JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Relations between Gröbner bases, differential Gröbner bases, and differential characteristic sets

MASTERARBEIT

zur Erlangung des akademischen Grades

Diplomingenieur

im Masterstudium

Computermathematik

Eingereicht von:

Christian Aistleitner

Angefertigt am:

Institut für Symbolisches Rechnen

Beurteilung:

Univ.-Prof. DI. Dr. Franz Winkler

Linz, Dezember 2010

Cover sheet template taken from [36].

This thesis was typeset using the Emacs [13], Inkscape [26], graphviz [20], xfig [46], and TeX Live [41] software packages on a Gentoo [17] GNU [18] / Linux [29] system.

This work was partially supported by the Austrian Science Foundation (FWF) under the project DIFFOP (P20336-N18) and Doctoral Program "Computational Mathematics" (W1214), project DK11.

Abstract

While Gröbner bases classically focus on purely algebraic settings, Gröbner basis literature followed the general trend of the last decades to also incorporate differential settings, which resulted in the notion of differential Gröbner bases. In the differential setting, there is also the much older, but different notion of differential characteristic sets. Although those three methods of elimination theory are closely related, literature does not provide a comparison of those methods.

The main contribution of this thesis is such a comparison.

Additionally, we give a presentation of Gröbner bases, differential Gröbner bases, and differential characteristic sets using a unified notation system that allows to easily identify and exhibit differences and matches between the different methods.

To the Studien- und Prüfungsabteilung's
(now Prüfungs- und Anerkennungsservice)
support during my studies.

Contents

Notation

If not explicitly listed otherwise, subscripts do not change the semantics of a symbol. For example p_1 shares semantics with p, as p_1 does not occur in this table.

Subscripts do not imply any order. Considering z_1, and z_2, either of $z_1 < z_2$, $z_1 = z_2$, or $z_1 > z_2$, may hold.

Primes do not refer to derivations. For example, p and p' are two completely different symbols. $p' = \delta(p)$ need not hold for any derivation δ.

The general intuition (although there are plenty exceptions) behind the case of symbols is the following: lowercase letters denote simple elements (e.g.: derivatives, differential polynomials), uppercase letters refer to collections of simple elements (e.g.: autoreduced sets, characteristic sets), double-stroke letters are used for collecting collections of simple elements (e.g.: sets of autoreduced sets, sets of characteristic sets).

Double-stroke letters:

$\mathbb{A}$			set of either autoreduced sets or regular systems
$\mathbb{B}$			set of characteristic sets
$\mathbb{C}$			complex numbers
$\mathbb{N}_0$			$\{0, 1, 2, \ldots\}$
$\mathbb{N}^+$			$\{1, 2, \ldots\}$
$\mathbb{Q}$			rational numbers
$\mathbb{R}$			real numbers
$\mathbb{Z}$			integer numbers

Fraktur letters:

$\mathfrak{D}(P)$	5.3	44	set of derivatives occurring in P
$\mathfrak{L}(P)$	5.3	44	set of leaders of the non-constants in P
$\mathfrak{N}(P)$	5.3	44	set of derivatives occurring in P that are not leaders

---

Greek letters:

Δ		23	set of derivations
$\Delta(p, q)$	5.21	50	Δ-polynomial of p and q
δ	2.3	22	derivation (typically an element of Δ)
Θ		23	derivative operators
Θ^+		23	proper derivative operators
θ, θ'			derivative operator
ϕ			derivative operator

Latin letters:

A	5.7	45	autoreduced set
a, a'			elements of A
$\mathrm{apredp}(p,q)$	5.5	44	p is algebraically pseudo-reduced with respect to q
$\mathrm{aredp}\,(p,q)$	4.3	36	p is algebraically reduced with respect to p
$\mathrm{areds}\,(p,P)$	4.3	36	p is algebraically reduced with respect to P
$\mathrm{aredt}\,(p,t,q)$	4.3	36	p is algebraically reduced with respect to t and p
$\mathrm{aremstepp}\,(p,p',q)$	4.4	37	q is the result of a single algebraical remainder step of p with respect to p'
$\mathrm{aremsteps}\,(p,P,q)$	4.4	37	q is the result of a single algebraical remainder step of p with respect to P
$\mathrm{aremstept}\,(p,t,p',q)$	4.4	37	q is the result of a single algebraical remainder step of p with respect to t and p'
$\mathrm{aremsws}\,(p,P,q)$	4.5	37	q is an algebraic stepwise remainder of p with respect to P
C	5.9	45	autoreduced set (typically a characteristic set)
$\mathrm{ComMonoid}\,(X)$		21	commutative monoid generated by X
c			constant, or coefficient
$\mathrm{coeff}_{\mathrm{I}}(p,z,d)$		17	coefficient of p (as univariate polynomial in z) with respect to z^d
$\mathrm{coeff}_{\mathrm{T}}(p,t)$		17	coefficient of p with respect to t via evaluation of p (as function from indeterminates to ground field) at t
d			element of $\mathbb{N}_0 \cup \{-\infty\}$ to denote the degree of some polynomial in an indeterminate
$\deg_z(p)$		17	degree of the polynomial p in the indeterminate z
$\mathrm{dpredas}(p,P)$	5.8	45	p is differentially pseudo-reduced with respect to A
$\mathrm{dpredp}(p,q)$	5.6	44	p is differentially pseudo-reduced with respect to q
$\mathrm{dpreds}(p,P)$	5.8	45	p is differentially pseudo-reduced with respect to P
$\mathrm{dpremas}(p,A,q)$	5.14	48	q is a differential pseudo-remainder of p with respect to A
$\mathrm{dpremras}(p,A,q)$	5.13	48	q is a respectful differential pseudo-remainder of p with respect to A
$\mathrm{dpremMstepd}\,(p,p',\theta',q)$	6.12	62	q is the result of a single differential pseudo-remainder Mansfield step of p with respect to θ', and p'
$\mathrm{dpremMstepp}\,(p,p',q)$	6.12	62	q is the result of a single differential pseudo-remainder Mansfield step of p with respect to p'
$\mathrm{dpremMsteps}\,(p,P,q)$	6.12	62	q is the result of a single differential pseudo-remainder Mansfield step of p with respect to P

dpremMsws (p, P, q)	6.13	63	q is differential stepwise pseudo-remainder of p with respect to Mansfield steps and P
dredp (p, q)	6.3	57	p is differentially reduced with respect to q
dreds (p, P)	6.3	57	p is differentially reduced with respect to P
dremdis (p, P, q)	6.4	57	q is a differential remainder of p with respect to the differential ideal generated by P
dremsws (p, P, q)	6.5	58	q is a differential stepwise remainder of p with respect to P
F		21	field having characteristic zero
$F[X]$			polynomial ring over F in the indeterminates X
$F\{Y\}$		23	differential polynomial ring over F in the differential indeterminates Y and the derivations Δ
g, g'			element of G, or G'
G, G'			set of polynomials that are a Gröbner basis (in Appendix A the set to generate the ideal for the congruence equation)
gcd (p, q)			greatest common divisor of p and q
H_P	5.12	47	set of initials and separants of P
H_P^∞			smallest multiplicatively closed set containing 1 and the initials and separants of P. To be read as $(H_P)^\infty$. Compare H_P and H^∞.
H^∞	2.13	24	smallest multiplicatively closed set containing 1 and the elements of H
$H^{o\,o}$		26	set of factors of H^∞
h			element of H or H'
I		23	index set for Y
I_P	5.12	47	set of initials of P
i, i'			element of I
init(p)	5.11	47	initial of p
J			ideal
j			element of J
k			index (typically ranging over a subset of $\mathbb{N}_0$)
lc (p)	4.2	36	leading coefficient of p
$\mathrm{lcd}_D\big(y_{i,\theta}, y_{i,\theta'}\big)$	5.19	50	least common derivative of $y_{i,\theta}$ and $y_{i,\theta'}$
$\mathrm{lcd}_P(p, q)$	5.20	50	least common derivative of p and q
lcm (t, s)			least common multiple of t and s
lead(p)	5.2	43	highest ranking indeterminate occurring in p
ltp (p)	4.2	36	leading term of p
lts (P)	4.2	36	set of leading terms in P
M			set of polynomials, whose separants and initials are used for premultiplication when pseudo-reducing
m		23	number of elements in Δ
n		23	number of elements in I, respectively Y
ord(θ)	B.1	79	total order of the derivative operator θ
$\mathrm{ord}_\delta(\theta)$	B.1	79	order of the derivative operator θ with respect to the derivation δ
p, p'			polynomial

pdpredas(p, A)	5.8	45	p is partially differentially pseudo-reduced with respect to A
pdpredp(p, q)	5.4	44	p is partially differentially pseudo-reduced with respect to q
pdpreds(p, P)	5.8	45	p is partially differentially pseudo-reduced with respect to P
pseudoS (p, q)	5.18	50	pseudo-S-polynomial of p and q
q			polynomial
R		17	ring
$\mathrm{Res}_z(p, q)$		28	resultant of p and q with respect to z
r, r'			element of R
S_P	5.12	47	set of separants of P
$\mathrm{S}\,(p, q)$	4.6	38	S-polynomial of p and q
s			term
sep(p)	5.11	47	separant of p
T	4.2	36	set of terms
Terms (p)	4.2	36	set of terms occurring in p
t			term
u			term
X		21	set of indeterminates
Y		23	family $(y_i)_{i\in I}$
y_i			either an element of Y or a short-hand notation for $y_{i,1}$
$y_{i,\theta}$			derivative
Z			subset of $(y_{i,\theta})_{i\in I,\theta\in\Theta}$
z, z'			indeterminate (typically an element of X, or $(y_{i,\theta})_{i\in I,\theta\in\Theta}$)

Lines along symbols:

$\overline{P}^{\Theta}$	2.6	23	differential closure of P
$\overline{P}^{\Theta,<z}$	5.22	51	$\overline{P}^{\Theta}$ with derivatives bounded by z
$\lvert P\rvert$			number of elements in P

Punctuation:

$J : H^{\infty}$	2.14	25	saturation of J by H

Parentheses:

$R\,(X)$			algebraic extension of the ring R by the elements of X
$\langle P\rangle$		21	algebraic ideal generated by P in $F\{Y\}$
$\langle P\rangle_R$		21	algebraic ideal generated by P in R

$\langle\!\langle P \rangle\!\rangle$		21	radical algebraic ideal generated by P in $F\{Y\}$
$\langle\!\langle P \rangle\!\rangle_R$		21	radical algebraic ideal generated by P in R
$[P]$	2.8	23	differential ideal generated by P in $F\{Y\}$
$R[X]$			algebraic polynomial ring over R in X
$[\![P]\!]$	2.10	24	radical differential generated by P in $F\{Y\}$
$F\{Y\}$		23	differential polynomial ring over F with differential indeterminates Y and the derivations Δ
$\lvert P \rvert$			number of elements in P

Conventions

Besides the conventions for symbols listed on page 11, we use the following conventions on basic mathematics, and layout.

