal form. For later reference, we state this as a remark.

Remark 6.9. Since a matrix in Hermite normal form is essentially in row echelon form, it follows immediately that its rows must be R-linearly independent.

[1] Please note that this reference contains a typo: Row-reducedness (called "row-properness" there) is there required for a matrix to be in Hermite normal form—which does contradict the other assumptions. The other sources do not mention it.

The next property concerns the connection between Hermite normal forms and Popov normal forms: In [BLV06, Lemma 2.6] it has been proved that in the ordinary polynomial case a ξ-Popov normal form is already in Hermite normal form if $\xi \in \mathbb{N}^t$ is chosen in a certain way. This translates easily to the Ore polynomial case.

Lemma 6.10 ([BLV06, Lemma 2.6])**.** *Let $\xi \in \mathbb{N}^t$ and assume that $M \in R^t$ is in ξ-Popov normal form with the pivot of the i^{th} row being in the $j_i{}^{th}$ column for all $1 \leq i \leq s$. If ξ fulfills*

$$\xi_{j_i} - \xi_k \geq \deg M_{i,j_i}$$

for all row-indices i and all $k < j_i$, then up to row-permutation M is in Hermite normal form with the same pivots.

Proof. Let $1 \leq i \leq s$. We consider the pivot of M at position (i, j_i). Let $k < j_i$. Our goal is to prove that $M_{i,k} = 0$. Assume this was not the case. Then $(MD_\xi)_{i,k}$ has the degree $\deg M_{i,k} + \max \xi - \xi_k$ where D_ξ is the matrix from Definition 6.3. Since the pivot is at position (i, j_i) and $\mathrm{LC}_{\mathrm{row}}(MD_\xi)$ is in row echelon form, we obtain

$$\deg M_{i,j_i} + \max \xi - \xi_{j_i} > \deg M_{i,k} + \max \xi - \xi_k$$

or, equivalently, using the condition on ξ

$$\deg M_{i,j_i} > \deg M_{i,k} + \xi_{j_i} - \xi_k \geq \deg M_{i,k} + \deg M_{i,j_i}$$

which is a contradiction. Thus, $M_{i,k}$ must be zero, and we have shown that the pivots are the left-most non-zero entries in their respective rows. Furthermore, they are monic by Definition 6.3 and—since the shift ξ is applied column-wise—of largest degree in their column. Thus, all conditions of Definition 6.7 are fulfilled. □

It is easy to see that for all Hermite normal forms there exists a ξ such that the matrix is also in ξ-Popov normal form: For this, we use an idea of [BLV06]. Let $MR^s t$ be in Hermite normal form, and let $d = \deg M$. Define $\xi = (0, d, 2d, \ldots, (t-1)d)$. Then, every non-zero entry in the last column of MD_ξ has a degree which is less than that of every non-zero entry in any other column. Thus, a pivot of $\mathrm{LC}_{\mathrm{row}}(MD_\xi)$ can only be in the last column if it corresponds to the first non-zero entry of MD_ξ. Since M is in Hermite normal form, this means that this entry must already be a pivot of M in the Hermite normal form sense. Similarly, we see that the pivots in the other columns are the same in the Hermite normal form sense and in the ξ-Popov normal form sense. Thus, M is in ξ-Popov normal form.

We give an example for the lemma.

Example 6.11. Consider

$$M = \begin{pmatrix} 1 & 1 & X^2 \\ 0 & X & X-1 \end{pmatrix} \in {}^2Q(X)^3$$

and $\xi = (0, 4, 8)$. We have $\partial_\xi = (\partial^8, \partial^4, 1)$ in Definition 6.3, and since

$$\mathrm{LC}_{\mathrm{row}}(MD_\xi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

we see that M is in ξ-Popov normal form with pivots in the positions $(1,1)$ and $(2,2)$. Since we do have $\xi_2 - \xi_1 = 4 \geq \deg M_{2,2} = 1$, we conclude that M is in Popov normal form. Of course, this could also easily be seen directly in this case.

Conversion of a matrix $M \in {}^sR^t$ into Hermite normal form can be done using the Euclidean algorithm in the form of Lemma 5.16. Assume that the first non-zero column of M has index j. Applying the lemma to it yields $Q \in \mathrm{Gl}_s(R)$ such that

$$QM = \begin{pmatrix} 0 & \cdots & 0 & g & * & \cdots & * \\ \vdots & & \vdots & 0 & & & \\ \vdots & & \vdots & \vdots & & \tilde{M} & \\ 0 & \cdots & 0 & 0 & & & \end{pmatrix}$$

where $\tilde{M} \in {}^{s-j-1}R^{t-1}$. We can proceed recursively with $\tilde{M}$ obtaining a matrix in row echelon form. Enforcing the degree constraint can be done exactly as with the Popov normal form. Note that the row echelon form cannot be disturbed since the entries left of the pivots are all zero.

This algorithm shows that every matrix can be transformed into Hermite normal form. Also we may conclude that the first pivot is alway a greatest common right divisor of the entries of the first non-zero column of the original matrix: This is easy to see once we proved the uniqueness of the Hermite normal form in Corollary 6.31. Another way to see this is to use Lemma 5.16. Since we will need this fact later, we write it down as remark.

Remark 6.12. Let $M \in {}^sR^t$ and $U \in \mathrm{Gl}_s(R)$ be given such that UM is in Hermite normal form. Then the first pivot of UM is always a greatest common right divisor of the entries of the first non-zero column of M.

We will need a degree bound for the Hermite normal form of a matrix later similar to that we derived for Popov normal forms in Remark 6.5. For quadratic matrices over commutative fields such a bound can be found in [GK09, Corollary 3.4]. It is straightforward to generalise this to our case which we will do in the remainder of this section. The proofs are essentially the same as in the reference with the only exception being the integration of the number of columns in appropriate places.

Theorem 6.13. *[GK09, Theorem 3.3] Let $M \in {}^sR^t$ with $\deg M \leq d$ and full row rank. Let $UM = H$ for a unimodular matrix $U \in \mathrm{Gl}_s(R)$ and $H \in {}^sR^t$ being in Hermite normal form having no zero rows. Then there exists a unimodular $V \in \mathrm{Gl}_s(R)$ such that $M = VH$, $UV = \mathbf{1}_s$ and $\deg V \leq d$.*

Proof. Since U is unimodular, the inverse V trivially exists. Let $j_1 > \ldots > j_s$ be the pivot indices of H. We prove the claim about the degree of V by induction on the column index i of V. For $i = 1$ from Remark 6.12 we obtain that $0 \neq H_{1,j_1} = \mathrm{gcrd}(M_{*,j_1})$. Thus $\deg H_{1,j_1} \leq d$, and from $V_{*,1}H_{1,j_1} = A_{*,j_1}$ we conclude that $\deg V_{*,1} \leq d$.

Assume now that $i \leq t$ and that for $1 \leq k < i \leq t$ we know that $\deg V_{k,*} \leq d$. We will now prove that also $\deg V_{i,*} \leq d$. For this we need to distinguish two cases: If $\deg V_{i,*} \leq \max\{\deg V_{k,*} \mid k < i\} \leq d$ then there is nothing to do. Otherwise, if $\deg V_{i,*} > \max\{\deg V_{k,*} \mid k < i\}$, then since by Definition 6.7 $\deg H_{i,j_i} > \max\{\deg H_{k,j_i} \mid 1 \leq k < s\}$, for $1 \leq v \leq t$ we obtain $\deg M_{v,j_i} = \deg V_{v,i}H_{i,j_i}$ because $M_{v,j_i} = \sum_{\mu=1}^{i} V_{v,\mu}H_{\mu,j_i}$ and all the other terms are of lower degree by our assumptions. Since v was arbitrary, we conclude $\deg V_{i,*} \leq d$. By induction the claim follows. □

In [GK09], two corollaries are extracted from this theorem which we state in the following.

Corollary 6.14 ([GK09, Corollary 3.3])**.** *Let M, U and V be as in Theorem 6.13. Then* $\deg U \leq (s-1)\deg M$.

Proof. By Lemma 5.15 we know that row-reduction applied to V yields a matrix in $\mathrm{Gl}_s(K)$. Without loss of generality, we may assume that the row-reduced form of V is $\mathbf{1}_s$. Moreover, since $\mathbf{1}_s = UV$ using the uniqueness of the inverse we can compute the degree bound on U by [BCL06, Theorem 2.2]. Since—with the notation of [BCL06, Theorem 2.2]—it is $\nu_j = \deg(\mathbf{1}_m)_{j,*} = 0$ for all j, we obtain

$$\deg U_{j,*} \leq \nu_j + \sum_{k=1}^{s} (\mu_j - \nu_j) - \min\{\mu_k \mid k = 1,\dots,m\} \leq \sum_{k=1}^{s} \mu_j - \min\{\mu_k \mid k = 1,\dots,m\}.$$

Now, the bound on $d \geq \deg V \geq \mu_j$ for all j that was obtained in Theorem 6.13 implies $\deg U_{j,*} \leq (s-1)d$. □

This corollary immediately yields.

Corollary 6.15 ([GK09, Corollary 3.4])**.** *Let M and H be as in Theorem 6.13. Then* $\deg H \leq s \deg M$.

Proof. We have $\deg H = \deg(UM) \leq \deg U + \deg M = s \deg M$ by the usual rules for matrix degrees and the previous corollary. □

6.3 Gröbner bases for modules over Ore polynomials

Invented by Bruno Buchberger in his Ph. D. thesis [Buc65], Gröbner bases have since then become an important tool in computer algebra. Their most prominent application is—without doubt—solving polynomial equations. But they can be used also for a variety of other tasks like checking ideal equality or computing ideal intersections. They may also be applied to more exotic problems such as theorem proving (see, for example, [GG03, Section 24.1]), reachability in Petri nets (for example, in [GG03, Section 24.2]), graph colouring (for example, in [AL94, Section 2.7]) or integer programming (see, for example, [AL94, Section 2.8]).

Gröbner bases were originally developed for ideals in rings of commutative and multivariate polynomials with coefficients coming from a field. Later on, extensions were made. First, Gröbner bases can be defined for modules over such polynomial rings. See, for example, [AL94, Chapter 3]. Second, extensions to polynomials over more general rings have been made. We mentioned this already in Section 5.2. Confer, for example, [Pau07] for a possible approach to this. Third, there are generalisations to differential polynomials (not to be confused with differential operators). Here, we refer to [CF07] or [Man91]. Note that in this setting the termination of Buchberger's algorithm is usually not given.

Finally, Gröbner bases have been ported to non-commutative rings as well. This seems first to have appeared in [Ber78] for free algebras. In [CS98] so-called *Ore algebras* were considered—iterated Ore polynomial rings with the additional condition that the indeterminates commute with each other. Confer also [Lev05] who treats so called G-algebras.

In this thesis we chose to use the presentation of Gröbner bases from [BGTV03] where Gröbner bases are discussed for Poincaré-Birkhoff-Witt rings. Poincaré-Birkhoff-Witt rings are a class of non-commutative rings with a commutation rule that is slightly more involved than that of Ore polynomials—see [BGTV03, Definition 2.2.5]. However, Ore polynomials (and more generally even Ore algebras) are a subset of Poincaré-Birkhoff-Witt rings as proved in [BGTV03, Corollary 2.3.3]. Thus we can utilize the results of [BGTV03] for our purposes. They have a comprehensive chapter on Gröbner bases for free modules which—in the form of row-spaces of matrices—is our main concern.

In this section, we will briefly summarise the results from [BGTV03, Chapter 5] for the convenience of the reader and also in order to adapt the notation to our simple case of Ore polynomials.

Let K be again a skew field with automorphism $\sigma\colon K \to K$ and σ-derivative $\vartheta\colon K \to K$. As before, we set $R = K[\partial;\sigma,\vartheta]$. For some $t \geq 1$, we consider the free module R^t of row-vectors of length t. Let $\mathfrak{e}_1,\ldots,\mathfrak{e}_t$ denote the canonical basis of R^t, that is, for $1 \leq i \leq t$ the vector $\mathfrak{e}_i$ has all its entries equal to zero except for the i^{th} one which is just the unit of R. A *monomial* in R^t is then defined to be an expression of the form $\partial^\alpha \mathfrak{e}_i$ where $\alpha \geq 0$ is a non-negative integer and $1 \leq i \leq t$. Just as in the commutative case we need to order these terms in a sensible way.

Definition 6.16 (Admissible ordering/[BGTV03, Definition 5.3.7])**.** An *admissible term ordering* is a total ordering $<$ on the set of all terms such that

1. $\partial^\alpha \mathfrak{e}_i < \partial^{\alpha+\beta}\mathfrak{e}_i$ for all $\alpha \geq 0$ and $\beta \geq 1$ and all $1 \leq i \leq t$; and
2. $\partial^\alpha \mathfrak{e}_i < \partial^\beta \mathfrak{e}_j$ implies $\partial^{\alpha+\gamma}\mathfrak{e}_i < \partial^{\beta+\gamma}\mathfrak{e}_j$ for all α, β and $\gamma \geq 0$ and all $1 \leq i,j \leq t$.

The conditions simply mean that $<$ is compatible with the scalar multiplication of monomials in R to monomials in R^t. They are exactly the same as for Gröbner bases in free modules over commutative polynomial rings (see, for example, [AL94, Definition 3.5.1]); and very similar in spirit of admissible orderings for Gröbner bases of ideals (confer, for example, [Win96, Definition 8.2.1]).

As usual, we will write $\partial^\alpha \mathfrak{e}_i \leq \partial^\beta \mathfrak{e}_j$ for $\partial^\alpha \mathfrak{e}_i = \partial^\beta \mathfrak{e}_j$ or $\partial^\alpha \mathfrak{e}_i < \partial^\beta \mathfrak{e}_j$, and we write $\partial^\alpha \mathfrak{e}_i > \partial^\beta \mathfrak{e}_j$ for $\partial^\beta \mathfrak{e}_j < \partial^\alpha \mathfrak{e}_i$ and similarly for "$\geq$".

The only possible admissible ordering on the univariate ring R is to have $\partial^\alpha < \partial^\beta$ if and only if $\alpha < \beta$. This makes R into a Poincaré-Birkhoff-Witt ring—confer again [BGTV03, Definition 2.2.5]. There are two standard ways for extending an order from the ground ring to the free module: the term over position ordering and the position over term ordering. Both can be found in [BGTV03, Definitions 5.3.8 and 5.3.9], but we will repeat them here for the convenience of the reader. Note, that the definitions we give are not exactly the same since we chose to order the *positions*, that is, the basis vectors $\mathfrak{e}_1,\ldots,\mathfrak{e}_t$ differently. This is done in order to match the Hermite normal form and Popov normal form definitions as will be explained below in the Theorems 6.30 and 6.28.

We start with the term over position ordering. Here, the degrees of the monomials, the terms, obtain more attention than the positions.

Definition 6.17 (Term over position ordering/[BGTV03, Definition 5.3.8])**.** Let α and $\beta \geq 0$ and $1 \leq i,j \leq t$. Then $\partial^\alpha \mathfrak{e}_i$ is smaller than $\partial^\beta \mathfrak{e}_j$ with respect to the *term over position ordering* if and only if either $\alpha < \beta$ or $\alpha = \beta$ and $i > j$. In this case, we write $\partial^\alpha \mathfrak{e}_i <_{\text{TOP}} \partial^\beta \mathfrak{e}_j$.

An equivalent way to define the term over position ordering is to say that $\partial^\alpha \mathfrak{e}_i <_{\text{TOP}} \partial^\beta \mathfrak{e}_j$ if and only if $(\alpha,-i) <_{\text{lex}} (\beta,-j)$ where $<_{\text{lex}}$ denotes the usual lexicographic ordering. (Confer, for example, [Win96, Example 8.2.1 a] for the lexicographic ordering.) We have to multiply the position indices with minus one since we chose to order them ascendingly, that is, we have chosen to have $\mathfrak{e}_i >_{\text{TOP}} \mathfrak{e}_j$ if and only if $i > j$.

Since the degree is considered first, the term over position ordering acts similar to a graded ordering. (See, for example, [Win96, Example 8.2.1 b] for a definition of a graded ordering). We have

$$\begin{aligned}(0,\ldots,0,1) <_{\text{TOP}} (0,\ldots,0,1,0) <_{\text{TOP}} \ldots <_{\text{TOP}} (1,0,\ldots,0) <_{\text{TOP}} \ldots \\ <_{\text{TOP}} (0,\ldots,0,\partial) <_{\text{TOP}} (0,\ldots,0,\partial,0) <_{\text{TOP}} (\partial,0,\ldots,0) <_{\text{TOP}} \ldots \\ <_{\text{TOP}} (0,\ldots,0,\partial^2) <_{\text{TOP}} (0,\ldots,0,\partial^2,0) <_{\text{TOP}} (\partial^2,0,\ldots,0) <_{\text{TOP}} \ldots,\end{aligned}$$

just as one would expect for a graded ordering. This illustrates well that higher degree terms are always larger than lower degree terms and that terms of equal degree are sorted from right to left, that is, the term with the left-most position is always the largest.

We will now define the position over term ordering. In contrast to the term over position ordering defined above, here the position have more weight than the degrees of the terms.

Definition 6.18 (Position over term ordering/[BGTV03, Definition 5.3.9])**.** Let again α and $\beta \geq 0$ and $1 \leq i, j \leq t$. Then $\partial^\alpha \mathfrak{e}_i$ is smaller than $\partial^\beta \mathfrak{e}_j$ with respect to the *position over term ordering* if and only if either $i > j$ or $i = j$ and $\alpha < \beta$. This is denoted by $\partial^\alpha \mathfrak{e}_i <_{\text{POT}} \partial^\beta \mathfrak{e}_j$.

Also the position over term ordering can be defined in terms of the lexicographic ordering: We have $\partial^\alpha \mathfrak{e}_i <_{\text{POT}} \partial^\beta \mathfrak{e}_j$ if and only if $(-i, \alpha) <_{\text{lex}} (-j, \beta)$. Again, the position indices are negated to obtain an ascending order. Analogously to the term over position ordering, the position over term ordering has a strong connection to an ordering from polynomial algebra. Namely, it acts as a kind of lexicographic ordering. The sequence of monomials runs as

$$\begin{aligned}(0,\dots,0,1) <_{\text{POT}} (0,\dots,0,\partial) <_{\text{POT}} (0,\dots,0,\partial^2) <_{\text{POT}} \dots <_{\text{POT}} (0,\dots,0,1,0) <_{\text{POT}} (0,\dots,0,\partial,0)\\ <_{\text{POT}} (0,\dots,0,\partial^2,0) <_{\text{POT}} \dots <_{\text{POT}} (1,0,\dots,0) <_{\text{POT}} (\partial,0,\dots,0) <_{\text{POT}} (\partial^2,0,\dots,0) <_{\text{POT}} \dots\end{aligned}$$

with all $\partial^\alpha \mathfrak{e}_t$ being smaller than any $\partial^\beta \mathfrak{e}_{t-1}$ and so on.

There is another kind of ordering, which we will later link to the ξ-Popov normal form.

Definition 6.19 (ξ-term over position ordering)**.** Let $\xi \in \mathbb{N}^t$ be given. For α and $\beta \geq 0$ and $1 \leq i, j \leq t$, we say that $\partial^\alpha \mathfrak{e}_i$ is smaller than $\partial^\beta \mathfrak{e}_j$ with respect to the *ξ-term over position ordering* if either $\alpha - \xi_i < \beta - \xi_j$ or $\alpha - \xi_i = \beta - \xi_j$ and $i > j$. We will write this as $\partial^\alpha \mathfrak{e}_i <_{\text{TOP},\xi} \partial^\beta \mathfrak{e}_j$.

For $\xi = 0$ we obviously obtain just the term over position ordering. Like this, the ξ-term over position ordering can be expressed via the lexicographic ordering. We have $\partial^\alpha \mathfrak{e}_i <_{\text{TOP},\xi} \partial^\beta \mathfrak{e}_j$ if and only if $(\alpha - \xi_i, -i) <_{\text{lex}} (\beta - \xi_j, -j)$. Again, the negative second components are due to our ordering of the positions. This translation to the lexicographic ordering also immediately implies that the ξ-term over position ordering is admissible: For all α, β and $\gamma \geq 0$ as well as $1 \leq i, j \leq t$ we have $\partial^\alpha \mathfrak{e}_i <_{\text{TOP},\xi} \partial^\beta \mathfrak{e}_j$ if and only if $(\alpha - \xi_i, -i) <_{\text{lex}} (\beta - \xi_j, -j)$ which—since the lexicographic ordering is admissible—implies $(\alpha - \xi_i + \gamma, -i) <_{\text{lex}} (\beta - \xi_j + \gamma, -j)$ which is equivalent to $\partial^{\alpha+\gamma} \mathfrak{e}_i <_{\text{TOP},\xi} \partial^{\beta+\gamma} \mathfrak{e}_j$; and similarly for the first condition of Definition 6.16.

Another way of interpreting the ξ-term over position ordering is to use the matrix D_ξ that was defined in Definition 6.3. It is easy to check that

$$\partial^\alpha \mathfrak{e}_i <_{\text{TOP},\xi} \partial^\beta \mathfrak{e}_j \iff \partial^\alpha \mathfrak{e}_i D_\xi <_{\text{TOP}} \partial^\beta \mathfrak{e}_j D_\xi$$

for all α, β and $\gamma \geq 0$ and $1 \leq i, j \leq t$. Taking for instance $t = 4$ and $\xi = (2,2,0,0)$ as in Example 6.4 where we had $D_\xi = \operatorname{diag}(1, 1, \partial^2, \partial^2)$, this is illustrated by the following sequence

$$\begin{aligned}(0,1,0,0) <_{\text{TOP},\xi} (1,0,0,0) <_{\text{TOP},\xi} (0,\partial,0,0) <_{\text{TOP},\xi} (\partial,0,0,0) <_{\text{TOP},\xi} (0,0,0,1) <_{\text{TOP},\xi} (0,0,1,0)\\ <_{\text{TOP},\xi} (0,\partial^2,0,0) <_{\text{TOP},\xi} (\partial^2,0,0,0) <_{\text{TOP},\xi} (0,0,0,\partial) <_{\text{TOP},\xi} (0,0,\partial,0) <_{\text{TOP},\xi} (0,\partial^3,0,0)\\ <_{\text{TOP},\xi} (\partial^3,0,0,0) <_{\text{TOP},\xi} (0,0,0,\partial^2) <_{\text{TOP},\xi} (0,0,\partial^2,0) <_{\text{TOP},\xi} (0,0,0,\partial^3) <_{\text{TOP},\xi} (0,0,\partial^3,0)\end{aligned}$$

of all monomials of degree not greater than 3.

We can use [RR97] to characterise all admissible orderings in R^t: The definition of admissible orderings (Definition 6.16) corresponds to *positive rankings* in [RR97, Definition 1]. Furthermore, by [RR97, Theorem 7] (pointing themselves to Caboara & Silvestri), admissible orderings on R^t are *Riquier rankings*: Let $\partial^a \mathfrak{e}_i \le \partial^b \mathfrak{e}_i$. Then we must have $a \le b$ since otherwise $\partial^b \mathfrak{e}_i \le \partial^a \mathfrak{e}_i$ by first condition of Definition 6.16. But then we must have $\partial^a \mathfrak{e}_j \le \partial^b \mathfrak{e}_j$, again by the first condition of Definition 6.16.

Theorem 6.20. *All admissible orders $\le$ in R^t can be described by a matrix $M \in {}^s\mathbb{R}^{t+1}$ for some $s \ge 1$ with $M_{*,1} \ge_{\text{lex}} 0$ such that*

$$\partial^a \mathfrak{e}_i \le \partial^b \mathfrak{e}_j \iff M \begin{pmatrix} a \\ \mathfrak{e}_i \end{pmatrix} \le_{\text{lex}} M \begin{pmatrix} b \\ \mathfrak{e}_j \end{pmatrix}.$$

Proof. This is a special case of [RR97, Theorem 6]. □

Note, that we may always choose $s \le t+1$ because otherwise we would have linear dependend rows which cannot yield a decision if the previous rows did not.