- We use "ring" to refer to a commutative ring with identity.
- For polynomial rings we use "term" to denote a finite product of the polynomial ring's indeterminates (an indeterminate may occur more than once in such a product). We use "monomial" for the product of a term with an element of the ground field.
- We consider the result of empty operations as the neutral element with respect to this operation in the structure of interest. So for example,

$$\sum_{k=3}^{2} r = 0 \qquad \prod_{k=3}^{2} r = 1 \qquad \bigcap_{h\in\emptyset} hp = F\{Y\}, \tag{1}$$

  for some $r \in \mathbb{Z}$, and $p \in F\{Y\}$.

- We use $\deg_z(p)$ to denote the degree of p in z, where p is a not necessary univariate polynomial and z a indeterminate of p's polynomial ring. We set the degree of 0 to $-\infty$, and $\forall k \in \mathbb{N}_0 : -\infty < k$. For example, considering $0, 3$, and $y_3^4 y_1^2 + 4$ in $\mathbb{Q}[y_1, y_2, y_3]$, then

$$\deg_{y_1}\left(y_3^4 y_1^2 + 4\right) = 2 \qquad \deg_{y_2}\left(y_3^4 y_1^2 + 4\right) = 0 \tag{2}$$
$$\deg_{y_1}(3) = 0 \qquad \deg_{y_1}(0) = -\infty. \tag{3}$$

- In this thesis, we are in the unfortunate situation to combine two different branches of literature each using a different concept of coefficients. Hence, we introduce them both. The first variant ($\mathrm{coeff_T}$) interprets polynomials as functions from the terms to the ground field and evaluates such a function at a term. For example in $\mathbb{Q}[y_1, y_2, y_3]$ with $p := 2 + 11y_1^2 + y_2 + 3y_1^2 y_2 y_3 + 7y_1^2 y_3$, we obtain

$$\mathrm{coeff_T}\left(p, y_1^2 y_3\right) := 7 \qquad \mathrm{coeff_T}\left(p, y_1^2\right) := 11 \tag{4}$$
$$\mathrm{coeff_T}(p, y_3) := 0 \qquad \mathrm{coeff_T}(p, 1) := 2. \tag{5}$$

  $\mathrm{coeff_T}$ computes the coefficient with respect to a (possibly multivariate) term.

  The second variant ($\mathrm{coeff_I}$) reinterprets a polynomial ring $F[X]$ as univariate polynomial ring for a given indeterminate z (i.e.: $F[X \setminus \{z\}][z]$) and computes the coefficient of z^d in this domain, for a given degree d. Reconsidering the previous example we obtain

$$\mathrm{coeff_I}(p, y_1, 2) := 11 + 3y_2 y_3 + 7y_3 \tag{6}$$
$$\mathrm{coeff_I}(p, y_3, 1) := 3y_1^2 y_2 + 7y_1^2 \qquad \mathrm{coeff_I}(p, y_1, 0) := 2 + y_2. \tag{7}$$

  $\mathrm{coeff_I}$ computes the coefficient with respect to an indeterminate and a corresponding degree.

- We did not only attach numbers to formulas, which we reference, but we attached numbers to any formula, when space allowed it. Thereby, we make it easier to reference equations in discussions about this thesis.
- For most definitions, and theorems we provide references to literature (the "compare" part). The term "compare" in those references really means "compare" and does not automatically imply, we took the result unmodified from there. Instead, the given references are in the spirit of our definitions, and theorems.

1 Introduction

In this thesis, we relate three important concepts of computer algebra: Gröbner bases, differential Gröbner bases, and differential characteristic sets. All three concepts are part of elimination theory and allow to simplify systems of equations. These simplifications may for example lower the degree of certain indeterminates or decouple equations. Such simplifications typically aid when trying to solve a system of equations.

As of writing this thesis, Gröbner basis is not only the most prominent among the three concepts, but also undoubtedly constitutes an integral part of computer algebra, as for example the Gröbner basis bibliography [7] documents over 1000 scientific articles, books, etc. on the topic of Gröbner bases.

While Gröbner basis are typically applied to systems of equations in algebraic polynomial rings, Gröbner basis literature provides generalizations in various directions ranging for example from non-commutative settings (e.g.: [33]) to differential polynomial rings (e.g.: [8]).

As current research in computer algebra seems to progress towards treating not only algebraic equations (as in typical Gröbner basis settings), but also differential equations, especially the abstractions of Gröbner bases towards differential polynomial rings may be expected to gain relevance. While some researchers work in this direction (e.g.: Aleksey Zobnin), it seems that the theory of differential characteristic sets (which is a concept predating Gröbner bases, operating in differential polynomial rings, having similar applications as Gröbner bases) gained more momentum over the last two decades. Nevertheless, we do not know of any research trying to explicitly relating those three methods: Gröbner bases, differential Gröbner bases, and differential characteristic sets. In this thesis we give such a comparison.

In Section 2, we present the basic setting of this thesis and introduce notation for algebraic and differential polynomial rings. Using this notation, we motivate the use and importance of Gröbner bases in Section 3, where we show how elimination theory may help to solve systems of algebraic equations using resultants, Gröbner bases, and characteristic sets.

After those precursory parts, we present Gröbner bases in Section 4, followed by differential characteristic sets in Section 5. Finally, we introduce differential Gröbner bases in Section 6. Section 7 compares Gröbner bases, differential Gröbner bases, and differential characteristic sets.

While the individual sections are meant to be read sequentially, readers already familiar with Gröbner bases, differential Gröbner bases, and differential characteristic sets may skip directly to Section 7—the used notation is given in tabular form on page 11.

2 Setting

In this section, we present the mathematical setting of this thesis. While we present the notations ordered by their semantics, a condensed presentation of the used notation ordered by the symbols can be found on page 11 in tabular form.

We begin by presenting the algebraic notions, followed by the notions for differential aspects of polynomial rings. The third and last part of this section discusses saturation ideals.

2.1 Algebraic notions

Throughout this thesis, let F refer to a field having characteristic zero. F typically acts as coefficient domain for the used polynomial rings.

For any set P, we use $\mathrm{ComMonoid}\,(P)$ to denote the commutative monoid generated by P[1]. We use 1 as neutral element of this monoid.

By $R\,[X]$ we refer to the polynomial ring over R in X, where R is a ring, and X is a (not necessarily finite) set that is algebraically independent over R.

From now on, let X be an algebraically independent set over F. X may be finite, but it need not be finite.

To denote the ideal generated in a ring R by a set $P \subseteq R$[2], we use $\langle P\rangle_R$. If $R = F\{Y\}$[3], we may omit the subscript and denote $\langle P\rangle_R$ by $\langle P\rangle$.

For the radical ideal generated in a ring R by a set $P \subseteq R$, we use $\langle\!\langle P\rangle\!\rangle_R$ [4]. If $R = F\{Y\}$, we may again omit the subscript and denote $\langle\!\langle P\rangle\!\rangle_R$ by $\langle\!\langle P\rangle\!\rangle$.

The two main theorems for algebraic polynomial rings used in this thesis are Hilbert's basis theorem (Theorem 2.1) and Hilbert's Nullstellensatz (Theorem 2.2). While Hilbert's

[1] We later also introduce P^∞ for the commutative monoid generated by P. While both $\mathrm{ComMonoid}\,(P)$, and P^∞ result in the same mathematical object, there is a slight but crucial semantic difference between them, as we argue in Section 2.3.

[2] Although the observation also holds for the rest of this thesis, we want to emphasize here that by "$\subseteq$" we mean any subset. Hence, P can be empty, finite, infinite and even the whole ring R itself.

[3] Although, we define $F\{Y\}$ only later in Section 2.2, we already present $\langle P\rangle$ already here, to have the notions for algebraic ideals in one place.

[4] The approach to denote generated radical ideals by doubling the ideal generating brackets with almost no space in between comes from [22] for differential radical ideals as approach to avoid the classical notation $\{P\}$, which leads to confusion between the set containing P and the radical differential ideal generated by P.

The alternative would be to use the $\sqrt{\ }$ sign, which however distorts the rendered text when encountered in running text ("$\sqrt{[P]}$").

Hence, we adopted the approach of doubling the brackets and reducing the space between them and thereby obtain a nicer looking representation in running text—while still not introducing ambiguity, as $\langle\langle P\rangle\rangle$ (the ideal generated by the elements of the ideal generated by P; we never use this construct in this thesis, as the outer layer of angle brackets are redundant) differs from $\langle\!\langle P\rangle\!\rangle$ (the radical ideal generated by P) by its spacing and $\langle\langle P\rangle_R\rangle_R$ additionally differs from $\langle\!\langle P\rangle\!\rangle_R$ in the subscript R between the two closing brackets.

basis theorem asserts finite bases for ideals in polynomial rings in finitely many indeterminates, Hilbert's Nullstellensatz bridges between radical ideals and solutions of systems of equations.

Theorem 2.1 (Hilbert's basis theorem)**.** *[compare 45, Theorem 8.2.2, page 180] If X is finite, then every ideal in $F[X]$ has a finite basis.*

Theorem 2.2 (Hilbert's Nullstellensatz)**.** *[compare 45, Theorem 8.4.2, page 190] Let F be an algebraically closed field and J be an ideal in the polynomial ring $F[X]$ such that $J \neq F[X]$. Then the radical of J contains exactly those polynomials vanishing on all the common roots of J.*

After this presentation of the basic notions that we use in purely algebraic polynomial rings, we introduce the required notions of differential polynomial rings.

2.2 Differential notions

In this part we introduce differential polynomial rings along with ideals in them and finally establish a basis theorem and a Nullstellensatz.

To define a *differential* polynomial ring it is essential to model the differential structure. Therefore, we start by a definition of derivation followed by a restriction to commutative derivations, before actually defining differential polynomial rings in Definition 2.5.

Definition 2.3 (Derivation)**.** *[compare 28, I, 1, page 58] Let R be a ring. A function $\delta : R \to R$ is called a* derivation *on R if and only if*

$$\forall r, r' \in R : \delta(r + r') = \delta(r) + \delta(r') \tag{8}$$

and

$$\forall r, r' \in R : \delta(rr') = \delta(r)\, r' + r\, \delta(r')\,. \tag{9}$$

Definition 2.4 (Commuting derivations)**.** *Let R be a ring and Δ a set of derivations on R. We refer to the derivations as being* commutative *if and only if*

$$\forall\, \delta_1, \delta_2 \in \Delta\ \forall r \in R\ :\ \delta_1(\delta_2(r)) = \delta_2(\delta_1(r))\,. \tag{10}$$

While there exists elimination theory literature considering non-commuting derivations (e.g.: [24]), elimination theory literature typically only deals with commuting derivations. Hence, we also restrict ourselves to commuting derivations in this thesis.

Whenever, we use a set of derivations on some ring, we silently assume that those derivations commute for the given ring.

Definition 2.5 (Differential polynomial ring)**.** *[compare 28, I, 6, page 70] Let I be a finite set, $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ be algebraically independent over the field F of characteristic zero, and let Δ be a finite set of commuting derivations on $F\left[(y_{i,\theta})_{i\in I,\theta\in\Theta}\right]$, using Θ as abbreviation for* ComMonoid$\,(\Delta)$ *. We call $F\left[(y_{i,\theta})_{i\in I,\theta\in\Theta}\right]$ together with Δ the* differential polynomial ring *over F in $(y_i)_{i\in I}$ and Δ, if and only if*

$$\forall \delta \in \Delta : \delta|_F \text{ is a derivation on } F, \tag{11}$$

and additionally

$$\forall \delta \in \Delta \, \forall i \in I \, \forall \theta \in \Theta : \delta(y_{i,\theta}) = y_{i,\delta\theta}. \tag{12}$$

For the rest of this thesis, let I denote a finite set, such that $(y_{i,\theta})_{i \in I, \theta \in \Theta}$ is algebraically independent over F. We use n to refer to $|I|$, and Y as abbreviation for $(y_i)_{i \in I}$.

Furthermore, let Δ be a finite set of commuting derivations on $F\left[(y_{i,\theta})_{i \in I, \theta \in \Theta}\right]$, such that (11), and (12) hold. We use m to refer to $|\Delta|$, Θ as abbreviation for $\mathrm{ComMonoid}(\Delta)$, and Θ^+ to denote $\Theta \backslash \{1\}$. Finally, we denote the differential polynomial ring over F in Y and Δ by $F\{Y\}$.

From its definition, we see that $F\{Y\}$ can be interpreted as polynomial ring $F[X]$ when ignoring the differential structure of $F\{Y\}$, and choosing $X = (y_{i,\theta})_{i \in I, \theta \in \Theta}$. Typically, such an X is infinite. Nevertheless, this correspondence allows to carry notions we later develop for purely algebraic polynomial rings (e.g.: the Terms operator of Definition 4.2) to differential polynomial rings. Wherever necessary, we silently take advantage of this correspondence.

On the same note, we may use notions defined solely on $F\{Y\}$ also on $F[X]$ with finite X, as for $\Delta = \emptyset$, $F\{Y\}$ can be identified with $F[X]$.

The elements of (algebraic) ideals in differential polynomial rings are closed under addition and multiplications. However, they are not necessarily closed under derivations. We call ideals having this additional closure property *differential* ideals.

Definition 2.6 (Differential closure)**.** *Let $P \subseteq F\{Y\}$. We refer to the set*

$$\{p \in F\{Y\} \mid \exists q \in P \wedge \exists \theta \in \Theta : p = \theta(q)\} \tag{13}$$

by the differential closure *of P (or $\overline{P}^{\Theta}$[5]).*

Definition 2.7 (Differential ideal)**.** *An ideal J in $F\{Y\}$ is called* differential ideal *if and only if*

$$J = \overline{J}^{\Theta}. \tag{14}$$

Similarly, to how we generate (algebraic) ideals from a set, we can generate differential ideals from a set.

Definition 2.8 (Generated differential ideals)**.** *Let P be a subset of $F\{Y\}$. By $[P]$, we denote the smallest subset of $F\{Y\}$ containing P while being closed under applying derivations, multiplication by elements of $F\{Y\}$, and addition.*

Accordingly, radical differential ideals are differential ideals that are radical.

[5]While the notation $\overline{P}^{\Theta}$ may seem cumbersome when viewed on its own, it is part of a more expressive, clear notation approach allowing differential closure along selection of only some elements [1, § 11.4, Definition 11.5, page 202]. From this general notation approach, we only introduce the those two parts that are relevant in this thesis ($\overline{P}^{\Theta}$ from Definition 2.6, and $\overline{A}^{\Theta,<z}$ as used in Definition 5.22).

Definition 2.9 (Radical differential ideal). *A differential ideal J in $F\{Y\}$ is called* radical differential ideal *if and only if J is a radical ideal (i.e.:*

$$\forall j \in F\{Y\}\ \forall k \in \mathbb{N}^+ : \left(\left(j^k \in J\right) \implies j \in J\right)\right). \tag{15}$$

Definition 2.10 (Generated, radical differential ideals). *Let P be a subset of $F\{Y\}$. By $[\![P]\!]$, we denote the smallest subset of $F\{Y\}$ containing P while being closed under taking roots (i.e.:* (15) *holds), applying derivations, multiplication by elements of $F\{Y\}$, and addition.*

Before closing the introduction to basic notions around differential polynomial rings, we establish a basis theorem and a Nullstellensatz, just as we did in Section 2.1. While the differential Nullstellensatz directly corresponds to the Hilbert's Nullstellensatz (Theorem 2.2), there is no differential equivalent of Hilbert's basis theorem (Theorem 2.1). Finite bases need not exist for arbitrary differential ideals. However, they exist for *radical* differential ideals, as stated by the Ritt Raudenbush basis theorem.

Theorem 2.11 (Ritt Raudenbush basis theorem). *[compare 27, VII, § 27, Theorem 7.1, page 45]*[6] *For every* radical *ideal in $F\{Y\}$, there is a* finite $P \subseteq F\{Y\}$, *such that* $J = [\![P]\!]$.

Theorem 2.12 (Differential Nullstellensatz). *[compare 22, Theorem 2.7, page 8] Let F be an algebraically closed differential field and J be a differential ideal in $F\{Y\}$ such that $J \neq F\{Y\}$. Then the radical of J contains exactly those polynomials vanishing on all the common roots of J.*

The final part of Section 2 presents saturation ideals, which form an essential ingredient of differential characteristic set computations (Section 5).

2.3 Saturation ideals

In characteristic set literature, ideals are often encountered as saturation ideals, which are denoted by an ideal followed by a colon (":") and another expression. In this section, we present the notion of saturation ideals, relate it to quotients and additionally present an abstraction used in some modern differential characteristic set literature.

Before defining saturation ideals, we define a second variant of the commutative monoid generated by a set.

Definition 2.13 (Multiplicatively closed set with 1). *Let H be a subset of $F\{Y\}$. By H^∞ we denote the smallest multiplicatively closed subset of $F\{Y\}$ such that $1 \in H^\infty$ and $H \subseteq H^\infty$.*

[6] While it might appear close to heresy to not give an reference to Raudenbush or probably the most influential use through [38, IX, § 7, last sentence on page 165] for the Ritt Raudenbush basis theorem, we are nevertheless convinced that the elaboration of [27, VII, § 27, Theorem 7.1, page 45] is very practical and also favor the immediate relation to the important decomposition theorem in [27, VII, § 29, page 48].

We previously introduced ComMonoid on page 21 to construct the commutative monoid generated by a set, and we see that $H^\infty = \text{ComMonoid}(H)$ for any $H \subseteq F\{Y\}$. However, the use and semantics of $\text{ComMonoid}(H)$ and H^∞ are different. While we use $\text{ComMonoid}(H)$ to construct general products of elements of H, H^∞ carries the additional semantic of being used to saturate ideals.

It is tempting to merge those two different notations and ignore the semantic difference. However, in differential characteristic set literature (the main application of saturated ideals in our thesis) some advances towards extending H^∞ can be found, as we show later on page 26. Those generalizations only make sense when saturating ideals, and do not translate to the settings where we use $\text{ComMonoid}(H)$. Hence, the semantic difference between $\text{ComMonoid}(H)$ and H^∞ is crucial, when relating our notation to differential characteristic set literature, and we therefore separate between $\text{ComMonoid}(H)$ and H^∞ based on the required semantic.

With the help of Definition 2.13, we can now define saturation ideals.

Definition 2.14 (Saturation ideals)**.** *[compare 22, § 2.1, paragraph before Proposition 2.2, page 6] Let J be an ideal in $F\{Y\}$ and H be a subset of $F\{Y\}$. By the* saturation *of J by H (or $J : H^\infty$), we refer to*

$$J : H^\infty := \{p \in F\{Y\} \mid \exists h \in H^\infty : hp \in J\}. \tag{16}$$

It is important to notice that the two $^\infty$ within (16) are not related. The $^\infty$ on the left hand side of (16) is part of the colon notation—(16) defines the saturation of J by H, not the saturation of J by H^∞. The $^\infty$ on the right hand side of (16) refers to Definition 2.13. This two different uses of $^\infty$ are certainly bewildering. However, this dual use is ubiquitous in modern differential characteristic set literature (e.g.: [19, § 2, last but one paragraph, page 585]) and we therefore adopted it. Besides, this distinction is crucial to not misinterpret $J : H^\infty$ as $J : (H^\infty)$[7], which is the quotient of J with respect to H^∞, and is defined as

$$J : (H^\infty) := \{p \in F\{Y\} \mid \forall h \in H^\infty : hp \in J\} \tag{17}$$

for example in [28, Chapter 0, last paragraph of § 1, page 2][8]. In (17), both $^\infty$ refer to Definition 2.13.

The difference between (16), and (17) is the quantifier within the set. Although, there is a strong connection between (16), and (17)[9], we nevertheless do not go into details to avoid unnecessary, further notational confusion.

The quotient interpretation (17) is only used in above separation between (16), and (17). Everywhere else in this thesis, only the saturation interpretation (16) is used.

A crucial observation for saturation ideals is that they actually are ideals.

[7]The additional parenthesis around H^∞ are only used to disambiguate and not necessary for the quotient of J with respect to H^∞.