As an example, for $t = 3$ the term over position ordering and position over term ordering are described by the matrices

$$M_{\text{TOP}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad M_{\text{POT}} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

respectively. The matrix for the ξ-term over position ordering is

$$M_{\text{TOP},\xi} = \begin{pmatrix} 1 & -\xi_1 & -\xi_2 & -\xi_3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Another way to obtain all monomial orders on R^t is given by [RR97, Theorem 29]. The construction (already adapted to our case) is the following: Choose real numbers $M_i \in \mathbb{R}$ with $M_i > 0$ and real numbers $\lambda_i \in \mathbb{R}$.[2] Let $s_{ij} = 1$ if $M_i = M_j$ and $s_{ij} = 0$ otherwise. Choose integers u_{ij} satisfying

$$0 \le u_{ij} \le s_{ij}, \qquad u_{ii} = s_{ii} = 1, \qquad u_{ij} = u_{ji}, \qquad \text{and} \qquad u_{ik} \ge \min\{u_{ij}, u_{jk}\}$$

for all $1 \le i,j,k \le n$. Choose a permutation $\sigma\colon \{1,\dots,t\} \to \{1,\dots,t\}$ such that

$$u_{ik} > \min\{u_{ij}, u_{jk}\} \wedge \sigma(i) < \sigma(j) \implies \sigma(k) < \sigma(j).$$

Denote by π_s the projection of a real vector to its first s coordinates. Then we can define an admissible ordering $\le = \le_{M_1,\dots,M_t,\lambda_1,\dots,\lambda_t,\{u_{ij}\},\sigma}$ on all terms by

$$\partial^a \mathfrak{e}_i \le \partial^b \mathfrak{e}_j \iff \begin{pmatrix} u_{ij}(M_i a + \lambda_i) \\ \sigma(i) \end{pmatrix} \le_{\text{lex}} \begin{pmatrix} u_{ij}(M_j a + \lambda_j) \\ \sigma(j) \end{pmatrix}.$$

In [RR97, Theorem 29] it is shown that every admissible ordering has such a representation. We can easily translate the orderings obtained in this way to that in Theorem 6.20: For the upper rows,

[2] In [RR97], the M_i are $s_i \times m$ matrices where $1 \le s_i \le m$ and where m is the number of variables. But in our case we have $m = 1$, and thus are the M_i just numbers.

choose an index i and let $J = \{1 \le j \le n \mid M_i = M_j \wedge u_{ij} = 1\}$. Then a row of the matrix has M_i in the first position and λ_j at the $(j+1)^{\text{th}}$ position for $j \in J$. Do this for all i. The lower rows correspond to the matrix of the permutation σ.

Since the monomials form a K-basis of the left vector space R^t, we may write down every element of R^t as a K-linear combination of monomials in a unique way. Let $\mathfrak{v} \in R^t \setminus \{0\}$ be given and assume that

$$\mathfrak{v} = c_1\mathfrak{m}_1 + \ldots + c_r\mathfrak{m}_r$$

where $c_1, \ldots, c_r \in K \setminus \{0\}$ and $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ are pairwise different monomials. Let now an admissible ordering $<$ be given, and assume that $\mathfrak{m}_1 > \ldots > \mathfrak{m}_r$. In this case, we will call $\mathfrak{m}_1$ the *leading monomial* of $\mathfrak{v}$ with respect to $<$ and write $\mathfrak{m}_1 = \mathrm{lm}_<(\mathfrak{v})$. The coefficient c_1 is called the *leading coefficient* of $\mathfrak{v}$ with respect to $<$ which we denote by $c_1 = \mathrm{lc}_<(\mathfrak{v})$. Furthermore, the *leading term* of $\mathfrak{v}$ is $\mathrm{lt}_<(\mathfrak{v}) = c_1\mathfrak{m}_1 = \mathrm{lc}_<(\mathfrak{v})\mathrm{lm}_<(\mathfrak{v})$. If no confusion is possible, we will usually just write $\mathrm{lm}(\mathfrak{v})$ for $\mathrm{lm}_<(\mathfrak{v})$ and similar for the leading coefficient and the leading term. The leading monomial, coefficient and term of the zero vector remain undefined.

At this point, we emphasize the differences to the definitions for row bases in Section 5.2: The leading coefficient defined here is a single element of K while the leading vector defined in Section 5.2 is a vector in K^t. The concept of the leading monomial is roughly equivalent to the use of the degree in Section 5.2.

The next step is to define reduction. This is the point where the Gröbner basis theory deviates from the row basis theory of Section 5.2—although the names are similar. The latter is of course to be expected since our row bases theory itself is derived from a version of Gröbner basis theory.

Definition 6.21 (Reduction)**.** Let $F \subseteq R^t \setminus \{0\}$, and let $\mathfrak{v} = c_1\mathfrak{m}_1 + \ldots + c_r\mathfrak{m}_r \in R^t$ where $c_1, \ldots, c_r \in K \setminus \{0\}$ and $\mathfrak{m}_1 > \ldots > \mathfrak{m}_r$ are monomials in R^t. Then $\mathfrak{v}$ is said to be *reducible* by F if there are $1 \le i \le r$, an element $\mathfrak{f} \in F$ and $\gamma \ge 0$ such that $\mathfrak{m}_i = \partial^\gamma \mathrm{lm}(\mathfrak{f})$.

We call $\mathfrak{v}$ *irreducible* by F if it is not reducible by F.

Note that the zero vector is always irreducible.

Just as in the usual Gröbner basis theory or just as for row bases, reducibility implies that terms in a vector may be replaced by terms which are smaller with respect to the admissible ordering chosen. More precisely, if $\mathfrak{v} \in R^t$ is reducible by $F \subseteq R^t \setminus \{0\}$, that is, if there is a monomial $\mathfrak{m}_i$ occuring in $\mathfrak{v}$ with non-zero coefficient c_i and there is $\mathfrak{f} \in F$ such that there is a $\gamma \ge 0$ with $\mathfrak{m}_i = \partial^\gamma \mathrm{lm}(\mathfrak{f})$, then in

$$\mathfrak{v} - c_i\,\sigma^\gamma(\mathrm{lt}(\mathfrak{f})^{-1})\,\partial^\gamma \mathfrak{f}$$

the monomial $\mathfrak{m}_i$ no longer appears. Instead the smaller monomials from ∂^γ are substituted. This observation yields the Gröbner basis division algorithm.

Theorem 6.22 (Division algorithm/[BGTV03, Theorem 5.4.3])**.** *Fix an admissible ordring $<$. Given a vector $\mathfrak{v} \in R^t$ and $F = \{\mathfrak{f}_1, \ldots, \mathfrak{f}_k\} \subseteq R^t \setminus \{0\}$ there exist $u_1, \ldots, u_k \in R$ and $\mathfrak{r} \in R^t$ such that*

$$\mathfrak{v} = u_1\mathfrak{f}_1 + \ldots + u_k\mathfrak{f}_k + \mathfrak{r}$$

where

1. *$\mathfrak{r}$ is irreducible by F;*
2. *$\mathfrak{r} = 0$ or $\mathrm{lm}(r) \le \mathrm{lm}(\mathfrak{v})$; and*

3. *for* $1 \le i \le k$ *we have either* $u_i = 0$ *or* $\mathrm{lm}(u_i \mathfrak{f}_i) \le \mathrm{lm}(\mathfrak{v})$.

In this case, we call $\mathfrak{r}$ *the* remainder *of* $\mathfrak{v}$ *by division with* F.

The elements $u_1, \ldots, u_k$ from the previous theorem can be computed; the procedure is explained in [BGTV03, Algorithm 10]. Note that the algorithm is inherently non-deterministic since reduction might be possible by several elements of which one is chosen randomly. In [BGTV03, Example 5.4.5] the reader may find an example for the division algorithm applied to a module over the Weyl algebra.

With the division explained, we are now ready to come to the definition of a Gröbner basis. Instead of taking [BGTV03, Definition 5.4.7] directly, we use a different formulation which is shown to be equivalent in [BGTV03, Theorem 5.4.9].

Definition 6.23 (Gröbner basis)**.** Let $\mathfrak{M} \trianglelefteq R^t$ be a (left R-) submodule of R^t. A finite subset $G \subseteq \mathfrak{M} \setminus \{0\}$ is said to be a *Gröbner basis* for $\mathfrak{M}$ if for all $\mathfrak{v} \in R^t$ the remainder by division with G is zero if and only if $\mathfrak{v} \in \mathfrak{M}$.

Just as in the usual Gröbner basis theory one obtains the following results.

Lemma 6.24. *Every submodule* $\mathfrak{M} \trianglelefteq R^t$ *has a Gröbner basis* G*, the elements of* G *generate* $\mathfrak{M}$ *and the result of the division algorithm 6.22 applied to* $\mathfrak{v} \in R^t$ *and* G *does not depend on the order of the elements in* G.

Proof. These statements may be found in [BGTV03, Proposition 5.4.8, Corollary 4.10 and Theorem 5.4.9]. □

For a given module the Gröbner basis as defined above is not yet unique since, for example, adding more elements to a Gröbner basis cannot destroy the Gröbner basis property. Therefore, we need to introduce additional conditions.

Definition 6.25 (Reduced Gröbner basis/[BGTV03, Definition 5.4.17])**.** A Gröbner basis G for $\mathfrak{M} \trianglelefteq R^t$ is *reduced* if for all $\mathfrak{g} \in G$ we have $\mathrm{lc}(\mathfrak{g}) = 1$ and $\mathfrak{g}$ is irreducible by $G \setminus \{\mathfrak{g}\}$.

Again just as in the usual Gröbner basis theory for ideals of a commutative polynomial ring, there exists a notion of *S-polynomials* for elements of R^t and a corresponding *Buchberger criterion* for Gröbner bases in R^t. These may be found in [BGTV03, Definition 5.4.11 and Theorem 5.4.13]. They lead to a *Buchberger's algorithm* for R^t that is described in [BGTV03, Algorithm 11] with the proof of the correctness in [BGTV03, Theorem 5.4.16]. We do not repeat these result here since they will not be needed in the following discussion. We do, however, cite a sufficient condition for being a Gröbner basis which can be found in [BGTV03, Corollary 5.4.14] and which will turn out to exactly fit our needs below in the proofs of the Theorems 6.28, Theorems 6.29 and 6.30.

Theorem 6.26 ([BGTV03, Corollary 5.4.14])**.** *Let* $G = \{\mathfrak{g}_1, \ldots, \mathfrak{g}_r\} \subseteq R^n$ *with leading monomials* $\mathrm{lm}(\mathfrak{g}_k) = \partial^{\alpha_k} \mathfrak{e}_{j_k}$ *for* $1 \le k \le r$*. If* $j_i \ne j_k$ *whenever* $i \ne k$ *then* G *is a Gröbner basis for the (left* R*-) submodule* $R\mathfrak{g}_1 + \ldots + R\mathfrak{g}_s \trianglelefteq R^n$ *generated by its elements.*

6.4 Gröbner bases and normal forms

We are now going to draw the connection between the normal forms presented earlier in this chapter and Gröbner bases. The link between normal forms and Gröbner bases is not difficult to notice: For linear polynomials the Buchberger algorithm is essenially the same as computing a row echelon form of the coefficient matrix. See, for example, [AL94, Exercise 1.6.5]. A correspondence between Popov normal form, Hermite normal form and Gröbner bases seems first to have been described in [KRT07] for the case of commutative polynomials. In this section we will generalise their result to Ore polynomials. Also, besides the usual Popov normal form we will consider ξ-Popov normal forms as well.

The main idea in the proofs of the following theorems is to note the parallel between the pivots in the Definitions 6.1, 6.3 and 6.7 and the leading monomials with respect to the term orderings which we have defined above.

Remark 6.27. Let a non-zero vector $\mathfrak{v} \in R^t$ be given.

1. The leading term of $\mathfrak{v}$ with respect to the term over position ordering is the term of highest degree with lowest position index. It corresponds to the left-most non-zero entry of $\mathrm{LC}_{\mathrm{row}}(\mathfrak{v})$.
2. For $\xi \in \mathbb{N}^t$, the leading term of $\mathfrak{v}$ with respect to the ξ-term over position ordering is the left-most term whose degree minus the corresponding entry of ξ is minimal. It corresponds to the left-most non-zero entry of $\mathrm{LC}_{\mathrm{row}}(\mathfrak{v}D_\xi)$ where D_ξ is the matrix from Definition 6.3.
3. The leading term of $\mathfrak{v}$ with respect to the position over term ordering is the highest degree term of the left-most non-zero entry of $\mathfrak{v}$.

Using this idea about the correspondence between leading monomials and pivot elements, we are ready to prove that the Popov normal form, ξ-Popov normal form and Hermite normal form are reduced Gröbner bases for their respective row-spaces.

Althought the Popov normal form is but a special case of the ξ-Popov normal form—as we have seen above—we do want to prove separately that it is a Gröbner basis. Although the following theorem could be regarded merely as a corollary of Theorem 6.28, we feel that the simpler proof gives a better intuition.

Theorem 6.28. *Let $M \in R^{s}t$. Then up to row-permutation M is in Popov normal form if and only if its rows form a reduced term over position Gröbner basis for R^sM.*

Proof. As already mentioned above, the key point of this proof is that the pivots in the sense of Definition 6.1 and the leading monomials with respect to the term over position ordering correspond to each other as explained in point 1 of Remark 6.27.

Assume first that M is in Popov normal form. Since by Definition 6.1 this means that its leading row coefficient matrix is in row echelon form, we see that the pivots—which correspond to the pivots of $\mathrm{LC}_{\mathrm{row}}(M)$—must be in different columns. This means that the leading terms of the rows are at different positions. Thus, by Theorem 6.26 the rows of M form a Gröbner basis. From Definition 6.1 we see that the pivot elements must be monic. Since the leading terms of the rows are just the highest degree terms of the pivots—written at the corresponding position—we obtain that the leading coefficients of the rows are monic. The i^{th} row $M_{i,*}$ can only be reducible by the j^{th} row $M_{j,*}$ if the pivot entry in $M_{j,*}$ does not have a higher degree than the entry of $M_{i,*}$ in the same column. Since by

Definition 6.1 this is impossible for $i \neq j$, we conclude that the rows of M are even a reduced Gröbner basis.

Conversely, let now the rows of M be a reduced Gröbner basis for the row-space of M. We first prove that the leading terms must be at different positions. Assume that was not the case, that is, that $\mathrm{lm}(M_{i,*}) = \partial^\alpha \mathfrak{e}_j$ and also $\mathrm{lm}(M_{k,*}) = \partial^\beta \mathfrak{e}_j$ for some row indices $1 \leq i,k \leq s$. Then, $\alpha \leq \beta$ implies that $M_{k,*}$ is reducible by $M_{i,*}$ which can only be if $i = k$ since the rows are a reduced Gröbner basis—and similarly for $\beta \leq \alpha$. Since the leading terms correspond to the left-most highest degree entries in the rows, this means that the leading vector of each row has its left-most non-zero entry at a different position. Thus, after possibly reordering the rows of M we see that $\mathrm{LC}_{\mathrm{row}}(M)$ is in row echelon form. The pivot elements of $\mathrm{LC}_{\mathrm{row}}(M)$ are monic since the leading terms of the rows of M are. Analogously to how we proved that the leading terms are in different positions, we may conclude that—since the rows of M are a reduced Gröbner basis and thus are not reducible by each other—that the pivot elements have the largest degree in their respective columns. Thus, we have verified all conditions from Definition 6.1. □

A matrix whose rows are a reduced term over position Gröbner basis can be brought into Popov normal form by sorting its rows ascendingly with respect to the positions of their leading monomials. This can be easily seen from the proof since we have shown that the pivot elements correspond to the leading terms.

Theorem 6.29. *Let $M \in {}^sR^t$ and $\xi \in \mathbb{N}^t$. Then up to row-permutation M is in ξ-Popov normal form if and only if its rows form a reduced ξ-term over position Gröbner basis for R^sM.*

Proof. Again, the key insight to this proof will be that the pivots correspond to the leading terms. Assume first, that M is in ξ-Popov normal form with the pivot of the i^{th} row being in column j_i for $1 \leq i \leq s$. Fix an row index i and consider an entry $M_{i,k}$ for $k < j_i$. Since this is left of the pivot, we obtain

$$\begin{aligned}\deg M_{i,k} + \max\xi - \xi_k &= \deg(M_{i,k}\partial^{\max\xi-\xi_k}) = \deg(MD_\xi)_{i,k} \\ &< \deg(MD_\xi)_{i,*} = \deg(MD_\xi)_{i,j_i} = \deg(M_{i,j_i}\partial^{\max\xi-\xi_{j_i}}) = \deg M_{i,j_i} + \max\xi - \xi_{j_i}\end{aligned}$$

where D_ξ is the matrix from Definition 6.3. This is equivalent to

$$\deg M_{i,k} - \xi_k < \deg M_{i,j_i} - \xi_{j_i}$$

meaning that every term of $M_{i,*}$ at position $k < j_i$ is less than the highest degree term at position j_i with respect to the ξ-term over position ordering. Similarly, we can prove that for $\ell > j_i$ we have $\deg M_{i,\ell} - \xi_\ell \leq \deg M_{i,j_i} - \xi_{j_i}$ meaning again that all terms in that positions must be smaller than the highest degree term in position j_i. Thus, the pivots correspond to the leading terms of the rows with respect to the ξ-term over position ordering.

Since $\mathrm{LC}_{\mathrm{row}}(M)$ being in row echelon form implies that the pivots are in different columns and thus the leading terms are in different positions, by Theorem 6.26 we see that the rows of M form a Gröbner basis for R^sM. The leading terms of the rows must be monic since the pivots are 1. Since the shift ξ is applied column-wise, for every $1 \leq i \leq s$ the element M_{i,j_i} has a larger degree than all M_{k,j_i} with $k \neq i$. Since the leading term of the i^{th} row is at position j_i—or, in mathematical notation $\mathrm{lm}(M_{i,*}) = \partial^{\deg M_{i,*}}\mathfrak{e}_{j_i}$—we see that the i^{th} is not reducible by the other rows. Thus, by Definition 6.25 the rows of M are even a reduced Gröbner basis of the row-space of M.

Let on the hand now the rows of M form a reduced Gröbner basis for R^sM. We have to prove that for every $1 \leq i \leq s$ the left-most non-zero entry of the i^{th} row of $\text{LC}_{\text{row}}(MD_\xi)$ correspond to the leading monomial of $M_{i,*}$. Let the leading term be at position j_i and consider $k < j_i$. Then we must have $\deg M_{i,k} - \xi_k \leq \deg M_{i,j_i} - \xi_{j_i}$ since otherwise the leading term was at position k. In fact, since $k < j_i$ we must even have a strict inequality here since the leading term is in the left-most possible position. As before, this implies that

$$\deg(MD_\xi)_{i,k} < \deg(MD_\xi)i, j_i.$$

Analogously, for $\ell > j_i$ we obtain $\deg(MD_\xi)_{i,j_i} \geq \deg(MD_\xi)_{i,\ell}$ since $\deg M_{i,j_i} - \xi_{j_i} \geq \deg M_{i,\ell} - \xi_\ell$. Together, these two inequalities imply that the first non-zero entry of the i^{th} row of $\text{LC}_{\text{row}}(MD_\xi)$ is in column j_i.

Assume now, that for another row index $k \neq i$ we had $j_i = j_k$. Then, $\text{lm}(M_{i,*}) = \partial^\alpha \mathfrak{e}_{j_i}$ and $\text{lm}(M_{k,*}) = \partial^\beta \mathfrak{e}_{j_i}$ meaning that $M_{i,*}$ is reducible by $M_{k,*}$ if $\alpha \geq \beta$ or the other way around for $\beta \geq \alpha$. This contradicts the assumption that the rows of M form a reduced Gröbner basis. Thus, the leading terms are in different positions and hence the first non-zero entries of $\text{LC}_{\text{row}}(MD_\xi)$ are in different columns. After possibly rearrangig the rows, we may thus assume that the leading row coefficient matrix of MD_ξ is in row echelon form. In the same way, as above we may conclude that the entries of MD_ξ corresponding to the pivots of $\text{LC}_{\text{row}}(MD_\xi)$ have maximal degree in their column. Also, they must be monic since the leading terms are. Thus, MD_ξ is in Popov normal form meaning that M is in ξ-Popov normal form according to Definition 6.3. □

Also the next theorem could be seen as a corollary of Theorem 6.29 by Lemma 6.10. But again, we give an alternative proof here.

Theorem 6.30. *Let $M \in {}^sR^t$ have it's rows being sorted with respect to the position over term ordering. Then M is in Hermite normal form if and only if its rows form a reduced position over term Gröbner basis for R^sM.*

Proof. As already twice before, we have primarily to prove that the pivots in the sense of Definition 6.7 correspond to the leading terms of the rows with respect to the position over term ordering. Let first M be in Hermite normal form. Consider the i^{th} row of M for some row-index $1 \leq i \leq s$. Since the leading term is the highest degree term of the left-most non-zero entry of $M_{i,*}$, we see that $\text{lm}(M_{i,*})$ is in the same column as the pivot. Since all pivots are in different columns, we have a Gröbner basis by Theorem 6.26. The pivots are monic and of largest degree in their columns implying that M must be a reduced Gröbner basis.

Conversely, if the rows of M are a reduced Gröbner basis, then no two leading terms can be in the same column or else on of the corresponding rows would be reducible by the other. Since the position over term ordering makes the left-most non-zero entry of a vector the leading monomial, sorting the rows with respect to the position over term ordering brings M into row echelon form. Again the irreduciblity of the rows by each other implies that the pivots have the highest degree in their respective columns. Since the rows of M are a reduced Gröbner basis, the pivots are monic and thus M is in Popov normal form. □

The theorems which we have just proven allow us to use Gröbner basis theory to reason about the existence and uniqueness of the various normal forms.

Corollary 6.31. *For a given matrix $M \in {}^sR^t$ and every $\xi \in \mathbb{N}^t$, there exists unique matrices which are row-equivalent to M and which are in Popov normal form, ξ-Popov normal form and Hermite normal form, respecively.*

These normal forms all have the same number of rows which is equal to the rank of M in the sense of [BCL06, Definition 2.1] and not larger than s.

Proof. Since in the Theorems 6.28, 6.29 and 6.30 we have shown that all these forms are just reduced Gröbner bases with respect to the respective admissible orderings, existence and uniqueness follow from the existence and uniqueness of the reduced Gröbner basis in [BGTV03, Theorem 5.4.18].

Ore polynomial rings are (left and right) Euclidean and thus (left and right) Noetherian. Thus, by [Coh05, Theorem 4.6.7] they have invariant basis number. Since the different normal forms have all linearly independent rows by Lemma 6.6 and Remark 6.9, this implies that R^sM is (isomorphic to) a free module with the rows of the normal forms being bases. This implies that all normal forms must have the same number of rows. Since the Popov normal form is row-reduced, [BCL06, Theorem A.2] implies that the number of its rows equals the rank of M which cannot be larger than s. □

6.5 FGLM

This section does present a kind of an application for the interpretation of normal forms as Gröbner bases: Namely, we will rediscover [Vil96a, Algorithm 2]—that is used to convert column Popov normal forms of square matrices over commutative polynomials to column Hermite normal forms—as an instance of the famous *FGLM-algorithm*. Since we formulated the Gröbner basis theory in the previous sections for Ore polynomials, we can prove that the algorithm in [Vil96a] does work for this case as well. Moreover, we will introduce some additional modifications to that algorithm, though, to be able to deal with non-square matrices, too. Another difference is, that in our formulation the algorithm can be used to change between various normal forms while [Vil96a] considers only the case of conversion from Popov normal form to Hermite normal form. The latter case is arguably the most important one, though, as it is analogous to going from a degree ordering to an elimination ordering in the theory of Gröbner basis for commutative polynomial rings.

Note, that the proof here seems to be completely new, in [Vil96a] the algorithm is explained from a system-theoretical point of view.

Since computation of Gröbner bases does have exponential complexity—as was first reported in [MM82]—various strategies have been proposed to speed up this process. One method uses the fact that Gröbner bases for some admissible ordering usually compute faster than for other admissible orderings. The FGLM algorithm which is named after the initials of its inventors—Faugère, Gianni, Lazard and Mora—and which was presented in [FGLM93] allows to exploit this differences in the computation speed by giving an efficient method to compute a Gröbner basis of an ideal from another already known Gröbner basis. This means that if one seeks a basis for a slow admissible ordering, one may first compute a basis for a faster ordering and then use the FGLM-algorithm to change it to the desired ordering.

The original paper [FGLM93] addresses Gröbner bases for ideals of (multivariate) commutative polynomial rings. Although the computation itself does not in particular rely on the commutativity, there seem to be no generalisations of the FGLM-algorithm to non-commutative domains or to ideals yet. The only source known to the author is a short note in [Kou09].

The FGLM-algorithm achieves its efficiency by translating the problem of Gröbner basis conversion to a linear algebra problem. Instead of computing with polynomials, all computations are done

in the quotient of the ideal in question. Thus, a major restriction of the original FGLM-algorithm is that it can be applied only to zero-dimensional ideals, that is, ideals whose quotient is a finite dimensional vector space. There are also approaches for arbitrary ideals which exploit for instance the Hilbert polynomial. See [Tra97] for such an approach.

In this section we will translate the FGLM-algorithms to Gröbner bases in R^t where as before $R = K[\partial;\sigma,\vartheta]$ is the Ore polynomial ring over the skew field K with respect to the automorphism $\sigma\colon K \to K$ and the σ-derivative $\vartheta\colon K \to K$. This will allow us to convert Popov normal forms, ξ-Popov normal forms and Hermite normal forms of matrices—which we have shown to be Gröbner bases in the Theorems 6.28, 6.29 and 6.30—into each other. In our simple, univariate case we will be able to remove the restriction from [FGLM93] about the zero-dimensionality by taking advantage of the degree bounds in Remark 6.5 and Corollary 6.15.