[8]Analogous, modern definitions can be found if H^∞ were an ideal, as for example in [45, Definition 8.4.2, page 199], or [12, 4, § 4, Definition 5, page 194].

[9]For example, (16) has classically been formulated via unions of quotients. Also some results for saturations carry over to quotient settings. For example, Theorem 2.15 for purely algebraic ideals also holds for the quotient interpretation. However, for differential ideals the quotient interpretation does not allow to formulate such a result.

Theorem 2.15 (Saturated differential ideal is differential ideal). *[compare 28, I, 3, page 62] Let J be a (differential) ideal in $F\{Y\}$ and $H \subseteq F\{Y\}$. Then $J : H^\infty$ is again a (differential) ideal.*

Some pieces of differential characteristic set literature work towards generalizing Definition 2.13 by adding closure under factorization[10]—sometimes using the $^\infty$ notation (e.g.: [24, § 5.3, last but one paragraph of page 181]), sometimes using new notation (e.g.: [31, § 2.5, Definition 2, page 38]). Since this factorization chops individual polynomials into smaller parts, we suggest using a notation that reflects this chopping up. For example by using $H^{o\,o}$, where the $^\infty$ is chopped into $^{o\,o}$. Then we may incorporate factorization by

$$H^{o\,o} := \{p \in F\{Y\} \mid \exists q \in F\{Y\} : pq \in H^\infty\}\,, \tag{18}$$

and accordingly introduce factored saturation of J by H via

$$J : H^{o\,o} := \{p \in F\{Y\} \mid \exists h \in H^{o\,o} : hp \in J\}\,. \tag{19}$$

However, it turns out that (19) on its own is futile, as $J : H^\infty = J : H^{o\,o}$. Nevertheless, (18) proves useful, as it allows to specify more general congruence equations for pseudo-reductions. For example from $\operatorname{dpremMsws}(p, P, q)$ (see Definition 6.13), we obtain the congruence relation[11]

$$\exists h \in H_P^{o\,o} : \;\; hp \equiv q \pmod{[P]}\,, \tag{20}$$

while

$$\exists h \in H_P^{\infty} : \;\; hp \equiv q \pmod{[P]}\,, \tag{21}$$

would not hold. Hence, $^{o\,o}$ provides an important step towards generalizing pseudo-reduction even further than [1] did. Such a further generalization is however beyond the scope of this thesis and left to further research.

Having discussed the basic notions of polynomials and ideals, we continue by relating different elimination methods in the purely algebraic setting in Section 3, followed by a more detailed presentation of the relevant algebraic and differential approaches to elimination in Sections 4–6.

[10] A collection of the different formulations of generalizing $^\infty$ can be found in [1, § 4.3, Footnote 33, page 72].

[11] H_P denotes the set of separants and initials, which we define in Definition 5.12.

3 Simplifying systems of algebraic equations using elimination theory

In elimination theory, there are three main approaches to simplifying (and thereby aiding to solve) algebraic equations: resultants, Gröbner basis computations, and characteristic set methods.

In this section, we bring these three approaches in context and briefly exhibit their peculiarities with the help of two simple exemplary systems of algebraic equations. Afterwards, we relate our observations to the title of this thesis, where only Gröbner basis but neither resultants nor characteristic sets (for the algebraic setting) are mentioned.

There, we identify that Gröbner basis is the relevant core concept for our treatment, and hence only Gröbner bases receive a formal presentation (see Section 4) in addition to the intuitive presentation of the methods given in this section. A formal introduction of resultants, and algebraic characteristic sets is left to literature (e.g.: [16] for resultants, and [21], [23], and [42] for algebraic characteristic sets). Nevertheless we want to point out that a formal presentation of characteristic sets can also be obtained by restricting our presentation of differential characteristic sets in Section 5 to $\Delta = \emptyset$.

We now present the two exemplary systems of equations, which are then treated using resultants (Section 3.1), Gröbner bases computations (Section 3.2), and characteristic set methods (Section 3.3).

The first problem we consider is to find solutions of

$$p_1 = 0 \qquad\qquad p_2 = 0, \tag{22}$$

in $\mathbb{C}[y_1, y_2]$, using

$$p_1 := y_1^2 + 2y_1y_2 - 6y_1 + y_2^2 - 6y_2 + 9 \tag{23}$$
$$p_2 := y_1^2 + 2y_1y_2 - 6y_1 + 2y_2^2 - 9y_2 + 11. \tag{24}$$

The second problem is to find solutions to

$$q_1 = 0 \qquad\qquad q_2 = 0 \qquad\qquad q_3 = 0, \tag{25}$$

in $\mathbb{C}[y_1, y_2, y_3]$, using

$$q_1 := y_1y_2y_3 + y_1y_2 - y_2 + 1 \tag{26}$$
$$q_2 := -y_1y_2^2 + y_1y_2 + y_2^2 + y_2y_3^2 - y_2 + y_3 \tag{27}$$
$$q_3 := -y_1y_2^2 - y_1y_2y_3 + y_2^2 + y_2y_3^2 + y_2y_3 + y_3. \tag{28}$$

Using resultants, Gröbner basis computations and characteristic set methods, we now solve each of those problems and finally collect the relevant differences.

3.1 Resultants

A resultant[12] of two univariate polynomials is an element of the coefficient ring, equating to zero if and only if the original two polynomials have a common zero. For multivariate polynomials, the resultant effectively allows to eliminate indeterminates when trying to solve a system of equations.

Considering (22), we see that we cannot compute the resultant directly, as p_1 and p_2 are not univariate polynomials. Formally translating the polynomials from $\mathbb{C}[y_1, y_2]$ to $\mathbb{C}[y_1][y_2]$, we can compute the resultant of p_1 and p_2 (with respect to y_2)[13]

$$\mathrm{Res}_{y_2}(p_1, p_2) := y_1^4 - 6y_1^3 + 13y_1^2 - 12y_1 + 4 = (y_1 - 1)^2 (y_1 - 2)^2 . \tag{29}$$

Hence, p_1 and p_2 have a common zero if and only if (29) equates to 0. For this to happen, either $y_1 = 1$, or $y_1 = 2$ has to hold.

Computing the resultant of p_1 and p_2 with respect to y_1 we obtain

$$\mathrm{Res}_{y_1}(p_1, p_2) := y_2^4 - 6y_2^3 + 13y_2^2 - 12y_2 + 4 = (y_2 - 1)^2 (y_2 - 2)^2 . \tag{30}$$

Again, p_1 and p_2 have a common zero if and only if (30) equates to 0. For this to happen, either $y_2 = 1$, or $y_2 = 2$ has to hold.

Plugging the four possible choices for (y_1, y_2) into (22), we obtain the solution set

$$\{(1, 2), (2, 1)\} . \tag{31}$$

We now switch to the second problem described in the beginning of this section, and try to find solutions to (22).

Eliminating y_2 from q_1, and q_2, and also from q_1, and q_3, we arrive at

$$\mathrm{Res}_{y_2}(q_1, q_2) := y_1^2y_3^3 + 2y_1^2y_3^2 - y_1^2 - y_1y_3^3 - 3y_1y_3^2 - y_1y_3 + y_1 + y_3^2 + y_3 \tag{32}$$

$$\mathrm{Res}_{y_2}(q_1, q_3) := y_1^2y_3^3 + 3y_1^2y_3^2 + 2y_1^2y_3 - y_1y_3^3 - 4y_1y_3^2 - 4y_1y_3 - y_1 + y_3^2 + 2y_3 + 1. \tag{33}$$

Hence, for a common zero of the polynomials in (25), also both (32), and (33) have to equate to 0. Rewriting these considerations, we arrive at the system

$$\mathrm{Res}_{y_2}(q_1, q_2) = 0 \qquad \mathrm{Res}_{y_2}(q_1, q_3) = 0 \tag{34}$$

and look for solutions to this system in $\mathbb{C}[y_1, y_3]$. Hence, we compute the resultant of (32), and (33) with respect to y_1. However, we obtain

$$\mathrm{Res}_{y_1}(\mathrm{Res}_{y_2}(q_1, q_2), \mathrm{Res}_{y_2}(q_1, q_3)) = 0, \tag{35}$$

[12]Throughout this thesis, we use the term resultant to refer to the determinant of the Sylvester matrix of two univariate polynomials univariate polynomials. Other and more general notions of resultants are presented for example in [16].

[13]This translation of a multivariate polynomial into a univariate polynomial ring and moving the result back to the multivariate polynomial ring is cumbersome and only formal. Hence, we adopt the convention of denoting the relevant indeterminate besides the symbol Res and tacitly perform the required translation between the multivariate and the appropriate univariate polynomial rings.

as $\mathrm{Res}_{y_2}(q_1, q_2)$ and $\mathrm{Res}_{y_2}(q_1, q_3)$ are not relatively prime,

$$\gcd\left(\mathrm{Res}_{y_2}(q_1, q_2), \mathrm{Res}_{y_2}(q_1, q_3)\right) = (y_1 - 1)(y_3 + 1). \tag{36}$$

As furthermore

$$\mathrm{Res}_{y_1}\left(\frac{\mathrm{Res}_{y_2}(q_1, q_2)}{\gcd\left(\mathrm{Res}_{y_2}(q_1, q_2), \mathrm{Res}_{y_2}(q_1, q_3)\right)}, \frac{\mathrm{Res}_{y_2}(q_1, q_3)}{\gcd\left(\mathrm{Res}_{y_2}(q_1, q_2), \mathrm{Res}_{y_2}(q_1, q_3)\right)}\right) = 1, \tag{37}$$

we see that either $y_1 = 1$, or $y_3 = -1$ has to hold, for solutions of (25).

Assuming $y_1 = 1$, (25) simplifies to

$$y_2 y_3 + 1 = 0 \tag{38}$$
$$y_2 y_3^2 + y_3 = 0 \tag{39}$$
$$y_2 y_3^2 + y_3 = 0. \tag{40}$$

If $y_2 = 0$ held, (38) would not hold. However, any non-zero y_2 forces $y_3 = -\frac{1}{y_2}$, which is a solution to (25).

Assuming $y_3 = -1$, (25) simplifies to

$$-y_2 + 1 = 0 \tag{41}$$
$$-y_1 y_2^2 + y_1 y_2 + y_2^2 - 1 = 0 \tag{42}$$
$$-y_1 y_2^2 + y_1 y_2 + y_2^2 - 1 = 0 \tag{43}$$

From (41), we see $y_2 = 1$. For arbitrary y_1, this choice solves (25).