We will start this section by first exploring the quotient modules of the free module R^t. Then, we will identify finite dimensional subspaces in which we can carry out our computations. The last point is translating the FGLM-algorithm to this situation.

Let the rows of $M \in {}^sR^t$ form a Gröbner bases for its row-space R^sM. Later, M will be in (ξ-) Popov normal form or Hermite normal form; but in the moment any Gröbner basis will be fine. The quotient module R^t/R^sM naturally is a left R-module and thus also a K-vector space. The multiplication with ∂ acts on R^t/R^sM as a *K-pseudo-linear transformation* in the sense of [Jac37] or [BP96]: There, for a K-space V an endomorphism φ of V is called K-pseudo-linear if for all vectors v and $w \in V$ and all scalars $a \in K$ the identities

$$\varphi(v+w) = \varphi(v) + \varphi(w) \qquad \text{and} \qquad \varphi(av) = \sigma(a)\varphi(v) + \vartheta(a)v$$

hold. This is easily seen to be the case for the left multiplication with ∂ in R^t/R^sM since for $\mathfrak{v} \in R^t$ and $a \in K$ denoting the residue class of $\mathfrak{v}$ in R^t/R^sM by $\overline{\mathfrak{v}}$ we have

$$\partial a\overline{\mathfrak{v}} = \overline{\partial a\mathfrak{v}} = \overline{\sigma(a)\partial\mathfrak{v} + \vartheta(a)\mathfrak{v}} = \sigma(a)\partial\overline{\mathfrak{v}} + \vartheta(a)\overline{\mathfrak{v}}$$

by the commutation rule (Equation (3.1)) and the R-linearity of the canonical projection from R^t to R^t/R^sM.

Assume for a moment that R^t/R^sM has a finite K-dimension. Fixing a basis $\mathfrak{B} = (e_1,\dots,e_d)$ we may express the action of ∂ in the following way: Define the matrix $A = (a_{ij}) \in {}^dK^d$ by taking the coefficients of the representation of the images of the basis vectors

$$\partial e_i = \sum_{i=1}^{d} a_{ij}e_j$$

for $1 \le i \le d$. Then for all $\mathfrak{v} \in R^t$ we have

$$(\partial\overline{\mathfrak{v}})_{\mathfrak{B}} = \sigma(\mathfrak{v}_{\mathfrak{B}})A + \vartheta(\mathfrak{v}_{\mathfrak{B}})$$

where $\mathfrak{v}_{\mathfrak{B}}$ denotes the coordinate vector of $\mathfrak{v}$ with respect to $\mathfrak{B}$ and where σ and ϑ are applied coordinate-wise. The matrix A is called a *defining $\mathfrak{B}$-matrix* or a *$\mathfrak{B}$-connection* in [CK02]. See also [Jac37, Section 2] or [BP96, Page 4]. If $\mathfrak{C}$ is another basis of R^t/R^sM, then the defining $\mathfrak{C}$-matrix B can be computed from A by a *gauge transformation* from the following identity

$$BP = \vartheta(P) + \sigma(P)A$$

where $P \in \mathrm{Gl}_d(K)$ is the change of basis matrix from $\mathfrak{C}$ to $\mathfrak{B}$. Also, one may prove that using the identity $(\partial\mathfrak{v})_{\mathfrak{B}} = \sigma(\mathfrak{v}_{\mathfrak{B}})C + \vartheta(\mathfrak{v}_{\mathfrak{B}})$ as a definition for the action of ∂ every matrix $C \in {}^dK^d$ defines an R-linear structure on K^d. For both points we refer the reader once more to [Jac37].

Let now M be arbitrary again, that is, we no longer assume that the quotient had finite dimension. We cite the following result on bases of the quotient R^t/R^sM.

Lemma 6.32. *Let the rows of $M \in {}^sR^t$ form a Gröbner basis with the leading term of the i^{th} row being at position j_i for $1 \le i \le s$. Then a basis of R^t/R^sM is given by all residue classes of all monomials which are irreducible with respect to the rows of M. More precisely, the irreducible monomials are all monomials $\partial^\alpha \mathfrak{e}_{j_i}$ for $\alpha < \deg M_{i,j_i}$ and $1 \le i \le s$ and all monomials $\partial^\beta \mathfrak{e}_k$ where $k \notin \{j_1,\dots,j_s\}$ and $\beta \ge 0$. If M is in Popov normal form or Hermite normal form, then the j_i are just the pivot indices.*

Moreover, assigning a vector its remainder by Gröbner basis division with the rows of M is a K-linear map.

Proof. This follows immediately from [BGTV03, Proposition 5.6.2 and Proposition 5.6.3] and the correspondence of the pivot indices and the leading monomials. □

We will call the basis from the previous lemma the *canonical basis* of R^t/R^sM and denote it by $\mathfrak{B}$. We emphasize that it depends on the admissible ordering with respect to which M is a Gröbner basis: For different orderings the same space will most likely have different canonical bases. Also, the canonical basis will in general be an infinite set of vectors. Thus, we cannot describe the multiplication by ∂ by a (finite) matrix here. Yet we can easily read off the result from the Gröbner basis M itself: Taking any element $\overline{\partial^\alpha \mathfrak{e}_k}$ of the canonical basis multiplication with ∂ will yield

- if M has a leading term in the k^{th} column in position (i,k) and $\alpha = \deg M_{i,k} - 1$—that is, if there is a row-index i such that $\mathrm{lm}(M_{i,*}) = \partial^{\alpha+1}\mathfrak{e}_k$—, then $\partial\overline{\partial^\alpha \mathfrak{e}_k} = \overline{\partial^{\alpha+1}\mathfrak{e}_k - M_{i,*}}$, and
- otherwise we simply have $\partial\overline{\partial^\alpha \mathfrak{e}_k} = \overline{\partial^{\alpha+1}\mathfrak{e}_k}$.

In the first case the representation of $\overline{\mathrm{lm}(M_{i,*}) - M_{i,*}}$ can be easily read off from M if its rows are a reduced Gröbner basis since the property that the rows are irreducible by each other means that no monomial in $\mathrm{lm}(M_{i,*}) - M_{i,*}$ can be reduced by the rows of M. Thus, the residue classes of these monomials will be canonical basis vectors and by linearity of the residue class mapping, the coefficients are just the coefficients of the monomials in $\mathrm{lm}(M_{i,*}) - M_{i,*}$.

For our version of the FGLM-algorithm, it will be sufficient to work in certain subspaces of R^t/R^sM. Given a degree bound $d \ge 0$, for any set $\mathfrak{S}$ of monomials, we define $\mathfrak{S}_{\le d} = \{\mathfrak{s} \in \mathfrak{S} \mid \deg \mathfrak{s} \le d\}$. Abusing this notation, if $\mathfrak{T}$ is the set of residue classes of the elements of $\mathfrak{S}$ then we denote by $\mathfrak{T}_{\le d}$ the residue classes of $\mathfrak{S}_{\le d}$. If all elements in $\mathfrak{S}$ are irreducible, then $\mathfrak{T}_{\le d}$ will be a subset of the canonical basis $\mathfrak{B}$ of R^t/R^sM.

Using this notation, for a degree bound $d \ge 0$ we define the *truncated (canonical) basis* $\mathfrak{B}_{\le d}$ with respect to d. Of course, it depends again on the admissible ordering that was chosen. The truncated canonical bases will span the subspaces of R^t/R^sM in which we will compute our FGLM-algorithm. We order the elements of $\mathfrak{B}_{\le d}$ ascendingly with respect to the position over term ordering. That means if for $1 \le k \le t$ we define

$$\tau_k = \begin{cases} \min\{\alpha - 1, d\}, & \text{if } \mathrm{lm}(M_{i,*}) = \partial^\alpha \mathfrak{e}_k \text{ for some row-index } i, \text{ and} \\ d, & \text{otherwise} \end{cases}$$

then the truncated basis $\mathfrak{B}_{\leq d}$ is just

$$\overline{\mathfrak{e}_t},\ldots,\overline{\partial^{\tau_t}\mathfrak{e}_t},\quad \overline{\mathfrak{e}_{t-1}},\ldots,\overline{\partial^{\tau_{t-1}}\mathfrak{e}_{t-1}},\quad \ldots,\quad \overline{\mathfrak{e}_1},\ldots,\overline{\partial^{\tau_1}\mathfrak{e}_1}.$$

For a given d we restrict the multiplication of ∂ to the truncated canonical basis by projecting on the K-span $\langle\mathfrak{B}_{\leq d}\rangle$ of $\mathfrak{B}_{\leq d}$. This is again a pseudo-linear map since for every $v \in \langle\mathfrak{B}_{\leq d}\rangle$ and every $a \in K$ we have

$$\pi\big(\partial a v\big) = \pi\big(\sigma(a)\partial\pi(v) + \vartheta(a)\pi(v)\big) = \sigma(a)\pi(\partial v) + \vartheta(a)\pi(v) = \sigma(a)\pi(\partial v) + \vartheta(a)v$$

using $v = \pi(v)$ which follows from $v \in \langle\mathfrak{B}_{\leq d}\rangle$. The defining $\mathfrak{B}_{\leq d}$-matrix T of this map can be computed completely analogously to the $\mathfrak{B}$-case. We would like to give more details in here, though, since the finite dimensional case is important for the following tasks. For this, we remark that for an element $\partial\overline{\partial^\alpha\mathfrak{e}_k}$ of $\partial\mathfrak{B}_{\leq d}$ Gröbner basis division to find its coordinate vector is not necessary if there is either no leading term in the k^{th} column or if $M_{i,*}$ has a leading term at postion k but $\alpha+1 < \deg M_{i,k}$. This will be the case if $\alpha \leq \tau_k$. Then the coordinate vector is just the next basis vector or 0 if $\alpha = d$. Otherwise, we need to do reduction which—as explained above—does not need actual computation in the case of a reduced Gröbner basis.

We can distinguish these cases using the indices of the basis vectors and $\tau_1,\ldots,\tau_t$. The (representatives of the) basis vectors $\mathfrak{b}_1,\ldots,\mathfrak{b}_{\tau_t+1}$ have their non-zero entry in the t^{th} position, $\mathfrak{b}_{\tau_t+2},\ldots,\mathfrak{b}_{\tau_t+\tau_{t-1}+2}$ have it in position $t-1$, and so on. Thus, $\mathfrak{b}_i$ is of the form $\overline{\partial^\alpha\mathfrak{e}_k}$ if

$$\tau_{k+1}+\ldots+\tau_t+(t-k) < i \leq \tau_k+\ldots+\tau_t+(1+t-k)$$

where we will then have just $\alpha = i-\tau_{k+1}-\ldots-\tau_t-(t-k)-1$. We summarize this in the following remark.

Remark 6.33. Let $d \geq 0$ be a degree bound. Taking the i^{th} basis vector $\mathfrak{b}_i$ of the truncated basis $\mathfrak{B}_{\leq d}$, the j^{th} coordinate of $\partial\mathfrak{b}_i$ will be either

1. 0, if $0 < i-\tau_t-\ldots-\tau_{k+1}-(t-k) < \tau_k+1$ for some k and $k \neq i+1$, or
2. 1, if $0 < i-\tau_t-\ldots-\tau_{k+1}-(t-k) < \tau_k+1$ for some k and $k = i+1$, or
3. $-\operatorname{coeff}(\mu-1, M_{k,z})$, if $i = \tau_t+\ldots+\tau_k+(1+t-k)$ for some k and where $\mu = j-\tau_t-\ldots-\tau_{z+1}-(t-z)$ for some z such that $0 < \mu \leq \tau_z+1$.

We will refer to the defining $\mathfrak{B}_{\leq d}$-matrix T as the *truncated multiplication matrix*. We emphasize that by the remark T can be computed from M using just "copy& paste".

We can find (the transpose of) this matrix also at the beginning of [Vil96a, Section 4] as matrix A, where the basis elements are ordered in a probably different way than in our presentation. The definition of the matrix is motivated differently from our case by being part of a *minimal realisation*—see [Vil96a, Definition 1]—of the Hermite normal form which we seek to compute.

Example 6.34. We consider $R = \mathbb{Q}(X)[\partial;\mathrm{id}, d/dX]$. Let

$$M = \begin{pmatrix} \partial^2+X & X-1 & \partial-X \\ X+1 & \partial+1 & \partial-X \end{pmatrix} \in {}^2R^3.$$

Since $\operatorname{lm}_{\leq_{\text{TOP}}}(M_{1,*}) = \partial^2\mathfrak{e}_1$ and $\operatorname{lm}_{\leq_{\text{TOP}}}(M_{2,*}) = \partial\mathfrak{e}_2$ we see—using Theorem 6.26—that M is a Gröbner basis with respect to the term over position ordering. Since M is reduced, it is thus—by Theorem 6.28—in Popov normal form. The irreducible monomials with respect to M and $\leq_{\text{TOP}}$ are

$$\mathfrak{e}_1, \partial\mathfrak{e}_1, \mathfrak{e}_2, \mathfrak{e}_3, \partial\mathfrak{e}_3, \partial^2\mathfrak{e}_3, \partial^3\mathfrak{e}_3, \partial^4\mathfrak{e}_3\ldots$$

and the canonical basis of R^3/R^2M consists of their residue classes.

Set now $d=4$. Then the truncated basis $\mathfrak{B}_{\le d}$ is

$$\overline{\mathfrak{e}_3}, \overline{\partial\mathfrak{e}_3}, \overline{\partial^2\mathfrak{e}_3}, \overline{\partial^3\mathfrak{e}_3}, \overline{\partial^4\mathfrak{e}_3}, \overline{\mathfrak{e}_2}, \overline{\mathfrak{e}_1}, \overline{\partial\mathfrak{e}_1}$$

sorting it in the way we agreed upon. This yields the truncated matrix T which is just

$$\begin{array}{c} \\ \overline{\mathfrak{e}_3} \\ \overline{\partial\mathfrak{e}_3} \\ \overline{\partial^2\mathfrak{e}_3} \\ \overline{\partial^3\mathfrak{e}_3} \\ \partial^3\mathfrak{e}_3 \\ \overline{\mathfrak{e}_2} \\ \overline{\mathfrak{e}_1} \\ \overline{\partial\mathfrak{e}_1} \end{array} \begin{array}{c} \begin{array}{cccccccc} \overline{\mathfrak{e}_3} & \overline{\partial\mathfrak{e}_3} & \overline{\partial^2\mathfrak{e}_3} & \overline{\partial^3\mathfrak{e}_3} & \overline{\partial^4\mathfrak{e}_3} & \overline{\mathfrak{e}_2} & \overline{\mathfrak{e}_1} & \overline{\partial\mathfrak{e}_1} \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ X & -1 & 0 & 0 & 0 & -1 & -X-1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ X & -1 & 0 & 0 & 0 & 1-X & -X & 0 \end{pmatrix} \end{array} \in {}^8\mathbb{Q}(X)^8$$

using Remark 6.33 where $\tau_1=2$, $\tau_2=1$ and $\tau_3=4$. We can check that indeed, for example,

$$(\partial\overline{\mathfrak{e}_2})_{\mathfrak{B}_{\le d}} = \overline{\mathfrak{e}_2}\mathfrak{B}_{\le d}T = \left(X\overline{\mathfrak{e}_3} - \overline{\partial\mathfrak{e}_3} - \overline{\mathfrak{e}_2} - (X+1)\overline{\mathfrak{e}_1}\right)_{\mathfrak{B}_{\le d}}.$$

Remark 6.35. We will also need to represent the residue classes of the canonical basis vectors $\mathfrak{e}_1,\ldots,\mathfrak{e}_t$ of R^t. Their representation can be computed from $\tau_1,\ldots,\tau_t$ as well: If $\tau_i \ge 0$ for some $1 \le i \le t$, then $\mathfrak{e}_i$ is irreducible by M and its residue class is just $\mathfrak{b}_\mu$ where $\mu = \tau_t + \ldots + \tau_{i+1} + (1+t-i)$. Otherwise, $\mathfrak{e}_i$ is reducible by M and as above the j^{th} coordinate will be $-\operatorname{coeff}(\partial^{\mu-1}, M_{k,z})$, where $i = \tau_t + \ldots + \tau_k + (1+t-k)$ for some k and where $\mu = j - \tau_t - \ldots - \tau_{z+1} - (t-z)$ for some z such that $0 < \mu \le \tau_z + 1$.

Also the coordinate vectors of the residue classes of the basis vectors can be found in [Vil96a, Section 4] as columns of the matrix B. Again, they are sorted in a way different from our conventions here.

Finally, we need to reason about how big the truncated spaces in which we will work need to be.

Remark 6.36. Let the rows of $M \in {}^sR^t$ be a reduced Gröbner basis. Let $d \ge 0$. The residue classes of the monomials of degree not larger than d span a subspace in R^t/R^sM of dimension at most td. Therefore, this subspace is included in $\langle \mathfrak{B}_{\le td} \rangle$.

Example 6.41 shows that this bound is sharp.

Again, we can relate this to [Vil96a, Section 4]: Since M in that paper is square, there is a pivot, that is, a leading monomial in every column of M. This is obvious if M is in Hermite normal form or in Popov normal form, but does also hold for every other reduced Gröbner basis since otherwise the rows were reducible by each other. Thus, the number of truncated basis elements that need to be considered does never exceed $s(\deg M)$. In [Vil96a, Equation (13)], the coordinates with respect to the canoncial basis are calculated in the columns of the *block Krylov matrix* $M(A,B,\nu)$—since there the multiplication matrix is defined as the transpose of ours, the action of the indeterminate x is expressed by left multiplication of A and not right multiplication as in our approach. Also, since $\sigma = \mathrm{id}$ in [Vil96a], it suffices to multiply by A.

We will now assume that the rows of $M \in {}^sR^t$ are a reduced Gröbner basis with respect to an admissible ordering $<_1$ and that we know a bound $d \geq 0$ on the degrees of a reduced Gröbner basis of R^sM with respect to an ordering $<_2$. This is for example the case if M is in Popov normal form—that is, if we have $<_1 = <_{\text{TOP}}$—and we are considering $<_2 = <_{\text{POT}}$—see the degree bound in Corollary 6.15.

We will state the algorithm first and proof its correctness later in Theorem 6.38. In the algorithm all computations can be done using linear algebra. This is detailed in Remark 6.40.

Algorithm 6.37 (FGLM for normal form conversion)**.**

Input Two admissible orderings $<_1$ and $<_2$, a matrix $M \in {}^sR^t$ such that the rows form a reduced Gröbner basis with respect to $<_1$ and a degree bound d for the reduced Gröbner basis of R^sM with respect to $<_2$.

Output A matrix $N \in {}^sR^t$ such that the rows are a reduced Gröbner basis of R^sM with respect to the ordering $<_2$.

Procedure

1. Compute the set of monomials $\mathfrak{B}_1$ such that the truncated basis of R^t/R^sM with respect to $<_1$ and td is $\overline{\mathfrak{B}_1} = \{\overline{\mathfrak{b}} \mid \mathfrak{b} \in \mathfrak{B}_1\}$ as well as the correspondending multiplication matrix T. See Remark 6.33 for how to do this.

   Compute also the coordinates of the canonical basis vectors $\mathfrak{e}_1, \ldots, \mathfrak{e}_t$ of R^t with respect to to $\overline{\mathfrak{B}_1}$. See Remark 6.35.

2. Initialise $C \leftarrow \emptyset$, $\mathfrak{B}_2 \leftarrow \emptyset$ and $G_2 \leftarrow \emptyset$.

   Below elements will be added to $\mathfrak{B}_2$ and C only simultaneously, therefore we consider the elements of $\mathfrak{B}_2$ to be indexed with respect to to the elements of C.

   When the algorithm terminates, G_2 will contain a Gröbner basis for R^sM, $\mathfrak{B}_2$ will contain representatives for the truncated basis of R^t/R^sM with respect to d and $<_2$ and C_i will be the coordinate vector of $\overline{(\mathfrak{B}_2)_i}$ with respect to $\overline{\mathfrak{B}_1}$.

3. If there are monomials of degree less than $d+1$ that are not divisible by G_2, then:

   (a) Choose the smallest such monomial $\mathfrak{m}$ with respect to $<_2$ and compute its coordinate vector w with respect to $\overline{\mathfrak{B}_1}$.

   If, for example, $<_1 = <_{\text{POT}}$ and $<_2 = <_{\text{TOP}}$, this can be done efficiently using the multiplication matrix T. See Remark 6.39.

   (b) If $\{w\} \cup C$ is linearly independent, then set $C \leftarrow \{w\} \cup C$ and $\mathfrak{B}_2 \leftarrow \{\mathfrak{m}\} \cup \mathfrak{B}_2$.

   (c) Else, there are $a_c \in K$ for all $c \in C$ such that $w = \sum_{c \in C} a_c c$. Set

   $$G_2 \leftarrow G_2 \cup \{\mathfrak{m} - \sum_{c \in C} a_c (\mathfrak{B}_2)_c\}.$$

   (d) Goto step 3.

4. Else, stop and return the matrix N containing the elements of G_2 as rows.

In [Vil96a, Algorithm 2] a slightly different approach is chosen: As explained above, the coordinates of all elements in the truncated basis are computed first and stored into the Krylov matrix $M(A,B,v)$. From this matrix then the first linearly independent columns are selected where the sorting is done with respect to lexicographic ordering. In Algorithm 6.37 above these steps are intermingled following the classical formulation of the FGLM algorithm.

Theorem 6.38. *Algorithm 6.37 is correct and terminates.*

Proof. Termination is obvious since in the loop in step 3 only a finite number of monomials are considered at all.

It remains to prove the correctness. For this we first note the invariant, that the elements of C are always K-linearly independent. This is clear since only those vectors are added to C in step 3 (b) that do not destroy this property. Consequently, also the residue classes of the elements of $\mathfrak{B}_2$ are K-linearly independent since the coordinate vectors of their projections are linearly independent and the coordinate map and the projection are linear maps.

Let in step 3 (c) $\mathfrak{g} = \mathfrak{m} - \sum_{c \in C} a_c (\mathfrak{B}_2)_c$. Since the monomials are considered in ascending order with respect to $<_2$, we must have $\operatorname{lm}_{<_2}(\mathfrak{g}) = \mathfrak{m}$ because the monomials in $\mathfrak{B}_2$ have been added before and are thus smaller. This also shows that the leading monomials of the elements of G_2 are not in $\mathfrak{B}_2$. Also multiples of the leading monomials of the elements in G_2 cannot be in $\mathfrak{B}_2$ since they are larger than the leading monomials by the second property of admissible orderings in Definition 6.16 and can thus not have been considered before the leading monomial. Since upon termination of the algorithm every monomial of degree lower than d has been considered and identified either as element in $\mathfrak{B}_2$ or as leading monomial in G_2 or a multiple thereof, we obtain

$$\operatorname{LM}(G_2)_{\leq d} \dot\cup \mathfrak{B}_2 = \mathfrak{T}_{\leq d}$$

where $\mathfrak{T}$ denotes the set of all monomials and where $\operatorname{LM}(G_2) = \{\partial^\alpha \operatorname{lm}(\mathfrak{g}) \mid \mathfrak{g} \in G_2 \text{ and } \alpha \geq 0\}$.

Consider again an element $\mathfrak{g} = \mathfrak{m} - \sum_{c \in C} a_c (\mathfrak{B}_2)_c \in G_2$. We need to prove that $\mathfrak{g} \in R^t M$. Let $\mathfrak{r} = \mathfrak{g} - \mathfrak{u}M$ be the remainder of $\mathfrak{g}$ by division with M according to Theorem 6.22. Then $\overline{\mathfrak{r}} = \overline{\mathfrak{g} - \mathfrak{u}M} = \overline{\mathfrak{g}}$ and the basis representation yields $(\overline{\mathfrak{g}})_{\mathfrak{B}_1} = w - \sum_{c \in C} a_c (\mathfrak{B}_2)_c = 0$. Since $\mathfrak{r}$ is irreducible this implies $\mathfrak{r} = 0$ and thus $\mathfrak{g} \in R^s M$.

Let now $\tilde{G}$ be a Gröbner basis of $R^s M$ with respect to $<_2$ and let $\tilde{\mathfrak{B}}$ denote the corresponding truncated basis with respect to d. Then since $G_2 \subseteq R^s M$, we must have $\tilde{\mathfrak{B}} \subseteq \mathfrak{B}_2$. We want to prove now that $\operatorname{lm}(\mathfrak{g}) \in \operatorname{LM}(G_2)$ for any $\mathfrak{g} \in \tilde{G}$. We know that $\deg \mathfrak{g} \leq d$. Thus, we have $\operatorname{lm}(\mathfrak{g}) \in \operatorname{LM}(G_2)$ or $\operatorname{lm}(\mathfrak{g}) \in \mathfrak{B}_2$. Assume that $\operatorname{lm}(\mathfrak{g})$ was in $\mathfrak{B}_2$. Then an element of $\mathfrak{B}_2$ was reducible by $\tilde{G}$ to a linear combination of elements in $\tilde{\mathfrak{B}} \subseteq \mathfrak{B}_2$ which is a contradiction to linearly independence of $\mathfrak{B}_2$. This implies that $\operatorname{lm}(\mathfrak{g}) \in \operatorname{LM}(G_2)$. Thus is every vector which is reducible by $\tilde{G}$ also is reducible by G_2 meaning that by Definition 6.23 G_2 is a Gröbner basis.

Since for every element $\mathfrak{g} \in G_2$ the leading monomial is not divisible by leading monomials of the other elements of G_2— it can not be divisible by an element added to G_2 earlier because of the condition in step 3, but also not by those chosen later since by the second property of Definition 6.16 monomials can only be divided by smaller ones—and since $\mathfrak{g} - \operatorname{lm}(\mathfrak{g})$ is a linear combination of monomials irreducible by G_2, we see that $\mathfrak{g}$ is irreducible by $G_2 \setminus \{\mathfrak{g}\}$. Also, the elements of G_2 are monic.

Thus, G_2 must be even a reduced Gröbner basis according to Definition 6.25. □

We remark that the computation of the smallest monomials can be speeded up using the truncated multiplication matrices discussed earlier. We concentrate here on the conversion of a matrix to Hermite normal form.

Remark 6.39. If $<_2 = <_{\text{POT}}$, that is, if we want to compute a Hermite normal form, then we first have to consider all monomials of the form $\partial^\alpha \mathfrak{e}_t$ for $0 \leq \alpha \leq d$, then those of the form $\partial^\alpha \mathfrak{e}_{t-1}$ and so on. We can realise this using the truncated multiplication matrix as follows: In step 3 of Algorithm 6.37 introduce and initialise the new variables $k \leftarrow t$ and $\alpha \leftarrow 0$. Also set $\mathfrak{m} \leftarrow \partial^\alpha \mathfrak{e}_k$ and $w \leftarrow \mathfrak{m}_{\mathfrak{B}_1}$—the

latter being not a real computation by Remark 6.35. Execute steps 3(b) and 3(c). In step 3(d), if $\alpha = d$ or if $\{w\} \cup C$ is linearly dependent, set $k \leftarrow k-1$, $\alpha \leftarrow 0$ and $\mathfrak{m} \leftarrow \partial^\alpha \mathfrak{e}_k$ and $w \leftarrow \mathfrak{m}_{\mathfrak{B}_1}$. Otherwise set $\alpha \leftarrow \alpha + 1$, and $\mathfrak{v} \leftarrow \partial\mathfrak{v}$ and $w = wT$. Iterate until $k = 0$.

Next, we reason about the complexity of the Algorithm 6.37. Again, we will consider only the conversion from Popov normal form to Hermite normal form. Let $M \in {}^sR^t$ be in Popov normal form. In the first two steps 1 and 2 there is not much to do, since the computation of T and the representations of the basis vectors do only involve copying coefficients from M as shown in the Remarks 6.33 and 6.35.

Step 3 is the only step where a real computation takes place. We use the simplifications outlined in Remark 6.39. Let $d = \deg M$. By Corollary 6.15 the degree bound in this case is md. The number of monomials that need to be considered is thus at most mdt and the size of $\mathfrak{B}_1$ is mdt^2 since we have t columns. To generate a monomial we either look it up from a list containing the unit vectors and their coordinates using Remark 6.35 or compute it as a product with T and the previous monomial. In the latter case to compute the coordinates we need $\mathcal{O}(mdt^2)$ applications of σ and ϑ and $\mathcal{O}(m^2d^2t^4)$ multiplications and additions in K for the multiplication by T. The most expensive step is to solve the $\mathcal{O}(mdt^2)$ variables system in step 3(b) which needs $\mathcal{O}(m^3d^3t^6)$ operations in K by [KS89, Bemerkung 2.19(2)]. The computation of $\mathfrak{m} - \sum_{c\in C} a_c(\mathfrak{B}_2)_c$ is again just copying coefficients since $\mathfrak{B}_2$ contains only (different) monomials and $\mathfrak{m} \notin \mathfrak{B}_2$.

The estimate becomes much lower if M happens to be a square matrix. Then, the degree bound is never needed because there will be a pivot in every row of M implying that R^t/R^sM is finite. This corresponds to the case of zero-dimensional ideals in the theory of commutative polynomials. We need to consider at most $\mathcal{O}(td)$ monomials. This bound can even be tightened more using the index of M which is $\operatorname{ind} M = \sum_{i=1}^s \deg M_{i,*}$ as introduced in [For75] if M is in Popov normal form. This yields a total complexity of $\mathcal{O}\big((\operatorname{ind} M)^4\big)$—almost the same complexity as in [Vil96a, Proposition 3].

Remark 6.40. Computation of a Popov normal form of $M \in {}^sR^t$ where the rows of M are a reduced Gröbner basis and $\deg M = d$ needs at most $\mathcal{O}(m^3d^3t^6)$ operations in K. If $s = t$ and M is in Popov normal form, then $\dim R^s/R^sM \le s(\deg M)$ and this bound can be lowered to $\mathcal{O}\big((\operatorname{ind} M)^4\big)$.

Example 6.41. We consider

$$M = \begin{pmatrix} 1 & X^2 \end{pmatrix} \in \mathbb{Q}[X]^2.$$

This matrix is in Hermite normal form with leading monomial being $\mathfrak{e}_1$. We want to compute a Gröbner basis for a position over term ordering $<_2$ with $\mathfrak{e}_1 <_2 \mathfrak{e}_2$. (This is not the ordering from Definition 6.18, but a mirrored version). Of course, this Gröbner basis must be M itself since it consists only of a single row. The degree bound for the Gröbner basis is thus $d = 2$.

The monomials of degree less than d are $\mathfrak{e}_1 <_2 \partial\mathfrak{e}_1 <_2 \partial^2\mathfrak{e}_1 <_2 \mathfrak{e}_2 < \partial\mathfrak{e}_1 <_2 \partial^2\mathfrak{e}_2$. The representations in the canonical basis of R^2/R^1M are

$$\overline{\mathfrak{e}_1} = \overline{-x^2\mathfrak{e}_2},\ \overline{x\mathfrak{e}_1} = \overline{-x^3\mathfrak{e}_2},\ \overline{x^2\mathfrak{e}_1} = \overline{-x^4\mathfrak{e}_2},\ \overline{\mathfrak{e}_2} = \overline{\mathfrak{e}_2},\ \overline{x\mathfrak{e}_2} = \overline{x\mathfrak{e}_2},\ \text{and } \overline{x^2\mathfrak{e}_2} = \overline{x^2\mathfrak{e}_2}.$$

Iterating, we find thus that the first five monomials are linearly independent modulo M. Only for $X^2\mathfrak{e}_2$ do we find the relation $\overline{\mathfrak{e}_1 + X^2\mathfrak{e}_2} = 0$ which yields the desired Gröbner basis.

This shows that the truncated basis with respect to d would have been too small for this computation since there already the second vector would have reduced to zero.

Example 6.42. Let $R = \mathbb{Q}[X]$. We consider

$$M = \begin{pmatrix} 1 & X & 1 \\ 1 & 0 & X \end{pmatrix} \in {}^2R^3.$$

The leading monomials with respect to term over position ordering are $(0,X,0)$ and $(0,0,X)$ making M a Gröbner basis by Theorem 6.26. The degree bound for the Hermite form in $2\deg M = 2$ by Corollary 6.15. The truncated canonical basis needs thus to be computed with a bound of $3\cdot 2 = 6$. It is

$$\mathfrak{B} = \overline{\mathfrak{e}_1}, X\overline{\mathfrak{e}_1}, X^2\overline{\mathfrak{e}_1}, X^3\overline{\mathfrak{e}_1}, X^4\overline{\mathfrak{e}_1}, X^5\overline{\mathfrak{e}_1}, X^6\overline{\mathfrak{e}_1}, \overline{\mathfrak{e}_2}, \overline{\mathfrak{e}_3}$$

and the multiplication matrix is

$$T = \begin{array}{c} \\ \overline{\mathfrak{e}_1} \\ X\overline{\mathfrak{e}_1} \\ X^2\overline{\mathfrak{e}_1} \\ X^3\overline{\mathfrak{e}_1} \\ X^4\overline{\mathfrak{e}_1} \\ X^5\overline{\mathfrak{e}_1} \\ X^6\overline{\mathfrak{e}_1} \\ \overline{\mathfrak{e}_2} \\ \overline{\mathfrak{e}_3} \end{array} \begin{array}{c} \begin{array}{ccccccccc} \overline{\mathfrak{e}_1} & X\overline{\mathfrak{e}_1} & X^2\overline{\mathfrak{e}_1} & X^3\overline{\mathfrak{e}_1} & X^4\overline{\mathfrak{e}_1} & X^5\overline{\mathfrak{e}_1} & X^6\overline{\mathfrak{e}_1} & \overline{\mathfrak{e}_2} & \overline{\mathfrak{e}_3} \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

since $X\mathfrak{e}_2 \equiv -\mathfrak{e}_1 - \mathfrak{e}_2 \pmod{R^2M}$ and $X\mathfrak{e}_3 \equiv -\mathfrak{e}_1 \pmod{R^2M}$.

The first monomial with respect to position over term ordering is $\mathfrak{e}_3$ having the coordinates $(0,0,0,0,1)$. This is unequal to zero. The next monomials are $X\mathfrak{e}_3$ and $X^2\mathfrak{e}_3$ with coordinates

$$(0,0,0,0,0,0,0,0,1)T = (-1,0,0,0,0,0,0,0,0)$$

and

$$(-1,0,0,0,0,0,0,0,0)T = (0,-1,0,0,0,0,0,0,0).$$

All three coordinate vectors are linearly independent. This obviously doesn't change if we add the coordinate vectors of $X^3\mathfrak{e}_3$, $X^4\mathfrak{e}_3$, $X^5\mathfrak{e}_3$ and $X^6\mathfrak{e}_3$. Since we have reached the degree bound, the next monomial to consider is $\mathfrak{e}_2$ with coordinates $(0,0,0,0,0,0,1,0)$. The coordinate vectors are still linearly independent. But for $X\mathfrak{e}_2$ with coordinates

$$(0,0,0,0,0,0,0,1,0)T = (-1,0,0,0,0,0,0,0,-1)$$

we obtain

$$(-1,0,0,0,0,0,0,0,-1) = (-1,1,0,0,0,0,0,0,0)\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and hence the last row of the Hermite form must be

$$X\mathfrak{e}_2 + \mathfrak{e}_3 + X\mathfrak{e}_3 = (0, X, X+1).$$

The next monomial we must consider is $\mathfrak{e}_1$ with coordinates $(1,0,0,0,0,0,0,0,0)$. Again we have a linear dependency

$$(1,0,0,0,0,0,0,0,0) = (0,-1,0,0,0,0,0,0,0)\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

and hence the next row of the Hermite form is

$$\mathfrak{e}_1 + X\mathfrak{e}_3 = (1,0,X).$$

Since there are no more monomials to be considered, we have the Hermite form

$$H = \begin{pmatrix} 1 & 0 & X \\ 0 & X & 1-X \end{pmatrix}$$

which is confirmed by MAPLE's built-in procedure.

7

Jacobson normal form

7.1 Definition

In this chapter, we consider a ring $R = K[\partial; \mathrm{id}, \vartheta]$ of differential operators over a (commutative) differential field (K, ϑ). We will be using the same notations for matrices as introduced in Section 5.1. In this chapter we will treat a two-sided normal form by which we mean a normal form with respect to simultanuous row- and column-operations. Expressed differently, we are looking for canonical representatives with respect to to *equivalence* where two matrices M and $N \in {}^sR^t$ are called *equivalent* if there are unimodular matrices $S \in \mathrm{Gl}_s(R)$ and $T \in \mathrm{Gl}_t(R)$ such that $SMT = N$.

We will be looking for normal forms which are diagonal matrices. The existence of strong diagonal forms (which will later be called Jacobson normal form) for matrices over rings goes back to Henry John Steven Smith who studied this concept for the integers. Therefore, over the integers the Jacobson normal form usually bears his name, the *Smith form*. Later on, generalisations to other kinds of rings were explored by Nathan Jacobson and Oswald Teichmüller. A statement about the uniqueness (up to similarity) was given by Tadashi Nakayama. For further historical remarks we refer the reader to [Coh85, Notes and comments for chapter 8].

The normal form we will be looking for is the following.

Definition 7.1. A matrix $M \in {}^mR^n$ is said to be in *Jacobson normal form* if $M = \mathrm{diag}(1, \ldots, 1, f, 0, \ldots, 0)$ where $f \in R$.

This is actually a simplified definition of the Jacobson form. The general definition which may, for example, be found (though not bearing a name) in [Coh85, Theorem 8.1.1] is the following: A matrix $M = (m_{ij}) \in {}^mD^n$, where D is any principal ideal domain, is in this general Jacobson normal form if and only if $m_{ij} = 0$ for $i \neq j$ and $Dm_{i+1,i+1}D \subseteq Dm_{i,i} \cap m_{i,i}D$ for all $i = 1, \ldots, \max\{m, n\} - 1$.

Since $D1 \cap 1D = D$ and $D0D = 0$, our definition of Jacobson form emerges as a special case of the general definition. In fact, one can show that the general definition always reduces to our definition if the ring D is simple–confer [Coh85, Cor. 8.1.2]. Simplicity is given for all fields of characteristic zero as we shall see below. Note, however, that we do not restrict ourselves to this case here. Instead we will give sufficient conditions—depending on the degree and size of the matrix—when a Jacobson

normal form as in Definition 7.1 can be computed even in positive characteristic. See Corollary 7.11 for the details.

The entry f in Definition 7.1 is not completely unique: It can be shown—confer, for example, [Coh85, Theorem 8.2.4]—that two matrices $\operatorname{diag}(1,\ldots,1,f,0,\ldots,0)$ and $\operatorname{diag}(1,\ldots,1,g,0,\ldots,0)$ in Jacobson normal form with f and $g \in R$ are equivalent if and only the number of non-zero diagonal entries is equal for both and we have

$$\frac{R}{Rf} \cong \frac{R}{Rg}.$$

Two elements f and $g \in R$ which fulfil the latter relation are said to be *similar*.

Thus, the Jacobson normal form is not a real normal form. Nevertheless, it is usually treated like that in the literature—and we follow this custom by keeping the "normal" in its name.

The algorithm which we present below seems to be the first Jacobson normal form algorithm for differential operators that is proven to compute in polynomial time. Up to now, this was only known for commutative polynomials—see [Vil96b, Corollary 6.1]—but for differential operators no such analysis has been done.

7.2 Naïve method

A proof that every matrix may be brought into (the general) Jacobson normal form may be found in [Coh85, Chapter 8]. There, elementary row and column operations akin to the Euclidean algorithm are used to reduce a given matrix $M \in {}^{s}R^{t}$ first to a matrix of the form $\operatorname{diag}(a_1,\tilde{M})$ where $a_1 \in R$ and $\tilde{M} \in {}^{s-1}R^{t-1}$. Then induction is used to get a (weak) diagonal form $\operatorname{diag}(a_1,\ldots,a_{\min\{s,t\}})$ with $a_1,\ldots,a_{\min\{s,t\}} \in R$. This is completely constructive and has been implemented, for example, in [CQ05]—although the complexity appears to be high in the worst case with respect to operations in the ground field K, since the reduction of one position may blow up the degrees of the entries in the yet untreated sub-matrices. There seems, however, to be no rigid complexity analysis of this approach in the literature.

Another way of obtaining a weak diagonal form is to use alternating row and column Hermite normal form computations. See [Sch10, Algorithm 2] where the Hermite normal form is replaced by more general Gröbner basis computations.

When the matrix is in (weak) diagonal form, one has to apply further computations on each consecutive pair of diagonal entries to get the desired Jacobson normal form. Assume thus, without loss of generality, $M = \operatorname{diag}(a_1,a_2)$ where $a_1,a_2 \in R \setminus \{0\}$. Cohn's approach (as given in the proof of [Coh85, Theorem 8.1.1]) for further reduction is to transform M by

$$\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} = \begin{pmatrix} a_1 & da_2 \\ 0 & a_2 \end{pmatrix}$$

where $d \in R$ is chosen in a way that a_1 is not a left factor of da_2. Then, we can again reduce the result to a (weak) diagonal form where the degree of a_1 strictly decreases. If no such d may be found, then one can argue—at least in the case where R is simple—, that a_1 is already a unit.

A problem remains to find such a d or to prove the non-existence. The latter is easy since—in the simple case—this happens precisely when a_1 is a unit. The first problem is harder, but for ground fields of characteristic zero, one may use a result by Kossivi Adjamagbo in order to determine a suitable d.

Lemma 7.2 ([Adj88, Lemme 6]). *Let $f, g \in R \setminus K$ and let $c \in K$ such that $pc - cp \neq 0$ for all $p \in R \setminus K$. Then there exists $0 \leq k \leq \max\{\deg g - \deg f + 1, 0\}$ such that f is not a right divisor of $c^{-k} g c^k$. An analogous statement holds for left division.*

If $\operatorname{char} K = 0$, then any c with $\vartheta(c) \neq 0$ will fulfil the condition $pc - cp \neq 0$ for all $p \in R \setminus K$.

Proof. We give a detailed proof as the source does not provide one, and as we need it for establishing the bound. We prove only the case of right division. It is an immediate consequence of the commutation rule that $\deg(gc - cg) \leq \deg g - 1$. We use this fact to do an induction over the difference of the degrees of f and g. If $\deg f > \deg g$ then the statement holds for $k = 0$. Let $\deg g - \deg f = n \geq 0$ and suppose the claim holds for $gc - cg \neq 0$, that is, suppose for $0 \leq k \leq \deg(gc - cg) - \deg f + 1$ or for $k = 0$ that f is not a right divisor of $c^{-k}(gc - cg)c^k$. Now, if we had $c^{-k} g c^k = af$ and $c^{-k-1} g c^{k+1} = bf$ for $a, b \in R$ then

$$c^{1-k} g c^k = caf \qquad \text{and} \qquad c^{-k} g c^{k+1} = cbf$$

which implies

$$c^{-k}(gc - cg)c^k = c^{-k} g c^{k+1} - c^{1-k} g c^k = c(b - a)f$$

contradicting our assumption. Hence f does not divide $c^{-k} g c^k$ or $c^{-k-1} g c^{k+1}$. Since $\deg(gc - cg) < \deg g$ we also have $k, k+1 \leq \deg g - \deg f + 1$.

If $\operatorname{char} K = 0$ and $\vartheta(c) \neq 0$, we may consider the K-linear map $\alpha = h \mapsto c^{-1} h c$. We have for all $k \geq 0$

$$\alpha(\partial^k) = c^{-1} \partial^k c = \partial^k + k c^{-1} \vartheta(c) \partial^{k-1} + \text{lower degree terms.}$$

Hence, if we restrict α to $R_{\leq n} = \{h \in R \mid \deg h \leq n\}$ where $n \geq \deg g$, letting $y = c^{-1}\vartheta(c) \neq 0$, the matrix for $\alpha | R_{\leq n}$ with respect to the K-basis $\partial^n, \ldots, \partial, 1$ is

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ ny & 1 & \ddots & \vdots \\ * & (n-1)y & \ddots & 0 \\ \vdots & \ddots & \ddots & 1 \\ * & \cdots & * & y \end{pmatrix}$$

which has only 1 as eigenvalue and $K \cdot 1$ as only eigenspace, since $k c^{-1} \vartheta(c) \neq 0$ for all $k \geq 1$. Hence for $p \in R \setminus K$ we will always have $pc - cp \neq 0$. □

The bound on k in the lemma is not found in Adjamagbo's original paper. But it is important here in order to make the computation finite: In the above problem of treating the matrix $\operatorname{diag}(a_1, a_2)$, we just need to test divide the elements $a_2, c^{-1} a_2 c^1, \ldots c^{-\ell} a_2 c^\ell$ for $\ell = \deg a_2 - \deg a_1 + 1$ by a_1; and by the lemma must find a non divisible element in that way.

We end this section with the remark, that this lemma does not hold for arbitrary characteristic. Consider for example the differential field $(\mathbb{F}_2(x, y), d/dx)$ where d/dx is the usual derivative with respect to x. Let $f = g = \partial^2 \in R = \mathbb{F}_2(x, y)[\partial; \mathrm{id}, d/dx]$. We have $(d/dx)x = 1 \neq 0$, but

$$gx = \partial^2 \cdot x = x\partial^2 + 2\partial \equiv x\partial^2 = xg \pmod 2.$$

Thus, obviously, f is a right divisor of $x^{-k}gx^k = g$ for every $k \geq 0$. In fact, for all $p \in \mathbb{F}_2(x)$ we have always $gp = p\partial^2 + 2(d/dx[p])\partial + (d^2p/dx^2) \equiv pg \pmod 2$.[1] This additionally proves that $\mathbb{F}_2(x,y)[\partial;\mathrm{id},d/dx]$ is not simple, since g commutes with ∂ and y, too.

Remark 7.3. On the other hand, the additional statement of Lemma 7.2—that for $\mathrm{char}\, K = 0$ every $c \notin \mathrm{Const}(K)$ will satisfy $pc - cp \neq 0$ and $\deg(pc - cp) < \deg p$ for all $p \in R \setminus K$—can be used to prove that for $\mathrm{char}\, K = 0$ and $\vartheta \neq 0$ the ring R must be simple: Assume we are given a two-sided ideal $I \trianglelefteq R$ which is neither $\{0\}$ nor R. Then I is generated by a non-zero element $p \in I$ of minimal degree. Using the lemma we can construct an element $pc - cp \in I \setminus \{0\}$ of strictly lower degree—a contradiction. Whence, non-trivial two-sided ideals cannot exist.

7.3 Preparing the matrix

We start this section with a simple yet very useful lemma which follows immediately from the homomorphism theorem. We will use it in the proof of Theorem 7.10 below. It yields also the motivation for the whole method.

Lemma 7.4. *Let $A \in {}^sR^t$, and let $P \in \mathrm{Gl}_s(R)$ and $Q \in \mathrm{Gl}_t(R)$ be unimodular. Then*

$$\frac{R^t}{R^s A} \to \frac{R^t}{R^s(PAQ)}, \quad \overline{\mathfrak{v}} \mapsto \overline{\mathfrak{v}Q}$$

is an isomorphism of left R-modules.

Proof. We consider the epimorphism $\varphi\colon R^s \to R^t/R^s PAQ$ which is defined as $\mathfrak{v} \to \overline{\mathfrak{v}Q}$. We have

$$\ker\varphi = \{\mathfrak{v} \in R^s \mid \mathfrak{v}Q \in R^s PAQ\} = R^s PA = R^s A,$$

and thus $R^t/R^s A \cong R^t/R^s(PAQ)$ by the first isomorphism theorem—see, for example, [Coh00, Theorem 1.17]. □

The lemma allows to transform quotient spaces of row spaces of matrices into nicer forms using elementary transformations on the matrix. Below, we will see that column- and row-reduction—see Section 5.2— can be used to obtain a particularly easy shape.

Lemma 7.5. *Let $A \in {}^sR^t$ be such that the submatrix of the non-zero columns is column-reduced, and assume that for $P \in \mathrm{Gl}_s(R)$ the non-zero rows of PA form a row-reduced submatrix. Then $PA = \mathrm{diag}(M, {}_{s-k}\mathbf{0}_{t-k})$ where $k \leq \min\{s,t\}$ and $M \in {}^kR^k$ is square and row-reduced.*

Proof. By [BCL06, Theorem A.2] the number of non-zero rows of PA equals the (left) row-rank of A which is defined as the maximal number of (left) R-linearly independent rows in R^sA in [BCL06, Definition 2.1] and similarly in [Coh85, Section 5.4]. Analogously, the (right) column-rank of A being the maximal number of (right) R-linearly independent columns equals the number of non-zero columns of A. Since the multiplication by P from the left is an isomorphism of right R-modules due to the unimodularity of P, the number of non-zero columns and the column-rank of A and PA must coincide. Since by [Coh85, Proposition 5.4.2] column- and row-rank of PA have the same value, we obtain that the number of non-zero rows and that of non-zero columns of PA must be equal. Thus, $PA = \mathrm{diag}(M, {}_{s-k}\mathbf{0}_{t-k})$ for some square matrix $M \in {}^kR^k$ where $k \leq \min\{s,t\}$. Furthermore, the sumbatrix M must be row-reduced since it consists of rows of the row-reduced matrix PA. □

[1] If we differentiate a polynomial $p \in \mathbb{F}_2[x]$ once then all even powers of x vanish and all odd powers become even. So d^2p/dx^2 becomes 0. Using the quotient rule this expands to $\mathbb{F}_2(x)$ as well.