Combining those two branches, we arrive at

$$\left\{(1, c_2, c_3) \in \mathbb{C}^3 \;\middle|\; c_2 \neq 0 \wedge c_3 = -\frac{1}{c_2}\right\} \cup \left\{(c_1, 1, -1) \in \mathbb{C}^3\right\} \tag{44}$$

as solution set for (25).

In Section 3.2, we continue to exhibit elimination methods by again trying find the solution sets of the above two examples, but this time using Gröbner bases techniques instead of resultants.

3.2 Gröbner bases

A Gröbner basis is a special kind of basis of an ideal. Once a Gröbner basis has been computed with respect to an admissible order (Definition 4.1) on the polynomial ring's indeterminates, membership can be decided algebraically. For certain orders (Theorem 4.11), Gröbner bases carry a triangular shape, easing equation solving.

Trying to solve (22) using Gröbner basis computations, the first step is to choose an admissible order on the terms of $\mathbb{C}[y_1, y_2]$. For this order, a Gröbner basis for $\langle\{p_1, p_2\}\rangle_{\mathbb{C}[y_1,y_2]}$ is computed. Using

$$g_1 := y_2^2 - 3y_2 + 2 = (y_2 - 1)(y_2 - 2), \tag{45}$$
$$g_2 := y_1^2 + 2y_1 y_2 - 6y_1 - 3y_2 + 7, \tag{46}$$

$G := \{g_1, g_2\}$ is such a Gröbner basis for a lexicographic order with $y_1 > y_2$.

From the definition of Gröbner bases, we see that G is a basis for $\langle\{p_1, p_2\}\rangle_{\mathbb{C}[y_1,y_2]}$. Therefore,

$$\langle\{p_1, p_2\}\rangle_{\mathbb{C}[y_1,y_2,y_3]} = \langle G\rangle_{\mathbb{C}[y_1,y_2,y_3]}\,, \tag{47}$$

and additionally

$$\langle\!\langle\{p_1, p_2\}\rangle\!\rangle_{\mathbb{C}[y_1,y_2,y_3]} = \langle\!\langle G\rangle\!\rangle_{\mathbb{C}[y_1,y_2,y_3]}\,. \tag{48}$$

Using Hilbert's Nullstellensatz (Theorem 2.2), we see that the systems (22), and

$$g_1 = 0 \qquad\qquad g_2 = 0, \tag{49}$$

have the same solutions.

We now try to find solutions to the system (49) instead of the system (22). This switch does not obviously simplify the problem as we trade a system of two equations for another system of (in this case also) two equations. However, (49) has to carry some structure (for being a Gröbner basis with respect to a lexicographic order), which need not be the case for (22).

In this example we see (from $g_1 = 0$) that either $y_2 = 1$, or $y_2 = 2$ has to hold.

For $y_2 = 1$, g_2 simplifies to

$$y_1^2 - 4y_1 + 4 = (y_1 - 2)^2\,. \tag{50}$$

We obtain the solution $(2, 1)$ for (y_1, y_2).

For $y_2 = 2$, g_2 simplifies to

$$y_1^2 - 2y_1 + 1 = (y_1 - 1)^2\,, \tag{51}$$

and we arrive at the solution $(1, 2)$.

Combining the two branches we obtain (31) as solution set for (49) and therefore again as solution set for (22).

Moving on to the second problem from the beginning of this section, we try to solve (25) using Gröbner basis computations. The first step is again to choose an admissible order on the terms of $\mathbb{C}[y_1, y_2, y_3]$ and compute a Gröbner basis for $\langle\{q_1, q_2, q_3\}\rangle_{\mathbb{C}[y_1,y_2,y_3]}$. Using

$$g_1' := y_2y_3 + 1, \tag{52}$$

$$g_2' := y_1y_3 + y_1 - y_3 - 1, \tag{53}$$

$$g_3' := y_1y_2 - y_1 - y_2 + 1, \tag{54}$$

$G' := \{g_1', g_2', g_3'\}$ is such a Gröbner basis for a lexicographic order with $y_1 > y_2 > y_3$.

Again using Hilbert's Nullstellensatz, we see that the systems (25), and

$$g_1' = 0 \qquad\qquad g_2' = 0 \qquad\qquad g_3' = 0, \tag{55}$$

have the same solutions.

In this example we see (from $g_1' = 0$) that y_2 needs to be non-zero and forces $y_3 = -\frac{1}{y_2}$, analogous to the discussion of (38). Using this choice, (55) simplifies to

$$0 = 0 \tag{56}$$
$$y_1 y_2 - y_1 - y_2 + 1 = 0 \tag{57}$$
$$y_1 y_2 - y_1 - y_2 + 1 = 0. \tag{58}$$

As $y_1 y_2 - y_1 - y_2 + 1 = (y_1 - 1)(y_2 - 1)$, we see that $y_1 = 1$ or $y_2 = 1$ has to hold.

Assuming $y_1 = 1$, we obtain a solution, regardless of the non-zero choice of y_2.

Assuming $y_2 = 1$, we see that $y_3 = -\frac{1}{y_2} = -1$, and obtain a solution, regardless of the choice of y_1.

We again obtain (44) as solution set for (55) and therefore as solution set for (25).

In Section 3.3 we finally use characteristic set methods to attack the same two systems one last time, before comparing the different approaches in Section 3.4.

3.3 Characteristic sets

Characteristic set methods decompose a radical ideal into a finite number of radical ideals, each having a "nice" representation—a characteristic set. Although a characteristic set is may be a basis for the ideal, it need not be one. Still, characteristic sets allow to decide the membership problem and provide a triangular structure, hence ease equation solving.

Trying to solve (22) using characteristic set methods, the first step is to choose a ranking (Definition 5.1) on the indeterminates of $\mathbb{C}[y_1, y_2]$. With this ranking, a characteristic decomposition of $\langle\langle\{q_1, q_2\}\rangle\rangle_{\mathbb{C}[y_1,y_2]}$ is computed. Using $y_1 > y_2$,

$$\langle\langle\{p_1, p_2\}\rangle\rangle_{\mathbb{C}[y_1,y_2]} = \langle\{(y_2 - 1)(y_2 - 2), y_1 + y_2 - 3\}\rangle_{\mathbb{C}[y_1,y_2]} : \{2y_2 - 3\}^{\infty} \tag{59}$$

is such a suitable decomposition[14]. Using Hilbert's Nullstellensatz, we see that the solutions of (22) and the solutions of

$$(y_2 - 1)(y_2 - 2) = 0 \tag{60}$$
$$y_1 + y_2 - 3 = 0 \tag{61}$$
$$2y_2 - 3 \neq 0 \tag{62}$$

coincide.

From (60), we see that either $y_2 = 1$, or $y_2 = 2$ has to hold. Exploiting (61), we can read off (31) as solution set to (60)–(62) and therefore again as solution set to (22).

[14]The right hand side of (59) is a "decomposition" of the left hand side of (59) into only one component. Hence, it is not plainly visible, that the right hand side of (59) actually constitutes a decomposition. The treatment of the second example from the beginning of this section shows a decomposition into two different components in (63). There, the decomposition is better visible.

Again, we switch to the second problem presented in the beginning of this section. Trying to solve (25) using characteristic set methods, we choose the ranking $y_1 > y_2 > y_3$ to obtain the characteristic decomposition

$$\begin{aligned}\langle\!\langle\{q_1, q_2, q_3\}\rangle\!\rangle_{\mathbb{C}[y_1,y_2,y_3]} = \langle\{y_1 - 1, y_2y_3 + 1\}\rangle_{\mathbb{C}[y_1,y_2,y_3]} : \{y_3\}^\infty \cap \\ \cap \ \langle\{y_2 - 1, y_3 + 1\}\rangle_{\mathbb{C}[y_1,y_2,y_3]}\end{aligned} \tag{63}$$

From characteristic set theory, we see that both ideals on the right hand side of (63) are radical. Hence, using Hilbert's Nullstellensatz on them, we see that each solution of (25) is either a solution of the system

$$y_1 - 1 = 0 \tag{64}$$
$$y_2y_3 + 1 = 0 \tag{65}$$
$$y_3 \neq 0 \tag{66}$$

or the system

$$y_2 - 1 = 0 \tag{67}$$
$$y_3 + 1 = 0 \tag{68}$$

and vice versa.

For the system (64)–(66), we see $y_1 = 1$ from (64). Furthermore, y_2 needs to be non-zero and forces $y_3 = -\frac{1}{y_2}$, analogous to the discussion of (38). Hence, the system (64)–(66) has the solution set

$$\left\{(1, c_2, c_3) \in \mathbb{C}^3 \;\middle|\; c_2 \neq 0 \wedge c_3 = -\frac{1}{c_2}\right\}. \tag{69}$$

For the system (67)–(68), we see $y_2 = 1$ from (67), and $y_3 = -1$, from (68). We arrive at the solution set

$$\left\{(c_1, 1, -1) \in \mathbb{C}^3\right\}. \tag{70}$$

Joining the two solution sets, we again arrive at (44) as solution set for (25).

Having treated the same two systems of equations with resultants, Gröbner bases computations, and characteristic set methods, we relate those methods in Section 3.4.

3.4 Comparison of different methods

Unsurprisingly, we arrived at (31) as solution set for (22) and at (44) as solution set for (25), regardless of whether using resultants, Gröbner basis computations, or characteristic set methods. Nevertheless, each of the approaches has advantages and disadvantages.

Resultant based methods attack the problem of finding common factors of polynomials. From the perspective of trying to find solutions of systems of equations, the output of resultant based methods typically yield projections of the solution set along different directions[15]. From those projections, it is tried to reclaim the solution set. If all computed resultants are non-zero[16], the method is straight forward. However, if a resultant vanishes[17], extra effort is needed to be able to proceed using resultants.

Gröbner basis have seen much research over the last decades and allow to simplify a system of equations automatically by a program. While solutions to systems of equations closely relate to the radical ideal generated by the system, Gröbner basis computations put focus on arbitrary ideals instead of radical ideals. Although this approach has advantages (e.g.: deciding the ideal membership problem also for non-radical ideals), it does not attack systems of equations at their heart (radical ideals generated by the equations) but rather at an intermediate stage (ideals generated by the equations)[18]. Nevertheless, they are today's typical tool of choice, when attacking systems of equations.

Although characteristic sets predate Gröbner bases and while they have seen research ever since, they lack the wide range of implementations that Gröbner bases come up with. However, especially in the last two decades, characteristic set methods began to again receive broad attention and new implementations arose. Characteristic set methods naturally attack radical ideals and therefore ease exhibiting properties of the systems of equations. However, due to this focus, it is harder to use characteristic sets to treat non-radical ideals. Furthermore, characteristic sets methods typically do not yield a basis of an ideal, but decompose an ideal into different, finitely many radical ideals, for which a characteristic set can be obtained more easily.

When finally trying to relate purely algebraic and differential elimination methods, resultants do not fit nicely into the picture. Although some research works towards translating resultant concepts to differential settings (e.g.: [11] for differential operators, or [9] for ordinary differential polynomial rings), already in the purely algebraic setting complications may arise and make detours necessary, as illustrated by the previous examples. In a differential setting those obstacles do not vanish but increase. Finally, the inner workings of computing resultants (both purely algebraically and also differentially) is inherently different from Gröbner bases and characteristic set methods. The efforts necessary to nicely, and concisely describe above obstacles and work around them are beyond the scope of this thesis. We leave the inclusion of such a comparison of purely algebraic and differential resultants to further research.

In the comparison of purely algebraic and differential elimination methods, Gröbner bases are a natural candidate: In the algebraic setting they enjoy great popularity in both applications and research and are at the heart of computer algebra. As the research interest of the community broadened from algebraic settings to differential

[15]For example, the solutions of equating (29) to 0 is a projection of the solution set (31) onto its first coordinate. The solutions of equating (30) to 0 is a projection of the solution set (31) onto its second coordinate.

[16]For example systems with finite solution sets over a field having characteristic zero, as in the first of the two problems from the beginning of this section.

[17]This happens for example if the solution sets are infinite, as in the second of the two problems from the beginning of this section.

[18]Hence, trying to read off solutions from Gröbner bases is typically harder than using methods attacking the radical ideal directly. For example when fixing y_2 the relevant factor occurs to the power 2 in both (50) and (51), while corresponding equation (61) in the treatment using characteristic set methods is linear.

settings, Gröbner bases techniques saw generalizations to the differential setting. Due to the pervasive use of Gröbner bases, those relations are essential. We present Gröbner bases in Section 4 and its generalization to differential polynomial rings in Section 6.

The generalization of Gröbner basis to differential settings described in Section 6.2 borrows ideas from differential characteristic sets as for example the use of differential *pseudo*-reduction instead of differential reduction. Hence, describing the generalization of Gröbner basis to differential settings and ignoring characteristic set methods would hide relevant relations. However, the history of characteristic set methods is quite the opposite of Gröbner bases. Initially, characteristic set methods have been described for differential settings and have later been specialized to algebraic polynomial rings with the rise of mechanical theorem proving. By treating characteristic set methods just as Gröbner basis and presenting the concept algebraically and afterwards lifting it to the differential setting, we would artificially reverse history. Therefore, we directly present characteristic set methods in the differential setting in Section 5.

A presentation of purely algebraic characteristic set methods does not allow to gain further insight, as algebraic characteristic sets can be obtained by restricting the treatment of Section 5 to $\Delta = \emptyset$. Hence, we omit purely algebraic characteristic set methods from our treatment. Further information on characteristic sets in purely algebraic polynomial rings can be found for example in [23], or [42].

In the following sections we present above concepts (Section 4 introduces Gröbner bases in a purely algebraic setting, Section 5 covers differential characteristic sets, and Section 6 presents Gröbner bases for differential polynomial rings) and finally compare them in Section 7.

4 Gröbner bases in algebraic polynomial rings

In this section, we introduce Gröbner bases in algebraic polynomial rings along with their key properties. This section forms (together with Section 5) the foundation for the discussion of differential Gröbner basis in Section 6

Our treatment is split into two parts. The first part introduces notions leading to algebraic reduction, while the latter part uses algebraic reduction to define and characterize Gröbner bases.

We want to remind ourselves that in Section 2.1 we chose F to be a field having characteristic zero, and X to be a not necessarily finite set that is algebraically independent over F.

4.1 Algebraic reduction

For the computation of Gröbner bases, typically a set of polynomials is reduced again and again until a representation as Gröbner basis is reached. In this part we give a description of the reduction of a polynomial. Section 4.2 uses this reduction to obtain Gröbner bases.

When reducing a polynomial, other polynomials are again and again subtracted therefrom to eliminate "cumbersome" monomials occurring in the original polynomial. Typically, this elimination requires to introduce other monomials, which are however less "cumbersome." For describing how "cumbersome" each of the monomials is, we use an order on their corresponding terms. This order has to respect multiplication. We call such orders admissible. Reduction for Gröbner bases tries to arrive at polynomials with monomials having low terms with respect to a given admissible order.

Definition 4.1 (Admissible order for terms)**.** *[compare 45, Definition 8.2.1, page 180] We call a total order $<$ on* $\operatorname{ComMonoid}(X)$ admissible order *on X if and only if*

$$\forall t \in \operatorname{ComMonoid}(X) \setminus \{1\} : \quad 1 < t, \textit{ and additionally} \tag{71}$$

$$\forall t, s, u \in \operatorname{ComMonoid}(X) : \quad t < s \implies ut < us. \tag{72}$$

Intuitively, an admissible order is a total order on the terms respecting the multiplicative structure of the terms—multiplying terms leads to higher ranking terms.

In literature, admissible orders are also called "term order" (e.g.: [2, Definition 5.3, page 189]) or (due to a different notion of "term" and "monomial") also "monomial order" (e.g.: [12, 2.2, Definition 1, page 55]).

For the rest of this section, let $<$ denote an arbitrary but fixed admissible order on X. With this order, we can identify the leading (i.e.: maximal with respect to $<$) term and its corresponding coefficient in a polynomial.

Definition 4.2 (Coefficients and leading terms)**.** *[compare 45, Definition 8.2.2, page 181] For any $p \in F[X]$ there is a minimal set $T \subseteq \mathrm{ComMonoid}(X)$ and for all t in T there are unique $c_t \in F \setminus \{0\}$ such that*

$$p = \sum_{t \in T} c_t t. \tag{73}$$

For $t \in \mathrm{ComMonoid}(X) \setminus T$, we set $c_t = 0$.

We use Terms(p) *to denote the terms occurring in p:*

$$\mathrm{Terms}(p) := T. \tag{74}$$

For $t \in \mathrm{ComMonoid}(X)$, we use $\mathrm{coeff_T}(p, t)$ *to refer to the coefficient of p in the term t:*

$$\mathrm{coeff_T}(p, t) := c_t. \tag{75}$$

If $p \neq 0$, we use $\mathrm{ltp}(p)$ *to denote the leading term of the polynomial p:*

$$\mathrm{ltp}(p) := \max_<(T). \tag{76}$$

We lift the notion of leading terms to sets $P \subseteq F[X]$:

$$\mathrm{lts}(P) := \{t \in \mathrm{ComMonoid}(X) \mid \exists p \in P \setminus \{0\} : \mathrm{ltp}(p) = t\}. \tag{77}$$

Finally, we use $\mathrm{lc}(p)$ *to denote the leading coefficient of p:*

$$\mathrm{lc}(p) := \begin{cases} \mathrm{coeff_T}(p, \mathrm{ltp}(p)) & \textit{if } p \neq 0 \\ 0 & \textit{otherwise.} \end{cases} \tag{78}$$

The leading term of a polynomial is the crucial ingredient to reduction. For a polynomial p, reduction with respect to a polynomial q tries to get rid of those terms in p that contain $\mathrm{ltp}(q)$ as factor. If no such term occurs in p, we consider p algebraically reduced.

Definition 4.3 (Algebraically reduced polynomials)**.** *[compare 45, Definition 8.1.2, page 174] Let $P \subseteq F[X]$, $p, q \in F[X]$, and $t \in \mathrm{ComMonoid}(X)$. We say that p is* algebraically reduced *with respect to the term t and the polynomial q (or* $\mathrm{aredt}(p, t, q)$*) if and only if*

$$q = 0 \vee t\,\mathrm{ltp}(q) \notin \mathrm{Terms}(p). \tag{79}$$

p is algebraically reduced *with respect to the polynomial q (or* $\mathrm{aredp}(p, q)$*) if and only if*

$$\forall s \in \mathrm{ComMonoid}(X) : \mathrm{aredt}(p, s, q). \tag{80}$$

Finally, we use p is algebraically reduced *with respect to the set P (or* $\mathrm{areds}(p, P)$*) to denote*

$$\forall p' \in P : \mathrm{aredp}(p, p'). \tag{81}$$

Our presentation of algebraic reduction is split into two parts. First, we introduce a single step in the reduction process. Afterwards, we introduce reduction as successive application of those single reduction steps.

Definition 4.4 (Algebraic reduction step)**.** *[compare 45, Definition 8.2.4, page 182] Let $P \subseteq F[X]$, and $p, q \in F[X]$. If furthermore, $p' \in F[X]$ and $t \in \mathrm{ComMonoid}(X)$, we use q is the result of a single* algebraical remainder step *of p with respect to the term t and the polynomial p' (or* $\mathrm{aremstept}(p, t, p', q)$*) to denote*

$$\neg\mathrm{aredt}(p, t, p') \wedge q = p - \frac{\mathrm{coeff}_{\mathrm{T}}(p, t\,\mathrm{ltp}(p'))}{\mathrm{lc}(p')} t p'. \tag{82}$$

For $p' \in F[X]$, we say q is the result of a single algebraic remainder step *of p with respect to the polynomial p' (or* $\mathrm{aremstepp}(p, p', q)$*) to denote*

$$\exists\, t \in \mathrm{ComMonoid}(X) : \mathrm{aremstept}(p, t, p', q). \tag{83}$$

Finally, we say q is the result of a single algebraic remainder step *of p with respect to the set P (or* $\mathrm{aremsteps}(p, P, q)$*) if and only if*

$$\exists\, p' \in P : \mathrm{aremstepp}(p, p', q). \tag{84}$$

After defining a single reduction step, we can finally give a definition of reduction.