We remark that row-reduction applied to a column-reduced matrix may yield a matrix which is not column-reduced any longer. For example has the matrix

$$A = \begin{pmatrix} \partial^2 & \partial & 1 \\ \partial & 1 & 0 \\ \partial^2 & \partial^2 & 0 \end{pmatrix} \in {}^3R^3$$

the leading row coefficient matrix and leading column coefficient matrix

$$\mathrm{LC}_{\mathrm{row}}(A) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \mathrm{LC}_{\mathrm{col}}(A) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

and is thus column-reduced but not row-reduced. On the other hand, row-reduction leads to

$$B = \begin{pmatrix} 1 & -\partial & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A = \begin{pmatrix} 0 & 0 & 1 \\ \partial & 1 & 0 \\ \partial^2 & \partial^2 & 0 \end{pmatrix}$$

with leading row coefficient matrix and leading column coefficient matrix

$$\mathrm{LC}_{\mathrm{row}}(B) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \mathrm{LC}_{\mathrm{col}}(B) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$$

which is row-reduced but not column-reduced. Note, however, that the number of non-zero columns remains the same as predicted in the lemma.

The lemma may be interpreted in terms of quotient spaces as the following decomposition.

Corollary 7.6. *Let $A \in {}^sR^t$. Then there is a square matrix $M \in {}^kR^k$ with $k \leq \min\{s,t\}$ such that*

$$\frac{R^t}{R^s A} \cong \frac{R^k}{R^k M} \oplus R^{t-k}$$

and such that $R^k/R^k M$ has finite K-dimension.

Proof. By the previous lemma, applying row- and column-reduction to A yields a decomposition $PAQ = \mathrm{diag}(M, {}_{s-k}\mathbf{0}_{t-k})$ where $P \in \mathrm{Gl}_s(R)$ and $Q \in \mathrm{Gl}_t(R)$. We may assume that M is in Popov normal form. Then, since M is a Gröbner basis by Theorem 6.28, Lemma 6.32 imples that the residue classes of the irreducible monomials form a K-basis of $R^k/R^k M$. Since M is square and must therefor have a pivot, that is, a leading term in every column, there can be only finitely many irreducible monomials. Thus, we obtain $\dim_K R^k/R^k M < \infty$. □

7.4 Cyclic vectors

As already mentioned in the overview, our Jacobson normal form algorithm is based on so-called cyclic vectors. In this whole section let K be a commutative field with (id-) derivation $\vartheta\colon K \to K$ such that $\vartheta \neq 0$, and that we have set $R = K[\partial; \mathrm{id}, \vartheta]$. Let $A \in {}^sR^t$. As we have seen above in Corollary 7.6,

we may assume that A is decomposed into $A = \operatorname{diag}(M, {}_{s-k}\mathbf{0}_{t-k})$ where $M \in {}^{k}R^{k}$ is square and which leads to a decomposition of the factor module into a torsion and a free part.

We will concern ourself only with the torsion part. That means, in this whole section we will consider only the finite K-dimensional space $R^k/R^k M$. This space retains a R-module structure. In particular, an action of ∂ on its elements is defined which yields a so-called *pseudo-linear transformation* as studied, for example, in [Jac37] or [BP96]—see also Section 6.5. Under mild assumptions which are explained below $R^k/R^k M$ is a *cyclic module*, that is, a module that is generated by a single vector.

The motivation for this section comes from Lemma 7.4: The finite dimension of $R^k/R^k M$ implies already that a Jacobson normal form of M must have full rank since otherwise a contradiction to Lemma 7.4 would arise. Suppose for the moment, that R is a simple ring. That means, any Jacobson normal form of M must be of the form $\operatorname{diag}(1,\dots,1,f)$ for some $f \in R \setminus \{0\}$. Assume that S and $T \in \mathrm{Gl}_k(R)$ are such that $SMT = \operatorname{diag}(1,\dots,1,f)$. Then Lemma 7.4 yields

$$\frac{R^k}{R^k M} \cong \frac{R^k}{R^k (SMT)} \cong \frac{R^k}{R^k \operatorname{diag}(1,\dots,1,f)} \cong \frac{R}{R1} \oplus \dots \oplus \frac{R}{R1} \oplus \frac{R}{Rf} \cong \frac{R}{Rf}.$$

More precisely, if $\mathfrak{g} \in {}^{k}R$ denotes the last column $T_{*,k}$ of T, then the isomorphism above may by the lemma be represented as

$$\varphi \colon \frac{R^k}{R^k M} \to \frac{R^1}{R^1 f}, \quad \overline{\mathfrak{v}} \mapsto \overline{\mathfrak{v}\mathfrak{g}}$$

since the first $k-1$ entries of $\mathfrak{v}T$ can be ignored. This isomorphism actually shows two points: First, for simple rings R the module $R^k/R^k M$ must always be cyclic, and, second, the last column of transformation matrix T is—in sense which we be made more precise below—the most important part of S and T.

Below we will change our point of view. We will assume that any isomorphism φ from $R^k/R^k M$ to a cyclic module is given, and will then try to obtain corresponding transformation matrices. This question is treated in Section 7.5—while in the remainder of this section we will concentrate on the question when $R^k/R^k M$ is isomorphic to a cyclic module even if R is not simple. We will present a result from [CK02] answering the question, and modify it a little bit in order to fit with our main result, Corollary 7.11, below.

The first definition that we need in this section is that of a cyclic vector. Although it is usually stated in a more general way—see, for example, [CK02, Introduction]—, we will be content with a simplified version that is exactly tailored towards our needs.

Definition 7.7 (Cyclic vector)**.** Let $M \in {}^{k}R^{k}$ such that $\dim_K R^k/R^k M < \infty$. A vector $v \in R^k/R^k M$ is called a *cyclic vector* if $Rv = R^k/R^k M$.

A more general definition can be found in [CK02]. The source also contains a broad historic overview about the computation of cyclic vectors. The algorithm that is proposed in [CK02] itself is based on the following theorem which we cite in full but already adapted to our notation.

Theorem 7.8 ([CK02, Proposition 3.8])**.** *Let (K,ϑ) be a (commutative) differential field, let $R = K[\partial;\mathrm{id},\vartheta]$, and let $M \in {}^{k}R^{k}$ be such that $\mathfrak{M} = R^k/R^k M$ has the finite dimension d over K. Assume there exist $S_0 \subseteq \mathrm{Const}(K) \setminus \{0\}$ and $S \subseteq K$ such that $|S_0| = d = |S|$ and such that the elements of S are linearly independent over* $\mathrm{Const}(K)$.

Let $v \in \mathfrak{M}$. If there exists $u \in \mathfrak{M} \setminus Rv$ then there are $\lambda_0 \in S_0$ and $\lambda \in S$ such that

$$\dim_K R(v + \lambda\lambda_0 u) > \dim_K Rv.$$

The theorem immediately suggests an iterative way of computing a cyclic vector: Simply start with a random vector, and if it is not alreay cyclic then there is a finite set of canditates for a vector spanning a strictly larger space. Since the dimension of $R^k/R^k M$ is finite, this must yield a cyclic vector after a finite number of steps. This method is described in more depth in [CK02, Algorithm 4.1], while the appendix of [CK02] contains a MAPLE implementation.

For our Jacobson normal form algorithm below we will need a more special kind of cyclic vector than that which is computed by the general algorithm. More precisely, we will need to compute a cyclic vector v that has a representative $\mathfrak{v} \in K^k$ of degree 0. It turns out that only a minimal modification to the algorithm proposed by [CK02] is needed for that which concerns the choice of the vector u from Theorem 7.8. This modification is explained in the following corollary to Theorem 7.8.

Corollary 7.9. *Let $M \in R^k/R^k R$ be in Popov normal form, and let $d = \deg M$. If $kd \le [K : \mathrm{Const}(K)]$, then we may compute a vector $\mathfrak{v} \in K^k$ such that $R\overline{\mathfrak{v}} = R^k/R^k M$ using at most $\mathcal{O}(d^5k^5)$ operations in K.*

If the characteristic of K is zero, then the only condition for the existence of a cyclic vector is $\vartheta \neq 0$.

Proof. In the algorithm of [CK02] which is based on Theorem 7.8 the choices of v and u are arbitrary. So we may start with $v = \overline{\mathfrak{v}}$ where $\mathfrak{v} \in K^k$. Assume the classes of all unit vectors $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ of R^k are already in Rv, say $\overline{\mathfrak{e}_j} = h_j v$ where $h_j \in R$, then for an arbitrary $\mathfrak{u} = (u_1, \ldots, u_n) \in R^k$ we have

$$\overline{\mathfrak{u}} = \sum_{k=1}^{n} u_k \overline{\mathfrak{e}_k} = \Big(\sum_{k=1}^{n} u_k h_k\Big) v$$

and hence $\overline{\mathfrak{u}} \in Rv$, that is, v is cyclic.

By contraposition, if v is not cyclic, then we can find a unit vector $\mathfrak{e}_j$ such that $\overline{\mathfrak{e}_j} \notin Rv$. Since in the algorithm λ_0 and λ are chosen from K, we see that $v + \lambda_0\lambda\overline{\mathfrak{e}_j} = \overline{\mathfrak{v} + \lambda_0\lambda\,\mathfrak{e}_j}$ has a representative in K^k. So in each iteration of the algorithm the candidate for a cyclic vector is in $\overline{K^k}$.

The complexity analysis can be found in [CK02, Section 4] where we have to remember that by Lemma 6.32 we have $\dim_K R^k/R^k M \le kd$. Finally, the hypothesis $kd \le [K : \mathrm{Const}(K)]$—or $\vartheta \neq 0$ in the characteristic zero case—ensures the existence of the sets S and S_0 from Theorem 7.8 as explained in [CK02, Section 3] and [CK02, Section 5]. □

Assume that we have a cyclic vector $\overline{\mathfrak{v}}$ for $R^k/R^k M$. Since $\dim_K R^k/R^k M = d$ is finite, the products $\overline{\mathfrak{v}}, \partial\overline{\mathfrak{v}}, \ldots, \partial^d\mathfrak{v}$ must be linearly independent while by the cyclicity of $\overline{\mathfrak{v}}$ there can be no non-trivial relations between $\overline{\mathfrak{v}}, \partial\overline{\mathfrak{v}}, \ldots, \partial^{d-1}\mathfrak{v}$. That means the *annihilator* of $\overline{\mathfrak{v}}$—being a left ideal of R—is generated by an Ore polynomial of degree $d+1$. We denote the annihilator of $\overline{\mathfrak{v}}$ in R by $\mathrm{Ann}_R\,\overline{\mathfrak{v}}$ where we will sometimes ommit the subscript if no confusion may arise.

As above in Section 6.5, we may use defining matrices to do the computations in $R^k/R^k M$. Computing the coordinates of the scalar multiples of $\overline{\mathfrak{v}}$ in such a way needs at most $\mathcal{O}(d^2)$ derivations and $\mathcal{O}(d^3)$ additions and multiplications in K. Solving the resulting linear system needs another $\mathcal{O}(d^3)$ operations. This means that we may compute a generator of $\mathrm{Ann}_R\,\overline{\mathfrak{v}}$ using $\mathcal{O}(d^3)$ operations in K.

7.5 Computing Jacobson normal forms

Let as before $R = K[\partial; \mathrm{id}, \vartheta]$ for a commutative differential field (K, ϑ). Again, we assume that we are given $M \in {}^kR^k$ such that R^k/R^kM has finite dimension over K.

Let now a vector $\mathfrak{v} \in K^k$—that is, a vector with $\deg \mathfrak{v} = 0$—be given such that $\overline{\mathfrak{v}}$ is cyclic. Let $f \in R$ be such that $\mathrm{Ann}_R\, \mathfrak{v} = Rf$. The result that we want to prove in this section is that M is similar to a matrix $\mathrm{diag}(1, \ldots, 1, f)$ in Jacobson normal form where we can compute the transformation matrices from f in polynomial time.

The idea for the algorithm comes from the motivation in the previous section: The cyclic vector $\overline{\mathfrak{v}}$ yields an isomorphism

$$\varphi\colon \frac{R^k}{R^kM} \to \frac{R^1}{R^1f}$$

that is defined by $\overline{\mathfrak{v}} \mapsto \overline{1}$. We have already explained that this isomorphism is connected to the last column $\mathfrak{g} = T_{*,k}$ of the transformation matrix $T \in \mathrm{Gl}_k(R)$—provided that such a T exists.

Assume now that this T exists. Then $\varphi(\overline{\mathfrak{w}}) = \overline{\mathfrak{w}\mathfrak{g}}$ for all $\mathfrak{w} \in R^k$ by Lemma 7.4. In particular, substituting the unit vectors $\mathfrak{e}_1, \ldots, \mathfrak{e}_k$ of R^k for $\mathfrak{w}$ yields

$$\overline{\mathfrak{g}}_j = \varphi(\overline{\mathfrak{e}_j})$$

for all $1 \le j \le k$. In the proof of the theorem below, we will use that relation as definition of $\mathfrak{g}$. The question remains whether this is reasonable, that is, whether such a $\mathfrak{g}$ is indeed the last column of a unimodular matrix T and whether—in the affirmative case—for each such column transformation matrix T there exists a unimodular matrix $S \in \mathrm{Gl}_k(R)$ that brings the product MT into Jacobson normal form.

Theorem 7.10. *Let (K, ϑ) be a commutative differential field, and let $R = K[\partial; \mathrm{id}, \vartheta]$. Assume that we are given $M \in {}^kR^k$ in Popov normal form and $\mathfrak{v} \in R^k$ such that $\deg \mathfrak{v} = 0$ and $R\mathfrak{v} = R^k/R^kM$.*

Then we can compute S and $T \in \mathrm{Gl}_k(R)$ such that $SMT = \mathrm{diag}(1, \ldots, 1, f)$ where $f \in R$ using at most $\mathcal{O}\big(k^8(\deg M)^3\big)$ operations in K.

Proof. By Remark 6.40, we know already that $d = \dim_K R^k/R^kM \le k(\deg M)$ is finite, and that we can compute the canonical basis $\mathfrak{E} = (e_1, \ldots, e_d)$ of R^k/R^kM as well as the defining $\mathfrak{E}$-matrix from M by copy&paste—see the Remarks 6.33 and 6.35. We may assume here, that $d > 0$ since otherwise M is unimodular and the theorem can trivially be fulfilled using the inverse of M as transformation. The matrix of change of basis from $\mathfrak{E}$ to the cyclic basis $\mathfrak{F} = (\overline{\mathfrak{v}}, \partial\overline{\mathfrak{v}}, \ldots, \partial^{d-1}\overline{\mathfrak{v}})$ is just

$$P = \begin{pmatrix} (\overline{\mathfrak{v}})_{\mathfrak{E}} \\ (\partial\overline{\mathfrak{v}})_{\mathfrak{E}} \\ \vdots \\ (\partial^{d-1}\overline{\mathfrak{v}})_{\mathfrak{E}} \end{pmatrix} \in \mathrm{Gl}_d(K)$$

where—as before—the subscript denotes the coordinate vector with respect to the given basis. Using the defining $\mathfrak{E}$-matrix, P can be computed from the coordinates of $\overline{\mathfrak{v}}$ using no more than $\mathcal{O}(d^2)$ derivations and $\mathcal{O}(d^3)$ multiplications in K. Using P^{-1} to represent $\partial^d\overline{\mathfrak{v}}$ in the cyclic basis $\mathfrak{F}$, we obtain $f \in R$ with $\deg f = d$ and $\mathrm{Ann}_R\, \overline{\mathfrak{v}} = Rf$ as explained already in the end of the last section.

As already announced in the motivation, we now define $\mathfrak{g} \in {}^kR$ such that $\overline{\mathfrak{g}_j} = \varphi(\overline{\mathfrak{e}_j})$. The R-isomorphism $\varphi\colon R^k/R^kM \to R^1/R^1f$ that sends $\overline{\mathfrak{v}}$ to $\overline{1}$ can be computed using again the matrix P: Namely, if $\mathfrak{w} \in R^k$ then

$$\varphi(\overline{\mathfrak{w}}) = \overline{\mathfrak{w}}_{\mathfrak{E}} P \begin{pmatrix} \overline{1} \\ \overline{\partial} \\ \vdots \\ \overline{\partial^{d-1}} \end{pmatrix}$$

since the last matrix maps $\mathfrak{F}$ to the cyclic basis $\overline{1}, \overline{\partial}, \ldots, \overline{\partial^{d-1}}$ of R^1/R^1f. That is, we can set $\mathfrak{g}_j$ to be the row of $P\left(\partial^i\overline{\mathfrak{v}}\right)_{i=0}^{d-1}$ that corresponds to $\overline{\mathfrak{e}}_j$ if $\overline{\mathfrak{e}}_j$ is part of $\mathfrak{E}$; and we set $\mathfrak{g}_j$ to 0 otherwise.[2] Note, that this definition implies $\deg\mathfrak{g} < \deg f$. We may use $\mathfrak{g}$ to compute the image under φ for any $\mathfrak{u} = (u_1, \ldots, u_k) \in R^k$ as

$$\varphi(\overline{\mathfrak{u}}) = \sum_{j=1}^{k} u_k \varphi(\overline{\mathfrak{e}_j}) = \overline{\mathfrak{u}\mathfrak{g}}.$$

Since $\varphi(\overline{\mathfrak{v}}) = \overline{1}$ we must obtain $1 - \mathfrak{v}\mathfrak{g} \in Rf$, that is,

$$1 = \sum_{j=1}^{k} \mathfrak{v}_j \mathfrak{g}_j$$

since by $\deg\mathfrak{v} = 0$ and $\deg\mathfrak{g} < \deg f$ the summands on the right hand side have a degree strictly smaller than that of f. This yields $\gcrd(\mathfrak{g}_1, \ldots, \mathfrak{g}_k) = 1$.

Using Lemma 5.16, we may compute a matrix $T \in \mathrm{Gl}_k(R)$ such that $T^{-1}\mathfrak{g} = {}^t\mathfrak{e}_k$ where $\mathfrak{e}_k$ is the k^{th} unit vector of R^k using at most $\mathcal{O}(kd\max\{k^2, d^2\})$ operations in K with $\deg T$ and $\deg T^{-1} \le (k+1)d$. Multiplication by T yields $\mathfrak{g} = T\,{}^t\mathfrak{e}_k$, that is, $\mathfrak{g}$ is the last column $T_{*,k}$ of T. We will prove in the following that this T is already the sought transformation matrix.

For this, first we show that the last column of MT is a (right) multiple of f. Indeed, since the rows of M vanish in R^k/R^kM we obtain for every $1 \le j \le k$

$$\overline{0} = \varphi(\overline{M_{j,*}}) = \overline{M_{j,*}\mathfrak{g}}$$

and thus $M_{j,*}\mathfrak{g} \in Rf$. That means, using the Euclidean algorithm (or Lemma 5.16), we can compute $Q \in \mathrm{Gl}_k(R)$ such that

$$QMT = \begin{pmatrix} \tilde{M} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \\ * \cdots * & \lambda f \end{pmatrix}$$

where $\lambda \in R$, $\tilde{M} \in {}^{k-1}R^{k-1}$ and the $*$'s denote arbitrary elements from R.

We are next going to prove that λ is a unit. Let $h \in R$ be such that $h\overline{\mathfrak{e}_k} = 0$ in $R^k/R^k(QMT)$. That means that there exists $\mathfrak{w} \in R^k$ such that $h\mathfrak{e}_k = \mathfrak{w}QMT$, and comparing the k^{th} entry shows that h must be a left multiple of λf. This implies that $\mathrm{Ann}_R\,\overline{\mathfrak{e}_k} \subseteq R\lambda f$. Applying the homomorphism theorem for modules—see, for example, [Coh00, Corollary 1.16]—to this inclusion we obtain now using Lemma 7.4

$$\frac{R^1}{R^1f} \cong \frac{R^k}{R^kM} \cong \frac{R^k}{R^k(QMT)} \supseteq R\overline{\mathfrak{e}_k} \cong \frac{R}{\mathrm{Ann}_R\,\overline{\mathfrak{e}_k}} \twoheadrightarrow \frac{R^1}{R^1\lambda f}$$

[2] The equation $\mathfrak{g}_j = 0$ means that the pivot in the j^{th} row of M has degree 0. Thus $\overline{\mathfrak{e}}_j$ vanishes in R^k/R^kM.

where "$\twoheadrightarrow$" denotes a surjection. Comparing the K-dimensions, these homomorphisms lead to

$$\deg f = \dim \frac{R^1}{R^1 f} \geq \dim R\overline{\mathfrak{e}_k} \geq \dim \frac{R^1}{R^1 \lambda f}.$$

This inequality implies that $\lambda \neq 0$ since otherwise $R^1/R^1\lambda f$ would have infinite dimension. Furthermore, from this we obtain $\deg f \geq \dim R^1/R^1\lambda f = \deg\lambda + \deg f$ and thus $\deg\lambda = 0$. Thus, λ is a unit in R and we may without loss of generality assume that Q was chosen in such a way, that $\lambda = 1$.

Finally, the dimensions computed above yield $\deg f \geq \dim R\overline{\mathfrak{e}_k} \geq \deg f$. This implies that $\overline{\mathfrak{e}_k}$ must be a cyclic vector for $R^k/R^k(QMT)$. In particular exist $h_j \in R$ with $\deg h_j < \deg f$ for $1 \leq j \leq k-1$ such that $\overline{\mathfrak{e}_j} = h_j\overline{\mathfrak{e}_k}$ in $R^k/R^k(QMT)$, that is, such that $\mathfrak{e}_j - h_j\mathfrak{e}_k = \mathfrak{w}QMT$ for some $\mathfrak{w} \in R^k$. Comparing again the k^{th} entries on both sides we see that $h_j \in Rf$ and thus $h_j = 0$ because of the degree. This means that also $\mathfrak{w}_k$ must be zero, that is, that the last row of QMT is not used. Hence, $\mathfrak{e}_j$ is for all $1 \leq j \leq k-1$ already in the row space of $(\tilde{M}, {}_k\mathbf{0}_1)$ meaning that $\tilde{M}$ is invertible. This allows us to tranform QMT to $N = \operatorname{diag}(1,\ldots,1,f)$ using elementary row operations $Z \in \mathrm{Gl}_k(R)$.

Since the last column of MT is in ${}^kRf$, we can write MT as XN for some $X \in {}^kR^k$. We obtain $N = ZQXN$ which implies $(ZQ)X = \mathbf{1}_k$ since N—that only multiplies the last column of a matrix by $f \neq 0$—cannot be a zero divisor. Consequently, X is unimodular, and we can compute the transformation matrix $S = ZQ \in \mathrm{Gl}_k(R)$ that fulfills $SMT = N$ by inverting X. We know that the degree of MT is at most $(k+1)d + \deg M \leq (k+1)k(\deg M) + \deg M$, that is, the degree is in $\mathcal{O}(k^2 \deg M)$. Hence, by Lemma 5.15 we need at most $\mathcal{O}\big(k^2 \cdot k^2(\deg M)\max\{k^2, (k^2\deg M)^2\}\big) = \mathcal{O}\big(k^8 \cdot (\deg M)^3\big)$ operations in K in order to compute S. This is the most expensive step in the algorithm. □

Below, in Algorithm 7.12, we give an overview over the method that was presented in the proof of Theorem 7.10. Combining the theorem with the results from Section 7.3, we obtain the following corollary.

Corollary 7.11 (Main result)**.** *Let (K,ϑ) be a (commutative) differential field, let $R = K[\partial;\mathrm{id},\vartheta]$ and let $A \in {}^sR^t$. Let $k = \min\{s,t\}$ and $d = \deg A$. If*

$$kd \leq [K : \mathrm{Const}(K)]$$

or if the characteristic of K is zero and $\vartheta \neq 0$, then we can compute $f \in R$ and unimodular matrices $S \in \mathrm{Gl}_s(R)$ and $T \in \mathrm{Gl}_t(R)$ such that

$$SAT = \operatorname{diag}(1,\ldots,1,f,0,\ldots,0)$$

is in Jacobson normal form.

Computation of a Jacobson normal form needs at most $\mathcal{O}\big(std\max\{s^2,d^2\} + k^5d^5\big)$ operations in K, while the transformation matrices may be computed needing no more than $\mathcal{O}\big(k^8d^3\big)$ operations.

Proof. By Lemma 7.5, there are matrices $P \in \mathrm{Gl}_s(R)$ and $Q \in \mathrm{Gl}_t(R)$ such that $PAQ = \operatorname{diag}(M, {}_{s-\ell}\mathbf{0}_{t-\ell})$ where $M \in {}^\ell R^\ell$ with $\ell \leq k$ and M is row-reduced. Computing P and Q is done by applying first colmmn- and then row-reduction which each needs at most $\mathcal{O}\big(std\max\{s^2,d^2\}\big)$ operations in K by Lemma 5.14. Furthermore, the lemma also states that $\deg M \leq d$. Converting M to Popov normal form using the naïve methods needs $\mathcal{O}\big(std\max\{s^2t, td^2\}\big)$ operations according to Lemma 5.14 and the considerations before Remark 6.5.

We have $\dim R^k/R^k M \leq \ell\deg M$ and $\ell\deg M \leq kd \leq [K : \mathrm{Const}(K)]$ or $\mathrm{char}K = 0$ and $\vartheta \neq 0$ by assumption, and can thus compute a cyclic vector using Corollary 7.9 using at most $\mathcal{O}(k^5d^5)$ operations

in K. As mentioned in the end of Section 7.4, computing the annihilator Rf of this vector needs only $\mathcal{O}(k^3d^3)$ operations.

By Theorem 7.10, we may now compute S and $T \in \mathrm{Gl}_k(R)$ such that $SMT = \mathrm{diag}(1,\dots,1,f)$. This implies that

$$\mathrm{diag}(S,\mathbf{1}_{s-k})P \cdot M \cdot Q\,\mathrm{diag}(T,\mathbf{1}_{t-k}) = \mathrm{diag}(1,\dots,1,f,0,\dots,0)$$

is in Jacobson normal form. Computation of T needs computation of the greatest common right divisor of k elements of degree being less than kd, which can be done by Lemma 5.16 using at most $\mathcal{O}\big(k^2d\min\{k^2,k^2d^2\}\big) = \mathcal{O}\big(k^4d^3\big)$ operations in K with the result having $\deg T \le (k+1)kd \in \mathcal{O}(k^2d)$. The S is computed by inverting the product MT with f divided out of the last column. The degree of MT is at most $\mathcal{O}(k^2d+d) = \mathcal{O}(k^2d)$. Thus, using Lemma 5.15, S can be computed using at most $\mathcal{O}\big(k^4d\min\{k^2,k^4d^2\}\big) = \mathcal{O}\big(k^8d^3\big)$ operations in K. □

Algorithm 7.12 (Jacobson normal form)**.**

Input A matrix $A \in {}^sR^t$ of Ore polynomials $R = K[\partial;\mathrm{id},\vartheta]$ over a commutative differential field (K,ϑ) with $\vartheta \neq 0$ where $\mathrm{char}\,K = 0$ or $k \deg A \le [K\colon \mathrm{Const}(K)]$ for $k = \min\{s,t\}$.

Output A triple (f,S,T) of a polynomial $f \in R$ and unimodular matrices $S \in \mathrm{Gl}_s(R)$ and $T \in \mathrm{Gl}_t(R)$ such that

$$SAT = \mathrm{diag}(1,\dots,1,f,0,\dots,0).$$

Procedure

1. Apply column-reduction (analogously to Algorithm 5.13) to A obtaining $Q \in \mathrm{Gl}_t(R)$ such that the non-zero columns of AQ form a column-reduced submatrix.
2. Compute the Popov normal form of AQ obtaining $P \in \mathrm{Gl}_s(R)$ such that

$$PAQ = \begin{pmatrix} M & {}_k\mathbf{0}_{t-k} \\ {}_{s-k}\mathbf{0}_k & {}_{s-k}\mathbf{0}_{t-k} \end{pmatrix}$$

   with $k \le \min\{s,t\}$ and $M \in {}^kR^k$ in Popov normal form.
3. Let $d = \dim_K R^k/R^kM$. Compute the canonical basis $\mathfrak{E}$ and the defining $\mathfrak{E}$-matrix using Remarks 6.33 and 6.35.
4. Compute a vector $\mathfrak{v} \in K^k$ such that $\overline{\mathfrak{v}}$ is cyclic for R^k/R^kM as explained in Corollary 7.9.
5. Compute the matrix of change from $\mathfrak{E}$ to the cyclic basis as

$$P = \begin{pmatrix} (\overline{\mathfrak{v}})_{\mathfrak{E}} \\ (\partial\overline{\mathfrak{v}})_{\mathfrak{E}} \\ \vdots \\ (\partial^{d-1}\overline{\mathfrak{v}})_{\mathfrak{E}} \end{pmatrix} \in {}^dK^d.$$

   Here, the defining $\mathfrak{E}$-matrix can be used to compute the rows of P.
6. Set

$$(c_0,\dots,c_{d-1}) = (\partial^d\overline{\mathfrak{v}})_{\mathfrak{E}}P^{-1}$$

   and set $f = \partial^d - c_{d-1}\partial^{d-1} - \dots - \mathfrak{c}_1\partial - \mathfrak{c}_0 \in R$.

7. Compute
$$\mathfrak{g} = \begin{pmatrix} (\overline{\mathfrak{e}_1})_{\mathfrak{E}} \\ \vdots \\ (\overline{\mathfrak{e}_k})_{\mathfrak{E}} \end{pmatrix} P^{-1} \begin{pmatrix} 1 \\ \partial \\ \vdots \\ \partial^{d-1} \end{pmatrix} \in {}^{k}R.$$
(The first matrix only selects rows from $P^{-1}(\partial^j)_{j=0}^{d-1}$.)
8. Use Lemma 5.16 (or the Euclidean algorithm) to compute $T \in \mathrm{Gl}_k(R)$ such that $T^{-1}\mathfrak{g} = {}^{t}\mathfrak{e}_1$.
9. Compute MT and divide the last column by f from the right obtaining $X \in {}^{k}R^{k}$.
10. Compute $S = X^{-1}$ using Lemma 5.15.
11. Return
$$\Big(f,\ \mathrm{diag}(S, \mathbf{1}_{s-k})P,\ Q\,\mathrm{diag}(T, \mathbf{1}_{t-k})\Big).$$

An actual implementation of the algorithm could further decrease the running time of the computation. For example, if M has pivots of degree zero, then these could be brought to the top-left of M using row- and column-permutations. By Definition 6.1, the other entries below or above these entries must vanish and hence, we have a decomposition of M as
$$M = \begin{pmatrix} \mathbf{1}_q & B \\ \mathbf{0}_q & \tilde{M} \end{pmatrix}_{k-q}$$
where $B \in {}^{q}R^{k-q}$ denotes a matrix of arbitrary elements. (The identity matrix appears since pivot elements are monic.) Elementary column-operations can now be used to eliminate B. The modular computation must then only consider $\tilde{M}$ meaning that we have to consider a space of smaller dimension. This additional reduction might even make finding a cyclic vector possible at all, in case that the bound on the dimension derived from the degree and number of rows of M has been to pessimistic.

Part IV

Application in control theory

8

Flat outputs of control systems

8.1 Control theory

In this chapter we are going to present an example for the application of normal form computations in the field of linear control theory which is joint work with Dr. Felix Antritter over the course of the last year. We presented preliminary results in [AM10].

Linear control theory is concerned with the study of linear systems of equations involving various kinds of operators—most prominently derivations—which arise from models of real world problems from engineering, physics or biology. The connecting idea is that the equations are usually not solved directly but analysed for their properties.

In this first section we will strive to give a short and concise introduction to this vast field. Naturally, we cannot explain everything in detail here. Instead we focus on that excerpt of control theory in which our application does reside. For a more general overview we refer the interested reader to [Zer06a], [Ilc05], [IM05] and [Sch10, Chapter 1]. It is mainly these sources that we base this section on. Also [Zer06b] is a good starting point.

Let R be an arbitrary ring and let $\mathscr{S}$ be a left R-module. We will think of R as *operators* acting on a set of *signals*. For instance, R could be a ring of differential operators as in Section 3.2 and $\mathscr{S}$ could be smooth functions. See also Example 8.1 below where we will define the operators and signals we will be dealing with. Other pairs of operator rings with matching signal spaces can be found, for example, in [Zer08].

Matrices of operators act naturally on vectors of signals: Using the notations from Section 5.1, let such a matrix $A = (a_{ij})_{ij} \in {}^s R^t$ and a vector $w = {}^t(w_1, \ldots, w_t) \in {}^t\mathscr{S}$ be given. Then we define

$$A \bullet w = \begin{pmatrix} a_{11} & \cdots & a_{1t} \\ \vdots & \ddots & \vdots \\ a_{s1} & \cdots & a_{st} \end{pmatrix} \bullet \begin{pmatrix} w_1 \\ \vdots \\ w_t \end{pmatrix} = \begin{pmatrix} \sum_{k=0}^{t} a_{1k} \bullet w_k \\ \vdots \\ \sum_{k=0}^{t} a_{sk} \bullet w_k \end{pmatrix} \in {}^s\mathscr{S}$$

where the bullet denotes the module action. Using the R-module properties of $\mathscr{S}$ it is easy to prove

that $\mathbf{1}_t \bullet w = w$ as well as $(A+C)\bullet w = A\bullet w + C\bullet w$ and $(BA)\bullet w = B\bullet(A\bullet w)$ where $B \in {}^rR^s$ and $C \in {}^sR^t$ are additional matrices of operators. We will sometimes omit the bullet if no confusion can arise.

A (linear) *system* in this context is a set of equations which we write as a single matrix equation

$$Lw = 0$$

where $L \in {}^sR^t$ are the *system laws* while w is sometimes referred to as the *system variables*. Confer also [Zer08, Section 3], [IM05, Section 1.1], [ZL06, Section 1] or [Sch10, Section 1.2]. The intuition is that the signals w represent, for example, physical entities such as mass or velocity and the system laws describe their interaction. Closely connected to the system is the *behaviour*

$$\mathscr{B} = \{w \in {}^t\mathscr{S} \mid Lw = 0\}.$$

Confer again [Zer06a]. The matrix L in this context is also called a *representation* of $\mathscr{B}$. It is not uniquely determined by $\mathscr{B}$ but may be modified, for example, by multiplication with unimodular matrices from the left.

Often, linear systems will be denoted in a slightly different fashion as

$$Ax = Bu$$

where $A \in {}^nR^n$ and $B \in {}^nR^m$. The signals x are called the *state* of the system while u is called the *input*. This implies that the model has already been partitioned into entities that may be influenced directly and others which can only be controlled only indirectly through the interaction of the system variables via the system laws. In this context, the problem whether a system can be forced to reach any given state by only manipulating the inputs is known as *controllability*. Every system of the form $Ax = Bu$ may be regarded as a system in the previous sense by writing it as

$$(A, -B)\begin{pmatrix} x \\ u \end{pmatrix} = 0.$$

For the converse see [Zer06b, Section 3.2].

Example 8.1 ([AM11])**.** Let $\mathscr{M}(U, \mathbb{C})$ be the field of meromorphic functions over $\Omega \subseteq \mathbb{C}$. An example of a linear system is given by

$$\begin{aligned} \dot{x}_1(t) - s(t)\big(x_2(t-\tau) - x_2(t-2\tau)\big) &= 0 \\ \dot{x}_2(t) &= u(t-\tau) \end{aligned}$$

where x_1 and x_2 are the state, u is the input and $s \in \mathscr{M}(U, \mathbb{C})$ is a parameter. Here, the dot means derivation. If we denote the standard derivation operator by d/dt and the τ-shift by $\mathfrak{s}$ which acts on a function as $\mathfrak{s}a(t) = a(t-\tau)$, then we can define the iterated Ore polynomial ring

$$R = \mathscr{M}(U, \mathbb{C})[\partial; \mathrm{id}, \tfrac{d}{dt}][\delta; \mathfrak{s}, 0]$$

which allows us to write the system as a matrix equation

$$\underbrace{\begin{pmatrix} \frac{d}{dt} & s\delta^2 - s\delta \\ 0 & \frac{d}{dt} \end{pmatrix}}_{=A \in {}^2R^2} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 \\ \delta \end{pmatrix}}_{=B \in {}^2R^1} u.$$

(We omitt the variable t from the notation if no confusion can arise.) The ring R is called the ring of *differential time-delay operators*. We will see it again below.

Real world system are in general not linear. They can, however, often be *linearised*. See [Sch10, Section 1.1] for an example of simple non-linear system and its linearisation. We will treat only linear systems here.

8.2 Differential flatness

The properties we will concentrate on in this thesis are differential flatness and the connected concept of π-flatness—see Definitions 8.2 and 8.7. First discussed in [Mar92] and [FLMR95], flatness has become an important tool for applied control theory. Confer for example to [Lév09], [MMR97] or [SRA04] for some examples of applications. Extensions to time-delay systems have been proposed in [Mou95], [Pet00], [MCL10] and others; yet other approaches may be found in [RW97] or [CQR05].

We consider in this section an Ore polynomial ring $R = K[\partial; \mathrm{id}, \vartheta]$ over a differential skew field K with derivation $\vartheta\colon K \to K$. The exact field we use will be specified later. Our definition of flatness is similar to that of [CQR05, Definition 14].

Definition 8.2 (Flatness)**.** A system $Ax = Bu$ with $A \in {}^nR^n$ and $B \in {}^nR^m$ is *flat* if there exist matrices $P \in {}^mR^n$, $Q \in {}^nR^m$ and $T \in {}^mR^m$ such that

$$\begin{pmatrix} Q \\ T \end{pmatrix} {}^m\mathscr{S} = \mathscr{B} \qquad \text{and} \qquad PQ = \mathbf{1}_m$$

where $\mathscr{B} = \{\left(\begin{smallmatrix} x \\ u \end{smallmatrix}\right) \in {}^{m+n}\mathscr{S} \mid Ax = Bu\}$ is the behaviour and $\mathscr{S}$ the signal space.

In order to see the similarity with [CQR05, Definition 14], one has to replace the matrix R in that definition by $(A, -B)$, Q by $\left(\begin{smallmatrix} Q \\ T \end{smallmatrix}\right)$ and T by $(P, {}_m\mathbf{0}_m)$. Another way of characterising flatness is to say that $Ax = Bu$ is flat if and only if there are matrices $P \in {}^mR^n$, $Q \in {}^nR^m$ and $T \in {}^mR^m$ such that

1. for all $x \in {}^n\mathscr{S}$ and $u \in {}^m\mathscr{S}$ satisfying $Ax = Bu$ there exists exactly one $y \in {}^m\mathscr{S}$ such that $x = Qy$ and $u = Ty$,
2. $AQy = BTy$ for all $y \in {}^m\mathscr{S}$, and
3. for all $y \in {}^m\mathscr{S}$ exist $x \in {}^n\mathscr{S}$ and $u \in {}^m\mathscr{S}$ satisfying $Ax = Bu$ such that $y = Px$.

(Compare this way of explaining flatness also to [MCL10, Definition 2].) The equivalence to Definition 8.2 is easy to see: The second point follows from the first condition $\left(\begin{smallmatrix} Q \\ T \end{smallmatrix}\right) {}^m\mathscr{S} = \mathscr{B}$ since this just means that for $y \in {}^m\mathscr{S}$ we have $\left(\begin{smallmatrix} Qy \\ Ty \end{smallmatrix}\right) \in \mathscr{B}$, that is, $AQy = BTy$. Because of the equality in the first condition of the definition there must be at least one y for every $\left(\begin{smallmatrix} x \\ u \end{smallmatrix}\right) \in \mathscr{B}$ such that $Qy = x$ and $Ty = u$. Since $Qy = x = Q\tilde{y}$ for a second $\tilde{y}$ implies $y = PQy = PQ\tilde{y} = \tilde{y}$ using the second condition of Definition 8.2, there can only be one such y, that is, the uniqueness of the first point is proven. Last, the third point follows since

$${}^m\mathscr{S} = PQ\,{}^m\mathscr{S} = \begin{pmatrix} P, & {}_m\mathbf{0}_m \end{pmatrix} \begin{pmatrix} Q \\ T \end{pmatrix} {}^m\mathscr{S} = \begin{pmatrix} P, & {}_m\mathbf{0}_m \end{pmatrix} \mathscr{B},$$

that is, ${}^m\mathscr{S}$ equals the set of all Px where there is u such that $\left(\begin{smallmatrix} x \\ u \end{smallmatrix}\right) \in \mathscr{B}$, that is, such that $Ax = Bu$.

Another characterisation for flatness is given in [CQR05, Theorem 3 6]: Assuming that $\mathscr{S}$ is an injective cogenerator—see [CQR05, Definition 13]—, a system $Ax = Bu$ is flat if and only if the *system module*

$$\frac{R^{m+n}}{R^n(A,-B)}$$

is a free R-module. The later fact can be checked by computing the extension module. See [CQR05] for methods to do so and statements about which additional requirements on R have to be imposed. The actual computations in [CQR05] are done using Gröbner bases.

We will base our approach for checking flatness here on [MCL10]. There, flatness is computed using the concept of hyper-regular matrices.

Definition 8.3 ([MCL10, Definition 1])**.** A matrix $M \in {}^nR^m$ is *hyper-regular* if its Jacobson normal form—see Definition 7.1—is $\mathrm{diag}(1,\dots,1)$.

We recall that the diagonal matrix notation does not imply a square matrix. That is, the matrix $\mathrm{diag}(1,\dots,1)$ in the definition could be of the shape

$$\begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix} \quad \text{for } n \geq m, \qquad \text{or} \qquad (\mathbf{1}_n, {}_{m-n}\mathbf{0}_n) \quad \text{for } n \leq m.$$

Our main contribution is to get rid of the Jacobson normal form in the definition. This will lead to an algorithm with decreased theoretical complexity. Assume first that $n \geq m$. Then $M \in {}^nR^m$ is hyper-regular if and only if there are matrices $S \in \mathrm{Gl}_n(R)$ and $T \in \mathrm{Gl}_m(R)$ such that

$$SMT = \begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix}$$

Multiplying by T^{-1} from the right, this is equivalent to

$$SM = \begin{pmatrix} T^{-1} \\ {}_{n-m}\mathbf{0}_m \end{pmatrix}$$

This in turn is equivalent to

$$\underbrace{(\mathrm{diag}(T, {}_{n-m}\mathbf{0}_{n-m})\, S)}_{=Q} M = \begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix}$$

where $Q \in \mathrm{Gl}_n(R)$. Considering only the first m rows of Q we obtain a matrix $\tilde{Q} \in {}^mR^n$ such that $\tilde{Q}M = \mathbf{1}_m$. Thus, we have shown that hyper-regularity of M in the case $n \geq m$ implies the existence of a left inverse of M.

Conversely, if there is a left inverse $\tilde{Y} \in {}^mR^n$ of M, then this implies that all unit vectors are in the row space of M. This means, that row-reduction—see Algorithm 5.13—applied to M must yield a unimodular matrix $Y \in \mathrm{Gl}_n(R)$ such that

$$YM = \begin{pmatrix} F \\ {}_{n-m}\mathbf{0}_m \end{pmatrix}$$

with $F \in {}^mK^m$ being of full rank by [BCL06, Lemma A.1 (d)]—compare this also to the proof of Lemma 5.15. Thus, taking $S = \mathrm{diag}(F^{-1}, \mathbf{1}_{n-m})Y \in \mathrm{Gl}_n(R)$ and $T = \mathbf{1}_m$ we see that M is hyper-regular.

In the case $n \leq m$, the analogous considerations yield that M is hyper-regular if and only if it possesses a right inverse. We formulate this as a lemma.

Lemma 8.4. *A matrix $M \in {}^nR^m$ is hyper-regular if and only if $n \geq m$ and M has a left inverse or $n \leq m$ and M has a right inverse.*

Moreover, we may use row- or column-reduction to check for hyper-regularity.

In [MCL10], hyper-regularity is shown to be a useful tool for checking a system for flatness. We quote their main theorem.

Theorem 8.5 ([MCL10, Theorem 2])**.** *A system $Ax = Bu$ with $A \in {}^nR^n$, $B \in {}^nR^m$, $n \geq m$ and $(A, -B)$ having maximal rank is flat if and only if B and the matrix*

$$F = ({}_{n-m}\mathbf{0}_m,\ \mathbf{1}_{n-m})\tilde{M}A$$

are hyper-regular where $\tilde{M} \in \mathrm{Gl}_n(R)$ fulfils

$$\tilde{M}B = \begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix}.$$

We note that the assumptions are natural: The independence of the rows of $(A, -B)$ means that there are no superfluous equations—while the hyper-regularity of B means that the inputs are independent of each other. The matrix F in the theorem gives rise to a system $Fx = 0$ which is shown to be equivalent to $Ax = Bu$ in [MCL10, Proposition 1]. There, $Fx = 0$ is called the *implicit representation* while $Ax = Bu$ is the *explicit representation*.

In [MCL10, Theorem 2], there are also formulæ for computing the matrices from Definition 8.2 from the transformation matrices of the Jacobson normal forms of B and F. Reformulating this to the transformation matrices obtained by row-reduction of B and column-reduction of F, we derive the following algorithm for checking a system for flatness.

Algorithm 8.6 (Flatness)**.**

Input Matrices $A \in {}^nR^n$ and $B \in {}^nR^m$ with $n > m$, $(A, -B)$ having R-linearly independent rows and B being hyper-regular.

Output If the system is flat, then matrices $P \in {}^mR^n$, $Q \in {}^nR^m$ and $T \in {}^mR^m$ fulfilling the identities in Definition 8.2; else, $\perp$.[1]

Procedure

1. Apply row-reduction—see Algorithm 5.13—to B obtaining $\tilde{M} \in \mathrm{Gl}_n(R)$ such that
$$\tilde{M}B = \begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix}.$$
2. Compute the matrix $F = ({}_{n-m}\mathbf{0}_m,\ \mathbf{1}_{n-m})\tilde{M}A \in {}^{n-m}R^n$.
3. Apply column-reduction to F: If there is a matrix $\tilde{Q} \in \mathrm{Gl}_n(R)$ such that $F\tilde{Q} = (\mathbf{1}_{n-m},\ {}_{n-m}\mathbf{0}_m)$, then
   (a) Compute $\tilde{Q}^{-1}$.
   This can be done in parallel to computing $\tilde{Q}$ by recording the inverse transformations during column-reduction.

[1] We use $\perp$ as a symbol to represent a failed computation.

(b) Let Q be the last m rows of $\tilde{Q}$, that is,

$$Q = \tilde{Q}\begin{pmatrix} {}_{n-m}\mathbf{0}_m \\ \mathbf{1}_m \end{pmatrix} \in {}^{n}R^{m}.$$

(c) Set P to the last m rows of $\tilde{Q}^{-1}$, that is, $P = ({}_{m}\mathbf{0}_{n-m}, \mathbf{1}_m)\tilde{Q}^{-1} \in {}^{m}R^{n}$.

(d) Set $T = (\mathbf{1}_m, {}_{m}\mathbf{0}_{n-m})\tilde{M}AQ \in {}^{m}R^{m}$.

(e) Return Q, P and T.

4. Else, return $\perp$.

The algorithm is almost the same as [MCL10, Theorem 2] except that row- and column-reduction are used instead of Jacobson normal form computations. We note, that we have—using the definitions from the algorithm—the identity

$$PQ = ({}_{m}\mathbf{0}_{n-m}, \mathbf{1}_m)\tilde{Q}^{-1} \cdot \tilde{Q}\begin{pmatrix} {}_{n-m}\mathbf{0}_m \\ \mathbf{1}_m \end{pmatrix} = ({}_{m}\mathbf{0}_{n-m}, \mathbf{1}_m)\begin{pmatrix} {}_{n-m}\mathbf{0}_m \\ \mathbf{1}_m \end{pmatrix} = \mathbf{1}_m$$

from Definition 8.2. Moreover, for $y \in {}^{m}\mathscr{S}$ the equation

$$AQy = BTy$$

is upon left multiplication by $\tilde{M}$ equivalent to

$$\tilde{M}AQy = \begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix} Ty$$

since $\tilde{M}$ is unimodular. Using the definition of T from the algorithm this becomes

$$\tilde{M}AQy = \begin{pmatrix} \mathbf{1}_m \\ {}_{n-m}\mathbf{0}_m \end{pmatrix} (\mathbf{1}_m, {}_{m}\mathbf{0}_{n-m})\tilde{M}AQy = \begin{pmatrix} \mathbf{1}_m & {}_{m}\mathbf{0}_{n-m} \\ {}_{n-m}\mathbf{0}_m & {}_{n-m}\mathbf{0}_{n-m} \end{pmatrix} \tilde{M}AQy$$

Since F consists just of the lower $n-m$ rows of $\tilde{M}A$, we can rewrite the right hand side obtaining

$$\begin{pmatrix} (\mathbf{1}_m, {}_{n-m}\mathbf{0}_m)\tilde{M}A \\ F \end{pmatrix} Qy = \begin{pmatrix} (\mathbf{1}_m, {}_{n-m}\mathbf{0}_m)\tilde{M}AQ \\ {}_{n-m}\mathbf{0}_n \end{pmatrix} y$$

which holds if and only if

$$FQy = 0.$$

Since by the definition of Q we have

$$FQ = F\tilde{Q}\begin{pmatrix} {}_{n-m}\mathbf{0}_m \\ \mathbf{1}_m \end{pmatrix} = (\mathbf{1}_{n-m}, {}_{n-m}\mathbf{0}_m)\begin{pmatrix} {}_{n-m}\mathbf{0}_m \\ \mathbf{1}_m \end{pmatrix} = {}_{n-m}\mathbf{0}_m$$

where we used $F\tilde{Q} = (\mathbf{1}_{n-m}, {}_{n-m}\mathbf{0}_m)$, this last identity holds for all $y \in {}^{m}\mathscr{S}$. In total, we have proven that

$$\begin{pmatrix} Q \\ T \end{pmatrix} {}^{m}\mathscr{S} \subseteq \{\left(\begin{smallmatrix} x \\ u \end{smallmatrix}\right) \in {}^{n+m}\mathscr{S} \mid Ax = Bu\} = \mathscr{B}.$$

The other inclusion is obtained as follows: Let $Ax = Bu$ for $x \in {}^n\mathscr{S}$ and $u \in {}^m\mathscr{S}$. Then, $y = Px \in {}^m\mathscr{S}$, $Qy = QPyx = x$ and thus $BQy = AQy = Ax = Bu$. Multiplying the last equation with $\tilde{M}$ from the left, we obtain $Qy = u$. Thus, we have the other inclusion and all conditions of Definition 8.2 are fulfilled.