Definition 4.5 (Algebraic stepwise reduction)**.** *[compare 45, Theorem 8.3.1, page 183] Let $P \subseteq F[X]$, and $p, q \in F[X]$. We say that q is an* algebraic stepwise remainder *of p with respect to the set P (or* $\mathrm{aremsws}(p, P, q)$*) if and only if*

$$\mathrm{areds}(q, P), \quad \textit{and} \tag{85}$$
$$\exists k \in \mathbb{N}_0 : \mathrm{aremswc}(p, P, q, k), \tag{86}$$

where

$$\mathrm{aremswc}(p, P, q, 0) :\Longleftrightarrow p = q, \tag{87}$$
$$\mathrm{aremswc}(p, P, q, 1) :\Longleftrightarrow \mathrm{aremsteps}(p, P, q), \textit{ and} \tag{88}$$
$$\mathrm{aremswc}(p, P, q, k) :\Longleftrightarrow \exists p' \in F[X] : \mathrm{aremswc}(p, P, p', 1) \wedge \mathrm{aremswc}(p', P, q, k-1). \tag{89}$$

The relation between p and q is overly strict in above reduction specification and can be loosened. Nevertheless, the formulation of Definition 4.5 represents the formulations typically found in literature. Additionally, the presented approach translates nicely into differential reduction (Section 6.1).

With the help of Definition 4.5, we are now in the position to introduce Gröbner basis in Section 4.2.

4.2 Gröbner bases and their properties

As we see later in Theorem 4.12, Gröbner bases for an ideal allow to reduce every element of the ideal to zero. This important property is the difference between a basis and a Gröbner basis for an ideal.

This powerful property leads to a huge number of applications, if we are given a Gröbner basis. Nevertheless, we cannot easily use this criterion to check for or arrive at Gröbner bases, as ideals typically contain infinitely many elements. It turns out that it is not necessary to try to reduce all elements of an ideal, when trying to obtain a Gröbner bases: it is sufficient to check for the S-polynomials.

Definition 4.6 (S-polynomial)**.** *[compare 45, Definition 8.3.1, page 183] Let $p, q \in F[X]$. If $p \neq 0$ and also $q \neq 0$, we define the* S-polynomial *of p and q (or $\mathrm{S}(p, q)$) as*

$$\frac{1}{\mathrm{lc}(p)} tp - \frac{1}{\mathrm{lc}(q)} sq, \tag{90}$$

where $t, s \in \mathrm{ComMonoid}(X)$, such that

$$\mathrm{lcm}(\mathrm{ltp}(p), \mathrm{ltp}(q)) = t\mathrm{ltp}(p) = s\mathrm{ltp}(q). \tag{91}$$

Otherwise, we set $\mathrm{S}(p, q) := 0$.

If some set of polynomials allows to algebraically reduce all its S-polynomials to 0, the set is a Gröbner basis.

Definition 4.7 (Gröbner basis)**.** *[compare 45, Theorem 8.3.1, page 183] Let $G \subseteq F[X]$. G is a* Gröbner basis *if and only if $0 \notin G$ and*

$$\forall g, g' \in G : \mathrm{aremsws}(\mathrm{S}(g, g'), G, 0). \tag{92}$$

Some definitions of Gröbner bases allow 0 to be part of a Gröbner basis (e.g.: [45, Theorem 8.3.1, page 183]), while other definitions forbid 0 in Gröbner bases (e.g.: [2, Definition 5.37, page 207]). For reduction with respect to a Gröbner basis, it is not important, whether or not 0 is part of the Gröbner basis, as both variants reduce in exactly the same way. Also for the ideal generated by a Gröbner basis, an additional 0 would not have any impact. Despite the fact that most pieces of literature referenced in this thesis do not forbid 0 in Gröbner bases, we nevertheless choose to forbid 0 in Gröbner bases. On the one hand, this approach brings Gröbner bases and autoreduced sets (Definition 5.7) closer together. On the other hand, it seems that even most works allowing 0 in Gröbner bases intended to forbid it. In those works, Gröbner bases containing 0 typically allow to arrive at undefined situations when reducing with respect to such Gröbner bases, they cause problems in definitions, or they allow to build counter examples to proofs.

Forbidding 0 in Gröbner bases, we spare trouble in corner cases, without impeding on applicability or versatility of Gröbner basis.

Definition 4.7 does not coin an "admissible order" as we fixed an admissible order before. Note however that whether or not a subset $P \subseteq F[X]$ is a Gröbner basis depends on the chosen ordering. While for some admissible orderings P might be a Gröbner basis, it need not be a Gröbner basis for a different admissible ordering.

Typically, interest is not so much in Gröbner bases per se, but rather on Gröbner bases for a given ideal.

Definition 4.8 (Gröbner basis for an ideal)**.** *[compare 2, Definition 5.37, page 207] Let J be an ideal in $F[X]$. A Gröbner basis G in $F[X]$ is called* Gröbner basis *for J if and only if $\langle G \rangle_{F[X]} = J$.*

Definition 4.8 describes a crucial motivation for computing Gröbner bases. Given *some* basis of an ideal, computing a Gröbner basis of this ideal, we arrive at a *nice* basis for the same ideal. Gröbner bases allow for example to decide the (radical) membership problem, or effectively perform operations on ideals. And a Gröbner basis does not only exist for some special ideals, Gröbner basis exist for every ideal.

Theorem 4.9 (Every ideal has a Gröbner basis)**.** *[compare 45, Theorem 8.3.3, page 186] Let J be an ideal in $F[X]$. There exists a Gröbner basis for J.*

There are many possible approaches to arriving at Gröbner bases from a given basis of an ideal. The simplest and most straight-forward approach is to start with a candidate for a Gröbner basis, compute all possible S-polynomials, reduce those S-polynomials, adjoin the non-zero remainders to the candidate set, and iterate, until no new elements are adjoined. This approach is typically called "Buchberger's algorithm" (e.g.: [2, Theorem 5.53, page 213]) and in practice not the most efficient formulation. Much research has been devoted on speeding up Gröbner basis computations, among which the F_4 ([14]), F_5 ([15]), and SlimGB ([6]) formulations are prominent examples.

We continue presenting the relevant properties of Gröbner bases. Starting with the elimination property (Theorem 4.11, we continue with the relation between reduction and Gröbner bases (Theorem 4.12). Finally, we work towards a unique representative for the Gröbner bases of an ideal (Theorem 4.15).

In the Gröbner basis part of Section 3, we saw that the computed Gröbner bases typically contain equations involving only a small number of indeterminates; the higher ranking indeterminates have been eliminated. Such a basis eases equation solving, but cannot be expected in general. However, for admissible orders being block orders, we get the elimination property (Theorem 4.11), which leads to Gröbner bases, where higher ranking indeterminates are eliminated if possible.

Definition 4.10 (Block order)**.** *[compare 2, Examples 5.8.(iv), page 191] Let $X_1 \subseteq X$. We say that admissible order $<$ on X is a* block order *for X_1 on X if and only if*

$$\forall t, s \in \mathrm{ComMonoid}(X) : t < s \iff t_1 <_{X_1} s_1 \vee (t_1 = s_1 \wedge t_2 <_{X_2} s_2), \tag{93}$$

where

$$X_2 := X \backslash X_1, \tag{94}$$

$$<_{X_1} := < |_{\mathrm{ComMonoid}(X_1) \times \mathrm{ComMonoid}(X_1)}, \tag{95}$$

$$<_{X_2} := < |_{\mathrm{ComMonoid}(X_2) \times \mathrm{ComMonoid}(X_2)}, \tag{96}$$

and for each t *and* s *we choose*

$$t_1 \in \mathrm{ComMonoid}(X_1), t_2 \in \mathrm{ComMonoid}(X_2), \text{ such that } t = t_1 t_2, \text{ and} \tag{97}$$

$$s_1 \in \mathrm{ComMonoid}(X_1), s_2 \in \mathrm{ComMonoid}(X_2), \text{ such that } s = s_1 s_2. \tag{98}$$

In literature, block orders are also called "product orders" (e.g.: [45, Sentence after Theorem 8.4.5, page 192]).

Any lexicographic order is a block order, and they form an important group among the block orders.

Theorem 4.11 (Elimination property of Gröbner bases)**.** *[compare 45, Theorem 8.4.5, page 192] Let* $X_1 \subseteq X$*,* J *be an ideal in* $F[X]$*, and* G *be a Gröbner basis of* J *with respect to a block order for* X_1 *on* X*. Then*

$$J \cap F[X_1] = \langle G \cap F[X_1] \rangle_{F[X_1]}. \tag{99}$$

Using a block order on X for some $X_1 \subseteq X$, we see that for describing the $F[X_1]$ aspects of an ideal, those polynomials of a corresponding Gröbner basis that are in $F[X_1]$ suffice.

For lexicographic orders Theorem 4.11 states that the Gröbner basis has a certain triangular shape. Hence, Gröbner basis with respect to lexicographic orders ease equation solving.

Besides aiding equation solving, Gröbner bases (regardless of the chosen admissible order) also allow to decide the ideal membership problem.

Theorem 4.12 (Gröbner bases equivalences)**.** *[compare 45, Theorem 8.3.4, page 187] Let* J *be an ideal in* $F[X]$*, and* $P \subseteq J \setminus \{0\}$*. Then the following statements are equivalent:*

- *P is a Gröbner basis for J.*
- $\langle P \rangle_{F[X]} \supseteq J \wedge \forall p, q \in P : \mathrm{aremsws}(\mathrm{S}(p,q), P, 0)$. (100)
- $\langle \mathrm{lts}(J) \rangle_{F[X]} = \langle \mathrm{lts}(P) \rangle_{F[X]}$. (101)
- $\nexists j \in J : j \neq 0 \wedge \mathrm{areds}(j, P)$. (102)
- $\forall j \in J \, \forall p \in F[X] : \mathrm{aremsws}(j, P, p) \implies p = 0$. (103)
- $\forall j \in J : \mathrm{aremsws}(j, P, 0)$. (104)
- $\forall p \in F[X] : p \in J \iff \mathrm{aremsws}(p, P, 0)$. (105)

By listing (100) in Theorem 4.12, we reproduced (92) (after adding the first conjunctive part to assure that P is a Gröbner basis for J) from the definition of Gröbner bases (Definition 4.7) to collect all relevant equivalent formulations in a single place.

By (101), we give a characterization of Gröbner bases completely agnostic of reduction. Using this item, we could have presented Gröbner bases without ever mentioning reduction. However, it does not allow to specify Gröbner bases, but only Gröbner bases *for* *an ideal*—which however is the typical use-case for Gröbner bases. Furthermore, (101) does not directly lead to a method for computing Gröbner bases.

The formulations (102)–(105) are used later in Section 7.2 when comparing Gröbner bases to differential elimination methods. For this comparison it is advantageous to collect the relevant reduction properties of Gröbner bases in a single theorem. Among the above equations, (105) is especially noteworthy for stating that Gröbner bases allow to solve the ideal membership problem.