Finally, to see that Algorithm 8.6 is correct, it just remains to use Theorem 8.5 to conclude that the else-branch is reached and $\perp$ is returned if and only if the system is not flat.

In practice, it turns out that flatness alone is too strong—confer, for example, [MCL10]. Therefore, flatness is replaced with the weaker notation of π-flatness. We give a definition that corresponds to [MCL10, Definition 2].

Definition 8.7 (π-flatness)**.** Let K be a field with derivation $\vartheta\colon K \to K$ and automorphism $\alpha\colon K \to K$ such that $\alpha \circ \vartheta = \vartheta \circ \alpha$. We consider the iterated Ore polynomial ring $R = K[\delta;\alpha,0][\partial;\mathrm{id},\vartheta]$.

Let $\pi \in K[\delta;\alpha,0]\setminus\{0\}$ be given. A system $Ax = Bu$ with $A \in {}^nR^n$ and $B \in {}^nR^m$ is *π-flat* if there exist matrices $P \in {}^mR^n$, $Q \in {}^nR^m$ and $T \in {}^mR^m$ such that

$$\pi^{-1}\begin{pmatrix} Q \\ T \end{pmatrix} {}^m\mathscr{S} = \mathscr{B} \qquad \text{and} \qquad \pi^{-1}P \cdot \pi^{-1}Q = \mathbf{1}_m$$

The operator π^{-1} is called a *prediction operator* since it can be interpreted as to allow to consider the "future" of a signal. The iterated Ore polynomial ring is formed by extending ϑ to $K[\delta;\alpha,0]$ by coefficient-wise application. Since α and ϑ commute, one may show that this yields again a derivation which we also denote by ϑ and which allows the construction of R.

A slightly different definition of π-flatness is given in [CQR05, Definition 14] under the name π-freeness but only for domains with constant coefficients, that is, for the case $\alpha(K) = \vartheta(K) = \{0\}$. This means that R will be a commutative polynomial ring where α and ϑ only play a rôle if an element of R is applied to a signal. See also [CQR05, Section 8] for computations and characterisations.

Algorithm 8.6 works for π-flat systems as well: We simply need to do the computations with $K(\delta;\alpha,0)$ as coefficient domain using the construction of Section 3.5. Note, that $\tilde{R} = K(\delta;\alpha,0)[\partial;\mathrm{id},\vartheta]$ is well-defined since the derivation ϑ can be extended to fractions in $K(\delta;\alpha,0)$. Note also, that it may in general not be possible to localise $K[\delta;\alpha,0]$ by a smaller set—see Example 3.9.

Applying the flatness algorithm in $\tilde{R}$ will yield either $\perp$ or the matrices P, Q and T from Definition 8.7. Using [Coh00, Proposition 5.3], we may bring their entries to a common denominator $\pi \in K[\delta;\alpha,0]\setminus\{0\}$.

Using [MCL10, Theorem 2], we can again show that the algorithm is correct, that is, that the computation succeeds if and only if the system is π-flat.

We would like to note that Algorithm 8.6 has for the case of $K(\delta;\alpha,0)[\partial;\mathrm{id},\vartheta]$ been implemented in MAPLE. The package is available online at [Ant11].

We give now an example of a signal set for $K(\delta;\alpha,0)[\partial;\mathrm{id},\vartheta]$. This is a subset of a signal space which was introduced in [Zer06a, Section 3] or [Zer07, Section 3].

Example 8.8. Let $\tau > 0$ and consider the ring

$$R = \mathscr{M}(\mathbb{C})(\delta;\mathfrak{s},0)[\partial;\mathrm{id},d/dt]$$

of differential and time-delay operators with meromorphic coefficients where $\mathfrak{s}a(t) = a(t-\tau)$. This is well defined since by the chain rule we have $(d/dt)(\mathfrak{s}f)(t) = d/dtf(t-\tau) = \mathfrak{s}(df/dt)(t)$ for all $f \in \mathscr{M}(\mathbb{C})$.

We consider the following set of functions with support only in a (affine) half-plane

$$\mathscr{S} = \{f \in \mathrm{C}^\infty(\mathbb{C} \setminus E_f) \mid E_f \subseteq \mathbb{C} \text{ discrete, and } \exists t_f \in \mathbb{R} \forall t \in \mathbb{C}\colon \operatorname{Re} t < t_f \implies f(t) = 0\}.$$

We let δ and d/dt act normally on $\mathscr{S}$. For $\pi \in R$ we define

$$(\pi^{-1} \bullet f)(t) = \sum_{j \geq j_0} a_j(t) \delta^j f(t) = \sum_{\substack{j \geq j_0 \\ \tau^{-1}(\operatorname{Re} t - t_f) \geq j}} a_j(t) f(t - j\tau)$$

where $\pi^{-1} = \sum_{j \geq j_0} a_j \delta^j$ with $a_j \in \mathscr{M}(\mathbb{C})$ for $j \geq j_0$ is the series expansion of π^{-1}. Please note, that this sum is always finite. This definition makes $\mathscr{S}$ into a left R-module.

We would like to conclude the section with an example of how Algorithm 8.6 computes.

Example 8.9. Consider the ring R from the previous example and the system

$$\underbrace{\begin{pmatrix} \partial & s\delta^2 - s\delta \\ 0 & \partial \end{pmatrix}}_{=A \in {}^2R^2} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 \\ \delta \end{pmatrix}}_{=B \in {}^2R^1} u$$

from Example 8.1. The matrix B is hyper-regular with

$$\underbrace{\begin{pmatrix} 0 & \delta^{-1} \\ 1 & 0 \end{pmatrix}}_{=\tilde{M} \in \mathrm{Gl}_2(R)} B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Using $\tilde{M}$, we define

$$F = (0,1)\tilde{M}A = \begin{pmatrix} \partial, & s\delta^2 - s\delta \end{pmatrix}.$$

Also F is hyper-regular, as the calculation

$$F \underbrace{\begin{pmatrix} 0 & 1 \\ (s\delta^2 - s\delta)^{-1} & -(s\delta^2 - s\delta)^{-1}\partial \end{pmatrix}}_{=\tilde{Q} \in \mathrm{Gl}_2(R)} = (1,0)$$

shows. The inverse of $\tilde{Q}$ is

$$\tilde{Q}^{-1} = \begin{pmatrix} \partial & s\delta^2 - s\delta \\ 1 & 0 \end{pmatrix}.$$

This leads to the matrices

$$Q = \tilde{Q} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -(s\delta^2 - s\delta)^{-1}\partial \end{pmatrix} \qquad \text{and} \qquad P = (0,1)\tilde{Q}^{-1} = \begin{pmatrix} 1, & 0 \end{pmatrix}$$

as well as

$$T = (1,0)\tilde{M}AQ = (1,0) \begin{pmatrix} -\delta^{-1}\partial(s\delta^2 - s\delta)^{-1}\partial \\ 0 \end{pmatrix} = \begin{pmatrix} \mathfrak{s}(s)\delta^3 - \mathfrak{s}(s)\delta^2 \end{pmatrix} \partial - \begin{pmatrix} \mathfrak{s}(s)^2\delta^3 - \mathfrak{s}(s)^2\delta^2 \end{pmatrix}^{-1} s'$$

where we used the fact that

$$\partial(s\delta^2 - s\delta)^{-1} = (s\delta^2 - s\delta)^{-1}\partial + \frac{d}{dx}(s\delta^2 - s\delta)^{-1} = (s\delta^2 - s\delta)^{-1}\partial - (s^2\delta^2 - s^2\delta)^{-1} s'.$$

A common denominator is $\pi^{-1} = (\delta^2 - \delta)^{-1}$.

Part V

Conclusion

9

Conclusion and future work

In this thesis we have considered non-commutative polynomials, Ore polynomials. We have used these polynomials to model differential and integral operators. We have looked at matrices containing such polynomials as entries and their one- and two-sided normal forms. We have considered different notions of Gröbner bases over free modules over such polynomial rings and have connected them to the one-sided normal forms. As an application of this connection we have adapted the FGLM algorithm for converting normal forms into each other. Finally, we have utilised normal forms to solve a problem from control theory.

Integro-differential operators provide an interesting example of how Ore polynomials may be used to model operators from calculus. This has applications for the representation and the solving of initial or boundary value problems. A natural extension here—which would fit well with the overall theme of this thesis—is the generalisation to systems of boundary value problems. Also solving systems of differential equations could be done using row- and column-transformation which involve integral operators. Just as with differential operators, matrices of integro-differential operators and their normal forms can be expected to be useful in this context.

Other possibilities for future research would not use matrices but instead explore multivariate integro-differential operators: What if more than one derivation is considered? How about different integrals? And can, for example, difference operators be squeezed into this theory, either as addition to the derivation or with a summation operator as inverse in the form of a stand-alone difference-summation Weyl algebra?

In the part on one-sided normal forms, we have considered the Hermite normal form, the Popov normal form and shifted Popov normal forms. We have shown that all of them are reduced Gröbner bases with respect to particular monomial orderings. Then, we have identified a method of converting Popov normal forms to Hermite normal forms in the literature as an instance of the famous FGLM algorithm.

This work can of course be extended in various ways. Considering the connection of normal forms and Gröbner bases, an interesting question is how other Gröbner basis related methods and algorithms besides the FGLM algorithm translate to normal forms. For instance, another algorithm to compute a Gröbner basis from a given one with a different term ordering is the so-called Gröbner

walk. Future research might try to translate it to normal forms; or to identify a known method in the literature which is already using a Gröbner walk without the connection being known. For this, we expect the shifted Popov normal forms to play a prominent rôle as they allow one to represent a great variety of admissible orderings.

Also the other direction might be interesting to explore: Take any method or algorithm applied to normal forms and translate it to general Gröbner bases. This will most probably yield a way to translate applications of normal forms from the univariate case to the multivariate case where normal forms in the classical sense might not exist or might not be powerful enough. Gröbner bases, on the other hand, can easily be defined and computed for more than one variable.

The Jacobson normal form has been considered only for differential operators in this thesis and only for the case that the torsion module was cyclic. This allowed us to obtain a Jacobson normal form from the annihilator of the cyclic vector where the transformation matrices could be computed using basic methods. In general, for positive characteric or for other Ore polynomials than differential operators the torsion module will not be cyclic. A goal for future research would be to try to extend the algorithm also to these cases. At least the computation of the transformation matrices from a known decomposition of the torsion module into cyclic subparts seems to be within reach.

Experiments with the Jacobson normal form algorithm have shown that a wrong choice of the cyclic vector can lead to matrices with large coefficients. This is a problem which has also been noticed before—see, for example, [Bar99]—and refrains applied researchers from the use of the Jacobson normal form. It has almost always been possible, though, to also find a cyclic vector which yielded a matrix with comparatively low coefficients. It would be interesting to study, how a good choice for the cyclic vector can be made or whether there are methods to transform a bad cyclic vector to a better one.

We have shown how normal form computations may be applied to solve problems in control theory. In this thesis we just scratch the surface of this vast field. Our presentation here yields two immediate questions: First, using the connection between normal forms and Gröbner bases, how might Gröbner bases help to generalise univariate control theory algorithms to several variables? And, second, since certain normal forms have additional properties—such as the Popov normal form yielding a minimal degree representation of the row space—could this be exploited in order to obtain "nice" solutions to control theory problems? For instance, can the transformation matrices in the definition of flatness be chosen in a canonical way?

Appendices

Maple code

9.1 leading row coefficient matrices

A possible implementation for the *leading vector* defined in Section 5.1 in MAPLE is given by the following code. As it relies on the standard functions for coefficients and the degree of expressions, it is not applicable for Ore polynomial representations using the `OreAlgebra` package. Optional arguments denote the main variable of the expressions and a degree bound that is included for use in later functions.

```
lvector := proc(v::Vector, {deg::nonnegative := ∞ , var::symbol := 'X'})::Vector;
local d;
description "Compute the leading vector of a vector.";
    d := max(map(degree, v, var));
    if d ≤ deg then return map(coeff, v, var, d)
    else return map(0, v)
    end if
end proc:
```

Note that one has to make sure that the entries of the input vector are simplified since otherwise the `degree` function may give wrong results.

We want to illustrate the computation of the *leading row coefficient matrix* from Section 5.2 by the corresponding MAPLE code. First, we define an auxilliary function that maps a given function to each row of a matrix similar to what the built-in MAPLE function `map` does.

```
mapRows := proc(M::Matrix, f::procedure)::Matrix;
local s, t, N, i;
description "Map a function to all rows of a matrix.";
    s, t := LinearAlgebra:-Dimension(M);
    return <seq(f(M[i, 1 .. t]), i = 1 .. s)>
end proc:
```

Now, using the leading vector function defined earlier, a possible implementation for the leading row coefficient matrix can be given as follows. Note, that by the use of the `_rest` variable we can pass optional arguments to `lvector`.

```
LC := proc(M::Matrix)::Matrix;
local v, params;
    params := _rest:
```

```
    return mapRows(M, v → lvector(v, params))
end proc:
```

9.2 Popov normal form to Hermite normal form

We shortly give an implementation of these definitions in the computer algebra system MAPLE. Since MAPLE forces us to distinguish between vectors and matrices we will start with a procedure for the degree $\deg v$ of a (row) vector v. It expects as parameters a symbol Q that will denote how the variable ∂ is represented in MAPLE.[1] The second argument is the vector. The procedure may produce erroneous output if the entries of v are not expanded.

```
VectorDegree := proc(Q::symbol, v::Vector) :: extended_numeric:
description "Computes the degree of v w.r.t. the variable Q.":
    return max(map(p → degree(p,Q), v)):
end proc:
```

The definition of vector degrees can be expanded easily to matrices by first computing all row degrees and then selecting the maximum value. The parameters of this procedure are similar to the preceding one.

```
MatrixDegree := proc(Q::symbol, M::Matrix) :: extended_numeric:
description "Computes the degree of M w.r.t. the variable Q.":
local m,n:
    m,n := LinearAlgebra:-Dimension(M):
    return max(seq(RowDegree(Q,j,M),j=1..m)):
end proc:
```

Specialising the above code a little bit, we may also compute the j^{th} row degree $\deg M_{j,*}$ of a matrix M using the following procedure. The parameters are analogous to the former two procedures. The ASSERT statement will check the validity of its input if the `assertlevel` in the MAPLE `kernelopts` is set to 1 or more.

```
RowDegree := proc(Q::symbol, j::posint, M::Matrix) :: extended_numeric:
description "Computes the j-th row degree of M w.r.t. the variable Q.":
local m,n:
    m,n := LinearAlgebra:-Dimension(M):
    ASSERT(j ≤ m):
    return VectorDegree(Q,M[j,1..n]):
end proc:
```

The next procedure computes the leading monomial of the non-zero vector v with respect to position over term ordering where the first argument Q tells us how the variable ∂ is denoted in MAPLE. The procedure does not return a vector but a pair i,d such that $\operatorname{lm}(v) = \partial^d \mathbf{e}_i$. If the elements of v are not expanded then the output might not be correctly computed.

```
POTlmonom := proc(Q::symbol, v::Vector) :: list(nonnegint):
description "POT leading monomial of v as pair of position and degree.":
local p,i:
    p := LinearAlgebra:-Dimension(v):
```

[1] We would have liked to call the parameter `D`—but this causes trouble as `D` is a built-in function in MAPLE.

```
    for i to p do
        if v[i] ≠ 0 then return i, degree(v[i],Q) fi:
    od:
    error "Leading term of zero is undefined!":
end proc:
```

Analogously, the next procedure computes the leading monomial of the non-zero vector v with respect to term over position ordering. Parameters and output are as above. In fact, we use the trick that $\mathrm{lm}(v)$ with respect to term over position ordering equals $\partial^{\deg v}\,\mathrm{lm}(\mathrm{lv}(v))$ where the last leading term is taken with respect to position over term ordering.

```
TOPlmonom := proc(Q::symbol, v::Vector) :: list(nonnegint):
description "TOP leading monomial of v as pair of position and degree.":
local d,p:
    d := VectorDegree(Q,v):
    assert(d ≥ 0):
    POTlmonom(Q, map(p → coeff(p,Q,d)·Q^d, v)):
end proc:
```

We will now implement the computation of the truncated basis and multiplication matrix as in Remarks 6.35 and 6.33. The procedure expects as input a symbol Q that tells MAPLE how the variable ∂ is represented, a degree bound d, a procedure lt computing the leading term of a vector and finally the matrix $M \in {}^mR^n$ itself which must be a Gröbner basis for the ordering that is used in lt. The procedure returns the truncated multiplication matrix with respect to d, the coordinate vectors of the residue classes of the canonical basis vectors $\mathfrak{e}_1,\ldots,\mathfrak{e}_n$ of R^n and the dimension of truncated space. Note, that for an easier implementation we chose to order the vectors in the canonical basis differently than in the definition: Here, they are sorted with respect to to position in ascending order.

```
ModularSpace := proc(Q::symbol, d::posint, lt::procedure, M::Matrix)
    :: list:
description "Compute the truncated modular structure of R^n/R^m M.":
```

We start by computing the positions and degrees of the pivot elements in M: The meaning of a tuple (i,j,k) in the list ϱ is that there is a pivot at position (i,j) in M with degree $\deg M_{i,j} = k$. The list σ will contain information about the columns of M. If $\sigma_j = \infty$ then there is no pivot in the j^{th} column of M. Else, if $\sigma_j = (k,i)$ then there is a pivot of degree k in the i^{th} row. The list τ contains information about the elements of the truncated basis: These are precisely the vectors $\overline{\partial^k \mathfrak{e}_j}$ where $k < \tau_j$. Finally, e contains the dimension of the truncated space.

```
local ϱ,σ,m,n,e,a,T,τ,j,z,r,c,i,E,k:
    m,n := LinearAlgebra:-Dimension(M):
    ϱ:= [seq([j,lt(M[j,1..n])], j=1..m)]:
    σ:= [∞$n]:
    for j in ϱ do
        σ[j[2]] := [j[3], j[1]]:
    od:
    τ:= map(a → if a = ∞ then d else min(a[1],d) fi, σ):
    e := add(a, a in τ):
```

Initially, the truncated multiplication matrix T is just the zero matrix. We will fill in its entries later in the procedure. Also the list of coordinate vectors of the canonical basis elements is initially set to

just empty entries. The variable r will contain the sum $\sum_{s<j}\tau_s$ with j being the control variable of the outmost loop. This will be used to handle Remark 6.33. Initially, r is of course zero.

```
    T := Matrix(e,e,0):
    E := [empty$n]:
    r := 0:
    for j to n do
```

For the j^{th} column of M we have to check whether it contains a pivot of degree zero. This is the case if $\tau_j = 0$. That means that $\mathfrak{e}_j$ is reducible by M and we have to compute its coordinates as described in Remark 6.35. We start with a zero vector filling in the corresponding entries in a loop. The variable c corresponds to the sum $\sum_{s<k}\tau_k$ in the remark and i is μ. Furthermore, $\sigma_{j,2}$ corresponds to i in Remark 6.35.

```
        if τ[j] = 0 then
            z := Vector[row](e,0):
            c := 0:
            for k to n do
                for i from 0 to τ[k]-1 do
                    z[c+i+1] := -coeff(M[σ[j][2],k],Q,i):
                od:
                c := c+τ[k]:
            od:
            E[j] := z:
```

If the j^{th} column does not contain a pivot of degree zero then the representation of $\mathfrak{e}_i$ is just the $(r+1)^{\text{th}}$ unit vector according to Remark 6.35. Additionally, we have to treat the r^{th} through $(r+\tau_j-1)^{\text{th}}$ row of the truncated multiplication matrix corresponding to the truncated basis elements $\overline{\mathfrak{e}_j}$ through $\overline{\partial^{\tau_j-2}\mathfrak{e}_j}$. We first fill in the ones on the upper secondary diagonal according to Remark 6.33. If the row does not contain a pivot then we are already done. Otherwise, we treat $(r+\tau_j)^{\text{th}}$ row analogously to the computation of the coordinates in the case of a zero-degree pivot.

```
        else
            E[j] := Vector[row](e, shape=unit[r+1]):
            #
            for r from r+1 to r+τ[j]-1 do
                T[r,r+1] := 1:
            od:
            if σ[j] ≠ ∞ then
                c := 0:
                for k to n do
                    for i from 0 to τ[k]-1 do
                        T[r,c+i+1] := -coeff(M[σ[j][2],k],Q,i):
                    od:
                    c := c+τ[k]:
                od:
            fi:
            #
        fi:
    od:
    return T,E,e:
end proc:
```

Finally, we would like to present a MAPLE procedure implementing the conversion algorithm for the special case of converting a matrix $M \in {}^m R^n$ in Popov form into a matrix H in Hermite form. The input parameters are Q denoting how the variable ∂ is represented in MAPLE, the automorphism σ as map of vectors, the derivation ϑ as map of vectors and the matrix M which must be in Popov form. The output will be the Hermite form of M.

```
Convert := proc(Q::symbol, σ::appliable, ϑ::appliable, M::Matrix)
    :: Matrix:
description "Convert M in Popov form into Hermite form.":
```

The procedure starts by setting some constants: As usual, with m and n we denote the dimensions of the matrix, $d-1$ is the bound for the degrees in H. We use the procedure `ModularSpace` defined on page v to compute the truncated multiplication matrix T and a list E containing the coordinate vectors of the residue classes of the canonical basis vectors $\mathfrak{e}_1, \ldots, \mathfrak{e}_n$ of R^n in the truncated basis. The variable B is just $\mathfrak{B}_2$ from Algorithm 6.37, H is G_2 and C will hold the coordinate vectors of the entries in B. The variable r contains the number of linear independent elements in B.

```
local T,m,n,d,H,C,B,j,w,k,v,S,E,F,e:
    m,n := LinearAlgebra:-Dimension(M):
    d := m·n·MatrixDegree(Q,M)+1:
    T,E,e := ModularSpace(Q,d,v → TOPlmonom(Q,v),M):
    C := []:
    B := []:
    H := []:
```

Now, we iterate over the monomials in R^n. Since we are using a fixed term ordering—namely the position over term ordering—we have the procedure already specialised for this. The outer loop iterates over all column indices j and inner loop iterates over the exponents k from 0 through d. All the time, we have $w = \partial^k \mathfrak{e}_j$ and $v = w_{\mathfrak{B}_1}$. If v is linear independent of the previous coordinate vectors that have been stored in C then we add v to C and w to B and continue the loop with ∂w. Else do we compute a linear combination S such that $v = S^T C$.[2] Then we add $w - S^T B$ to H and break the inner loop continuing with the next column index. We are adding $w - S^T B$ to the top of H since the rows of the result should be sorted in descending order by Theorem 6.30.

```
    for j from n by -1 to 1 do
        w := Vector[row](n, shape=unit[j]):
        v := E[j]:
        for k to d do
            if nops(C) < LinearAlgebra:-Rank(<op(C),v>) then
                C := [op(C),v]:
                B := [op(B),w]:
                v := σ(v).T + ϑ(v):
                w := Q·w:
            else
                F := LinearAlgebra:-Transpose(<op(C),v>):
                S := LinearAlgebra:-LinearSolve(F):
                H := [w - LinearAlgebra:-Transpose(S).<op(B)>, op(H)]:
                break:
            fi:
        od: # Inner loop
```

[2] We have to transpose C since MAPLE's `LinearAlgebra:-LinearSolve` expects this.

```
    od: # Outer loop
    return <op(H)>:
end proc:
```

We give an example of a MAPLE session for a computation in $\mathbb{Q}[x]$ using the procedures just defined. In order to work with commutative polynomials we set $\sigma = \mathrm{id}$ and ϑ to be the zero map. The variable is denoted by x.

```
Q := 'x': σ := v → v: ϑ := v → map(0,v):
```

We consider the following example

```
M := <<1|x|1>,<1|0|x>>;
```

$$M := \begin{bmatrix} 1 & x & 1 \\ 1 & 0 & x \end{bmatrix}$$

The Hermite form is computed by our procedure using

```
H := Convert(Q,σ,ϑ,M);
```

$$H := \begin{bmatrix} 1 & 0 & x \\ 0 & x & 1-x \end{bmatrix}$$

We may check this result using MAPLE's built-in procedure for Hermite form computation:

```
H = LinearAlgebra:-HermiteForm(M);
```

$$\begin{bmatrix} 1 & 0 & x \\ 0 & x & 1-x \end{bmatrix} = \begin{bmatrix} 1 & 0 & x \\ 0 & x & 1-x \end{bmatrix}$$

9.3 Code extraction

The MAPLE code in this thesis is inserted using the *listings* package. This very useful LaTeX package allows the code to be included just as normal text with no need for the author to add special annotations. The package itself will take care for all formatting. The big advantage of this approach is that the code can just be copied and pasted from the LaTeX source file directly into MAPLE.

Of course, it is also possible to collect the functions presented here in a MAPLE source file that can then be used separately. The following *Awk* script extracts everything which is between `\begin{lstlisting}` and `\end{lstlisting}` in a LaTeX file. Applied to this thesis' source file it will thus yield the complete code included here.

```
BEGIN { CODE = 0 }
$0~/^\\end{lstlisting}/ { print "\n\n"; CODE = 0 }
{ if(CODE == 1) print $0 }
$0~/^\\begin{lstlisting}[^[]/ { CODE = 1 }
```

Nomenclature

$\mathrm{A}_1(\partial)$	first Weyl algebra, 11
$\mathrm{A}_1(\partial, \int)$	integro-differential Weyl algebra, 27
$A[\partial; \sigma, \vartheta]$	ring of Ore polynomials over A with respect to σ and ϑ, 10
$\mathrm{A}_1(\int)$	integro Weyl algebra, 28
$\mathrm{A}_1(\int)\int$	two-sided ideal generated by $\int$ in $\mathrm{A}_1(\int)$, 31
$\mathrm{C}^\infty(\mathbb{R})$	smooth functions over $\mathbb{R}$, 20
$\operatorname{coeff}(\partial^s, f)$	coefficient of ∂^s in f, 9
∂	Ore indeterminate, 9
$\deg f$	degree of f, 9
$\left\{ {m \atop k} \right\}$	diffnomial for m and k, 12
$\mathtt{E}$	boundary operator, 23
e_{ij}	boundary operator, 23
ε	evaluation map, 20
$\mathscr{F}[\partial]$	differential operators (only in Chapter 4), 21
$\mathscr{F}[\partial, \int]$	integro-differential operators, 21
$\mathscr{F}[\mathtt{E}]$	boundary operators, 21
$\mathscr{F}[\int]$	integral operators, 21
$\operatorname{lc}(\mathfrak{v})$	leading coefficient of $\mathfrak{v}$ with respect to $<$, 62
$\alpha <_{\text{lex}} \beta$	α is less than β with respect to to the lexicographic ordering, 59
$\operatorname{lm}(\mathfrak{v})$	leading monomial of $\mathfrak{v}$ with respect to $<$, 62

$\mathrm{lt}(\mathfrak{v})$	leading term of $\mathfrak{v}$ with respect to $<$, 62
$\mathfrak{v} <_{\mathrm{POT}} \mathfrak{w}$	$\mathfrak{v}$ is smaller than $\mathfrak{w}$ with respect to the position over term ordering, 60
$\mathfrak{v} <_{\mathrm{TOP},\xi} \mathfrak{w}$	$\mathfrak{v}$ is smaller than $\mathfrak{w}$ with respect to the ξ-term over position ordering, 60
$\mathfrak{v} <_{\mathrm{TOP}} \mathfrak{w}$	$\mathfrak{v}$ is smaller than $\mathfrak{w}$ with respect to the term over position ordering, 59
$\int$	integral map, 19
∂	differential indeterminate in the integro-differential Weyl algebra, 23
$\int$	integral indeterminate in the integro-differential Weyl algebra, 23
$K\langle\partial,\int\rangle$	integro-differential operators with constant coefficients, 23
$K(\partial;\sigma,\vartheta)$	full ring of fractions of $K[\partial;\sigma,\vartheta]$, 17
$\mathrm{lc}(f)$	leading coefficient of f, 9
${}_s\mathbf{0}_t$	$s \times t$ zero matrix, 39
$\mathbf{1}_s$	$s \times s$ identity matrix, 39
$\deg M$	degree of the matrix M, 39
$\mathrm{diag}(a_1,\ldots,a_n)$	diagonal matrix having the diagonal entries $a_1,\ldots,a_n$, 39
$\mathrm{Gl}_s(R)$	unimodular $s \times s$ matrices with entries in R, 39
$\mathrm{lv}(\mathfrak{v})$	leading vector of $\mathfrak{v}$, 39
$M_{i,*}$	i^{th} row of the matrix M, 39
$M_{\{i_1,\ldots,i_r\},*}$	matrix consisting of the rows $M_{i_1,*}, \ldots, M_{i_r,*}$ of the matrix M, 39
$M_{\overline{\{i_1,\ldots,i_r\}},*}$	equal to $M_{\{1,\ldots,s\}\setminus\{i_1,\ldots,i_r\},*}$, 39
$M_{*,j}$	j^{th} column of the matrix M, 39
$M_{*,\{j_1,\ldots,j_r\}}$	matrix consisting of the columns $M_{*,j_1}, \ldots, M_{*,j_r}$ of the matrix M, 39
$M_{*,\overline{\{i_1,\ldots,i_r\}}}$	equal to $M_{*,\{1,\ldots,s\}\setminus\{i_1,\ldots,i_r\}}$, 39
$\overline{\mathfrak{v}}$	residue class of $\mathfrak{v}$, 68
R^t	row vectors of length t with entries in R, 39
$R^s M$	row space of the matrix M, 40
${}^sR$	column vectors of length s with entries in R, 39
${}^sR^t$	$s \times t$ matrices with entries in R, 39
$\mathrm{Ann}_R\, v$	annihilator of v in R, 83

$A \bullet v$	A acts on v, 91
$\mathbb{R}$	real numbers, 20
$\mathrm{LC}^k_{\mathrm{row}}(M)$	k^{th} leading row coefficient matrix of the matrix M, 40
$\mathrm{LC}_{\mathrm{row}}(M)$	leading row coefficient matrix of the matrix M, 40
$\mathrm{LV}_{[}(d)]\mathfrak{M}$	d^{th} leading vector space of the module $\mathfrak{M}$, 42
$S^{-1}A$	left localisation of A by S, 17
$\perp$	failed computation, 95
$\mathscr{M}(U, \mathbb{C})$	field of meromorphic functions over $\Omega \subseteq \mathbb{C}$, 92

Index

Bibliography

[Adj88] K. Adjamagbo: *Sur l'effectivité du lemme du vecteur cyclique*. C. R. Acad. Sci. Paris Sér I Math., **vol. 306**(13): pp. 543–546, 1988.

[AL94] W. W. Adams and P. Loustaunau: *An introduction to Gröbner bases*. Graduate studies in mathematics. AMS, 1994.

[AM10] F. Antritter and J. Middeke: *An efficient algorithm for checking hyper-regularity of matrices*, July 2010. URL http://www.issac-conference.org/2010/. Poster presentation at ISSAC 2010.

[AM11] _____ *A toolbox for the analysis of linear systems with delays*. In: *Submitted to: 50th IEEE Conference on Decision and Control*, 2011.

[Ant11] F. Antritter: *kddt.mla*. www.unibw.de/eit8_1/forschung-en/index_html?set_language=en, Last accessed: June 2011. MAPLE package.

[Bar99] M. A. Barkatou: *On rational solutions of systems of linear differential equations*. Journal of Symbolic Computation, **vol. 28**(4–5): pp. 547–567, October 1999.

[Bax60] G. Baxter: *An analytic problem whose solution follows from a simple algebraic identity*. Pacific Journal of Mathematics, **vol. 10**: pp. 731–742, 1960.

[BCL06] B. Beckermann, H. Cheng, and G. Labahn: *Fraction-free row reduction of matrices of Ore polynomials*. Journal of Symbolic Computation, **vol. 41**: pp. 513 – 543, 2006.

[BD78] G. M. Bergman and W. Dicks: *Universal derivations and universal ring constructions*. Pacific Journal of Mathematics, **vol. 79**(2): pp. 293–337, 1978.

[Ber78] G. M. Bergman: *The diamond lemma for ring theory*. Advances in Mathematics, **vol. 29**(2): pp. 178–218, February 1978.

[BGTV03] J. L. Bueso, J. Gómez-Torrecillas, and A. Verschoren: *Algorithmic methods in non-commutative algebra*, vol. 17 of *Mathematical modelling: Theory and applications*. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2003.

[BIV89] R. Brüske, F. Ischebeck, and F. Vogel: *Kommutative Algebra*. Bibliographisches Institut, Mannheim, 1989. German.

[BLV99] B. Beckermann, G. Labahn, and G. Villard: *Shifted normal forms of polynomial matrices*. In: *Proceedings of the 1999 international symposium on Symbolic and algebraic computation*, ISSAC '99, pp. 189–196. ACM, New York, NY, USA, 1999. URL http://doi.acm.org/10.1145/309831.309929.

[BLV06] _____ *Normal forms for general polynomial matrices*. Journal of Symbolic Computation, **vol. 41**(6): pp. 708–737, June 2006.

[BP96] M. Bronstein and M. Petkovšek: *An introduction to pseudo-linear algebra*. Theoretical Computer Science, **vol. 157**(1): pp. 3–33, 1996. URL citeseer.ist.psu.edu/bronstein96introduction.html.

[Buc65] B. Buchberger: *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal (An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal)*. Ph.D. thesis, Mathematical Institute, University of Innsbruck, Austria, 1965. (English translation to appear in Journal of Symbolic Computation, 2004).

[CF07] G. Carrà-Ferro: *A survey on differential Gröbner bases*. In: M. Rosenkranz and D. Wang (eds.), *Gröbner Bases in Symbolic Analysis*, no. 2 in Radon Series on Computational and Applied Mathematics, pp. 77–108. De Gruyter, 2007.

[Che03] H. Cheng: *Algorithms for normal forms for matrices of polynomials and Ore polynomials*. Ph.D. thesis, University of Waterloo, 2003. Adviser-George Labahn.

[CK02] R. C. Churchill and J. J. Kovacic: *Cyclic vectors*. In: L. Guo, P. J. Cassidy, W. F. Keigher, and W. Y. Sit (eds.), *Differential algebra and related topics*, pp. 191–218. World Scientific Publishing Co. Pte. Ltd., 2002.

[CL07] H. Cheng and G. Labahn: *Output-sensitive modular algorithms for polynomial matrix normal forms*. Journal of Symbolic Computation, **vol. 42**: pp. 733–750, 2007.

[Coh61] P. M. Cohn: *On the embedding of rings in skew fields*. Proceedings of the London Mathematical Society, **vol. (3) 11**: pp. 511–30, 1961.

[Coh69] _____ *Free associatives algebras*. Bulletin of the London Mathematical Society, **vol. 1**(1): pp. 1–39, 1969.

[Coh85] _____ *Free rings and their relations*. Second edn. London Academic Press, London, 1985.

[Coh00] _____ *An introduction to ring theory*. Springer, Berlin Heidelberg New York, 2000.

[Coh03] _____ *Further Algebra and Applications*. Springer, London Berlin Heidelberg New York, 2003.

[Coh05] _____ *Basic Algebra*. Second edn. Springer, London Berlin Heidelberg New York, 2005.

[Cou95] S. C. Coutinho: *A Primer of Algebraic D-Modules*. No. 33 in London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1995.

[CQ05] G. Culianez and A. Quadrat: *Formes de Hermite et de Jacobson: implémentations et applications*. Tech. rep., INRIA Sophia Antipolis, 2005.

[CQR05] F. Chyzak, A. Quadrat, and D. Robertz: *Effective algorithms for parametrizing linear control systems over Ore algebras*. Appl. Algebra Eng., Commun. Comput., **vol. 16**(5): pp. 319–376, 2005.

[CS98] F. Chyzak and B. Salvy: *Non-commutative elimination in Ore algebras proves multivariate identities*. Journal of Symbolic Computation, **vol. 26**(2): pp. 187–227, 1998. URL citeseer.ist.psu.edu/chyzak97noncommutative.html.

[DCL08] P. Davies, H. Cheng, and G. Labahn: *Computing Popov form of general Ore polynomial matrices*. In: *Milestones in Computer Algebra (MICA) 2008*, pp. 149–156, 2008.

[FGLM93] J.-C. Faugère, P. M. Gianni, D. Lazard, and T. Mora: *Efficient computation of zero-dimensional Gröbner bases by change of ordering*. J. Symb. Comput., **vol. 16**(4): pp. 329–344, 1993.

[FLMR95] M. Fliess, J. Lévine, P. Martin, and P. Rouchon: *Flatness and defect of nonlinear systems: introductory theory and examples*. International Journal of Control, **vol. 61**(6): pp. 1327–1361, 1995.

[For75] G. D. Forney, Jr.: *Minimal bases of rational vector spaces with applications to multivariable linear systems*. SIAM J. Control, **vol. 13**: pp. 493 – 520, May 1975.

[Ger00] L. Gerritzen: *Modules over the algebra of the noncommutative equation* $yx = 1$. Arch. Math. (Basel), **vol. 75**(2): pp. 98–112, 2000.

[GG03] J. von zur Gathen and J. Gerhard: *Modern Computer Algebra*. Second edition edn. Cambridge University Press, Cambridge New York Port Melbourne Madrid Cape Town, 2003.

[GK09] M. Giesbrecht and M. S. Kim: *Computer Algebra in Scientific Computing*, vol. 5743 of *Lecture Notes in Computer Science*, chap. On Computing the Hermite Form of a Matrix of Differential Polynomials, pp. 118–129. Springer, Berlin / Heidelberg, 2009.

[Ilc05] A. Ilchmann: *Algebraic theory of time-varying linear systems: a survey*. In: P. Horáček, M. Šimandl, and P. Zítek (eds.), *Selected Plenaries, Milestones and Surveys*, pp. 312–318. 16^{th} IFAC world congress, IFAC, Prague, Czech Republic, July 2005.

[IM05] A. Ilchmann and V. Mehrmann: *A behavioral approach to time-varying linear systems. Part 1: general theory*. SIAM J. Control Optim., **vol. 44**(5): pp. 1725–1747, 2005.

[Jac37] N. Jacobson: *Pseudo-linear transformations*. The Annals of Mathematics, **vol. 38**(2): pp. 484–507, April 1937.

[Jac50] _____ *Some remarks on one-sided inverses*. Proc. Amer. Math. Soc., **vol. 1**: pp. 352–355, 1950.

[Jac85] _____ *Basic Algebra*, vol. I. Second edn. Dover Publications, 1985.

[Jež96] J. Ježek: *Non-commutative rings of fractions in algebraical approach to control theory*. Kybernetika, **vol. 32**(1): pp. 81–94, 1996.

[Kai80] T. Kailath: *Linear Systems*. Prentice-Hall Information and System Science Series. Prentice Hall, 1980.

[Kap76] I. Kaplansky: *An introduction to differential algebra*. Second edition edn. Hermann, Paris, 1976.

[Kou09] C. Koutschan: *Advanced Applications of the Holonomic Systems Approach*. Ph.D. thesis, RISC-Linz, Johannes Kepler University, September 2009. URL http://www.risc.uni-linz.ac.at/research/combinat/software/HolonomicFunctions/.

[KRR11] A. Korporal, G. Regensburger, and M. Rosenkranz: *Regular and singular boundary problems in* MAPLE. In: V. P. Gerdt, E. W. Mayr, W. Koepf, and E. H. Vorozhtsov (eds.), *Computer Algebra in Scientific Computing. Proceedings of the 13th International Workshop (CASC 2011)*, LNCS. Springer, Berlin, 2011. Accepted for publication.

[KRT07] C. Kojima, P. Rapisarda, and K. Takaba: *Canonical forms for polynomial and quadratic differential operators*. Systems & Control Letters, **vol. 56**(11–12): pp. 678–684, November–December 2007.

[KS89] K.-H. Kiyek and F. Schwarz: *Mathematik für Informatiker*, vol. 1. Teubner, 1989.

[Lam01] T.-Y. Lam: *A first course in noncommutative rings*. Graduate texts in mathematics, second edn. Springer, New York Berlin Heidelberg, 2001.

[Lev05] V. Levandovskyy: *Non-commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation*. Phd. thesis, Universität Kaiserslautern, June 2005.

[Lév09] J. Lévine: *Analysis and Control of Nonlinear Systems: A Flatness-based Approach*. Mathematical Engineering Series. Springer, 2009.

[Li96] Z. Li: *A Subresultant Theory for Linear Differential, Linear Difference and Ore Polynomials*. Ph.D. thesis, RISC, Johannes Kepler University Linz, 1996.

[Li98] _____ *A subresultant theory for Ore polynomials with applications*. In: K.-Y. Chwa and O. H. Ibarra (eds.), *Proceedings of ISSAC'98*, no. 1533 in Lecture Notes in Computer Science, pp. 132–139. Springer, 1998.

[Man91] E. Mansfield: *Differential Gröbner bases*. Ph.D. thesis, University of Sidney, 1991.

[Mar92] P. Martin: *Contribution à l'Étude des Systèmes Diffèrentiellement Plats*. Ph.D. thesis, école des Mines de Paris, 1992.

[MCL10] V. Morio, F. Cazaurang, and J. Lévine: *On the computation of π-flat outputs for linear time-delay systems*, 2010. Arxiv:math.OC/0910.3619v2.

[Mid10] J. Middeke: *Conversion between Hermite and Popov normal forms using an FGLM-like approach*. Albanian Journal of Mathematics, **vol. 4**(4): pp. 181–193, December 2010.

[MM82] E. W. Mayr and A. R. Meyer: *The complexity of the word problems for commutative semigroups and polynomial ideals*. Advances in Mathematics, **vol. 46**(3): pp. 305 – 329, 1982. URL http://www.sciencedirect.com/science/article/pii/0001870882900482.

[MMR97] P. Martin, R. M. Murray, and P. Rouchon: *Flat systems*. In: G. Bastin and M. Gevers (eds.), *Plenary Lectures and Minicourses, Proc. ECC 97, Brussels*, pp. 211–264, 1997.

[Mou95] H. Mounier: *Propriétés structurelles des systemes linéaires a retard: aspects théoriques et pratiques*. Ph.D. thesis, University of Paris XI, Paris, France, 1995.

[MR01] J. C. McConnell and J. C. Robson: *Noncommutative Noetherian Rings*. Second edn. American Mathematical Society, Providence, Rhode Island, 2001.

[MS03] T. Mulders and A. Storjohann: *On lattice reduction for polynomial matrices*. Journal of Symbolic Computation, **vol. 35**(4): pp. 377–401, April 2003.

[Ore31] Ø. Ore: *Linear equations in non-commutative fields*. The Annals of Mathematics, **vol. 32**(3): pp. 463–477, July 1931.

[Ore32a] Ö. Ore: *Formale Theorie der linearen Differentialgleichungen (Erster Teil)*. Journal der reinen und angewandten Mathematik, **vol. 167**: pp. 221 – 234, 1932.

[Ore32b] _____ *Formale Theorie der linearen Differentialgleichungen (Zweiter Teil)*. Journal der reinen und angewandten Mathematik, **vol. 168**: pp. 233 – 252, 1932.

[Ore33] O. Ore: *Theory of non-commutative polynomials*. Annals of Mathematics, **vol. 34**: pp. 480 – 508, 1933.

[OS74] K. B. Oldham and J. Spanier: *The fractional calculus*. Academic Press, New York-London, 1974.

[Pau07] F. Pauer: *Gröbner bases with coefficients in rings*. J. Symb. Comput., **vol. 42**(11-12): pp. 1003–1011, 2007.

[Pet00] N. Petit: *Systèmes à retards. Platitude en génie des proc édés et contrôle de certaines équations des ondes*. Ph.D. thesis, Ecole des Mines de Paris, Paris, France, 2000.

[Pop70] V.-M. Popov: *Some properties of control systems with irreducible matrix — transfer functions*. In: *Seminar on Differential Equations and Dynamical Systems, II*, vol. 144 of *Lecture notes in mathematics*, pp. 169–180. Springer, Berlin, 1970.

[Ros05] M. Rosenkranz: *A new symbolic method for solving linear two-point boundary value problems on the level of operators*. Journal of Symbolic Computation, **vol. 39**(2): pp. 171–199, 2005.

[Rot69] G.-C. Rota: *Baxter algebras and combinatorial identities (i, ii)*. Bulletin of the American Mathematical Society, **vol. 75**: pp. 335–334, 1969.

[RR97] C. J. Rust and G. J. Reid: *Rankings of partial derivatives*. In: *Proceedings of ISSAC 1997*, pp. 9–16. ACM, Maui, Hawaii, 1997.

[RR08] M. Rosenkranz and G. Regensburger: *Solving and factoring boundary problems for linear ordinary differential equations in differential algebras*. Journal of Symbolic Computation, **vol. 43**(8): pp. 515–544, 2008.

[RRM09] G. Regensburger, M. Rosenkranz, and J. Middeke: *A skew polynomial approach to integro-differential operators*. In: J. R. Johnson, H. Park, and E. Kaltofen (eds.), *Proceedings of ISSAC 2009*, pp. 287–294. ACM, 2009. URL http://issac2009.kias.re.kr/.

[RRTB11] M. Rosenkranz, G. Regensburger, L. Tec, and B. Buchberger: *Symbolic analysis for boundary problems: From rewriting to parametrized Gröbner bases*. In: U. Langer and P. Paule (eds.), *Numerical and Symbolic Scientific Computing: Progress and Prospects*, Texts and Monographs in Symbolic Computation. Springer, Wien Heidelberg London New-York, August 2011.

[RW97] P. Rocha and J. C. Willems: *Behavioural controllability of delay-differential systems*. SIAM J. Control Optimiz., pp. 254–264, 1997.

[Sch10] K. Schindelar: *Algorithmic aspects of algebraic system theory*. Ph.D. thesis, RWTH Aachen University, 2010.

[SRA04] H. Sira-Ramirez and S. K. Agrawal: *Differentially Flat Systems*. Marcel Dekker, New York, 2004.

[SST00] M. Saito, B. Sturmfels, and N. Takayama: *Gröbner deformations of hypergeometric differential equations*. Springer-Verlag, Berlin, 2000.

[Sta78] J. T. Stafford: *Module structure of weyl algebras*. Journal of the London Mathematical Society, **vol. 18**(3): pp. 429–442, 1978.

[Tra97] C. Traverso: *Hilbert functions and the Buchberger algorithm*. Journal of Symbolic Computation, (22): pp. 355–376, 1997.

[Ufn98] V. Ufnarovski: *Introduction to noncommutative Gröbner bases theory*. In: B. Buchberger and F. Winkler (eds.), *Gröbner Bases and Applications*, pp. 259–280. Cambridge University Press, 1998.

[Vet02] U. Vetter: *Einführung in die Algebra*. Lecture notes, Carl von Ossietzky Universität Oldenburg, 2002. Available online: ftp://gauss.mathematik.uni-oldenburg.de/pub/Vorlesungen/vetter/ALGLAT.pdf.

[Vil96a] G. Villard: *Computing Popov and Hermite forms of polynomial matrices*. In: T. Asano, Y. Igarashi, H. Nagamochi, S. Miyano, and S. Suri (eds.), *Proceedings of ISSAC'96*, no. 1178 in Lecture Notes in Computer Science, pp. 250–258. Springer, Osaka, December 1996.

[Vil96b] _____ *Some algorithms for matrix polynomials*. Tech. Rep. RT 157, Institut d'Informatique et Mathématiques Appliquées de Grenoble (IMAG), F-38031 Grenoble Cedex, 1996.

[Wae03] B. L. van der Waerden: *Algebra*, vol. Volume I. 9th edn. Springer, Berlin Heidelberg New York, 2003.

[Win96] F. Winkler: *Polynomial algorithms in computer algebra*. Springer, Wien New York, 1996.

[Zer06a] E. Zerz: *An algebraic analysis approach to linear time-varying systems*. IMA Journal of Mathematical Control and Information, **vol. 23**: pp. 113–126, 2006.

[Zer06b] _____ *Algebraic systems theory*, February 2006. Lecture notes, available online: http://www.math.rwth-aachen.de/~Eva.Zerz/ast.pdf.

[Zer07] _____ *State representation of time-varying linear systems*. In: *Gröbner Bases in Control Theory and Signal Processing*, no. 3 in Radon Series on Computational and Applied Mathematics, pp. 235–251, 2007.

[Zer08] _____ *Behavioral systems theory: A survey*. International Journal of Applied Mathematics and Computer Science, **vol. 18**(3): pp. 265–270, 2008.

[ZL06] E. Zerz and V. Levandovskyy: *Algebraic systems theory and computer algebraic methods for some classes of linear control systems*. In: Y. Yamamoto (ed.), *Proceedings of the International Symposium on Mathematical Theory of Networks and Systems (MTNS'06)*, July 2006.