Among all possible Gröbner bases some carry additional properties, as for example being mutually algebraically reduced or having each element having 1 as leading coefficient. As those properties allow finding good representatives among the Gröbner bases for a certain ideal, we introduce descriptive names for those properties in the following definition.

Definition 4.13 (Algebraically reduced and normed sets)**.** *[compare 45, Definition 8.3.2, pages 187–188] Let $P \subseteq F[X]$. Then P is called* algebraically reduced *if and only if*

$$\forall p, q \in P : p \neq q \implies \operatorname{aredp}(p, q). \tag{106}$$

P is called normed *if and only if*

$$\forall p \in P : \operatorname{lc}(p) = 1. \tag{107}$$

Using above notions, we can refine Theorem 4.9 to Theorem 4.14.

Theorem 4.14 (Every ideal has a unique normed, algebraically reduced Gröbner basis)**.** *[compare 25, Theorem 1.11, pages 3429] Let J be an ideal in $F[X]$. There exists a unique normed algebraically reduced Gröbner basis for J.*

As most computer algebra systems cannot deal (sufficiently well) with infinite sets, finite Gröbner bases are desirable. In the general setting, with an arbitrary set X, Gröbner bases need not be finite. However, when restricting to finite X[19], finite Gröbner bases always exist due to Hilbert's basis theorem (Theorem 2.1).

Theorem 4.15 (Finite normed algebraically reduced Gröbner bases)**.** *[compare 45, Theorem 8.3.6, pages 188] If X is finite, then every ideal in $F[X]$ has a unique finite normed algebraically reduced Gröbner basis.*

After this treatment of Gröbner basis in algebraic polynomial rings, it would be natural to present differential Gröbner bases in the following chapter. However, one of the different formulations of differential Gröbner bases is built upon ideas from differential characteristic set methods, which have not yet been discussed. We therefore continue to present differential characteristic sets in Section 5 and postpone the introduction of differential Gröbner bases to Section 6.

[19]A finite X is the typical setting anyways for purely algebraic problems. Only, when switching to differential problems, polynomial rings are typically built from infinitely many indeterminates.

5 Differential characteristic sets

In this section we present differential characteristic sets and pseudo-reduction. We base our treatment heavily on [1].

The first part presents differential characteristic sets via being partially differentially pseudo-reduced. In the second part, we introduce specifications to compute partial differential pseudo-remainders and relate them to differential characteristic sets. Finally, we discuss coherence in the third part, which constitutes an important step in differential characteristic set computation, as explained in the fourth and last part.

5.1 Definition via being differentially pseudo-reduced

Just as Gröbner basis are typically computed by reducing a set of polynomials again and again, characteristic sets are computed by reducing a set of polynomials again and again. However, characteristic sets base themselves on a different reduction notion. Instead of the reduction used for Gröbner bases, characteristic sets use pseudo-reduction. Pseudo-reduction does not focus on terms, but on indeterminates themselves. This shift in focus is reflected by no longer requiring an admissible order, but a ranking on the indeterminates.

Definition 5.1 (Ranking of derivatives)**.** *[compare 28, I, 8, page 75] A total order $<$ on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ for which the additional properties*

$$\forall i \in I\, \forall\theta \in \Theta\, \forall\phi \in \Theta^+ : y_{i,\theta} < y_{i,\phi\theta} \tag{108}$$

and

$$\forall i, i' \in I\, \forall\theta, \theta' \in \Theta\, \forall\phi \in \Theta^+ : y_{i,\theta} < y_{i',\theta'} \implies y_{i,\phi\theta} < y_{i',\phi\theta'} \tag{109}$$

hold is called ranking *on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.*

Intuitively, a ranking is a total order respecting the differential structure of the derivatives—applying derivations to indeterminates leads to higher ranking derivatives.

For the rest of this section, let $<$ denote an arbitrary but fixed ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Similarly to the introduction of leading terms for reduction, we now introduce methods to extract information from polynomials that is relevant for pseudo-reduction. The most crucial ingredient is the leader of a polynomial, which is the highest ranking indeterminate occurring in a polynomial.

Definition 5.2 (Leader)**.** *[compare 28, I, 1, page 75] Let $p \in F\{Y\}\backslash F$. We use the term* leader *of p (or* lead(p)*) for the highest ranking derivative occurring in p with respect to the ranking $<$:*

$$\operatorname{lead}(p) := \max\left\{ z \in (y_{i,\theta})_{i\in I,\theta\in\Theta} \,\middle|\, \deg_z(p) > 0 \right\}. \tag{110}$$

In order to get a more versatile notation, we lift the notation of the leader of a single differential polynomial to sets of differential polynomials along with non-leaders.

Definition 5.3 (Sets of derivatives, leaders, and non-leaders)**.** *[compare 22, § 2.3, first paragraph, page 4] Let $P \subseteq F\{Y\}$. We use the following notation*

$$\mathfrak{D}(P) := \left\{ z \in (y_{i,\theta})_{i \in I, \theta \in \Theta} \,\middle|\, \exists p \in P : \deg_z(p) > 0 \right\}, \tag{111}$$

$$\mathfrak{L}(P) := \{ z \in \mathfrak{D}(P) \mid \exists p \in P \backslash F : \operatorname{lead}(p) = z \}, \tag{112}$$

$$\mathfrak{N}(P) := \mathfrak{D}(P) \setminus \mathfrak{L}(P), \tag{113}$$

where $\mathfrak{D}(P)$ holds the derivatives *of P, $\mathfrak{L}(P)$ contains the* leaders *of P, and $\mathfrak{N}(P)$ gathers the* non-leaders *of P,*

Using the notion of a leader, we introduce (partial) differential pseudo-reducedness, autoreduced sets and finally characteristic sets.

Definition 5.4 (Partially differentially pseudo-reduced polynomials)**.** *[compare 1, Definition 3.15, page 53] Let $p, q \in F\{Y\}$. If q is zero, p is* partially differentially pseudo-reduced *with respect to q. If p is zero and q is non-zero, p is* partially differentially pseudo-reduced *with respect to q. If p is a non-zero constant and q is not a constant, p is* partially differentially pseudo-reduced *with respect to q. If both p and q are not constants, p is* partially differentially pseudo-reduced *with respect to q if and only if*

$$\forall \theta \in \Theta^+ : \theta(\operatorname{lead}(q)) \notin \mathfrak{D}(\{p\}) \tag{114}$$

Otherwise, p is not reduced with respect to q.

We use $\operatorname{pdpredp}(p, q)$ *to denote "p is partially differentially pseudo-reduced with respect to the polynomial q".*

The final ingredient for defining differentially pseudo-reduced polynomials in Definition 5.6, is the upcoming notion of being algebraically pseudo-reduced.

Definition 5.5 (Algebraically pseudo-reduced polynomials)**.** *[compare 1, Definition 3.16, page 53][20] Let $p, q \in F\{Y\}$. If q is zero, p is* algebraically pseudo-reduced *with respect to q. If p is zero and q is non-zero, p is* algebraically pseudo-reduced *with respect to q. If p is a non-zero constant and q is not a constant, p is* algebraically pseudo-reduced *with respect to q. If both p and q are not constants, p is* algebraically pseudo-reduced *with respect to q if and only if*

$$\deg_{\operatorname{lead}(q)}(p) < \deg_{\operatorname{lead}(q)}(q). \tag{115}$$

Otherwise, p is not reduced with respect to q.

We use $\operatorname{apredp}(p, q)$ *to denote "p is algebraically pseudo-reduced with respect to the polynomial q".*

Definition 5.6 (Differentially pseudo-reduced polynomials)**.** *[compare 1, Definition 3.16, page 53] Let $p, q \in F\{Y\}$. Then, p is said to be* differentially pseudo-reduced *with respect to the polynomial q (or* $\operatorname{dpredp}(p, q)$*) if and only if*

$$\operatorname{pdpredp}(p, q) \wedge \operatorname{apredp}(p, q). \tag{116}$$

[20] The first part of Definition 5.5 coincides with Definition 5.4 (after substituting "algebraically" for "partially differentially"). The important difference is between (114) and (115). While (114) focus on finding *proper* derivatives of $\operatorname{lead}(q)$, (115) only considers $\operatorname{lead}(q)$ itself.

Characteristic sets require their elements to be mutually differentially pseudo-reduced. We call such sets of mutually differentially pseudo-reduced elements autoreduced sets.

Definition 5.7 (Autoreduced sets)**.** *[compare 28, I, 9, third paragraph on page 77] Let $P \subseteq F\{Y\}$ and $A \subseteq P$. A is called* autoreduced set *of P if and only if $0 \notin A$, and additionally*

$$\forall a, a' \in A : a \neq a' \Longrightarrow \operatorname{dpredp}(a, a') \,. \tag{117}$$

Excluding 0 from autoreduced sets has rather practical than essential reasons. 0 does not contribute to the ideal generated by an autoreduced set, yet 0 causes lots of case distinctions and complications in proofs. Hence, we exclude it. Differential characteristic set literature typically either excludes all constants (not only 0) from autoreduced sets or does not specify whether or not constants are allowed. Works excluding all constants are unnecessary restrictive, while those not specifying whether or not constants are allowed typically allow to derive contradictions in their presentation. In [1], we improve on literature's treatment of constants and give a presentation of autoreduced set allowing non-zero constants. Additionally, [1, Section 12, pages 213–238] relate the concepts related to autoreduced sets to literature.

Any autoreduced set is finite, as can be seen by applying a variant of Dickson's Lemma (e.g.: [1, Lemma 3.24, page 58]).

After lifting "being differentially pseudo-reduced" to (autoreduced) sets in Definition 5.8, we are finally in the position to define differential characteristic sets in Definition 5.9.

Definition 5.8 ((Partially) differentially pseudo-reduced with respect to sets)**.** *[compare 1, Definition 5.8, page 87] Let $q \in F\{Y\}$ and $P \subseteq F\{Y\}$. We say that q is* partially differentially pseudo-reduced *with respect to the set P (or* $\operatorname{pdpreds}(q, P)$*) if and only if*

$$\forall p \in P : \operatorname{pdpredp}(q, p). \tag{118}$$

Accordingly, we use q differentially pseudo-reduced *with respect to to the set P (or* $\operatorname{dpreds}(q, P)$*) to denote*

$$\forall p \in P : \operatorname{dpredp}(q, p). \tag{119}$$

If P is an autoreduced set, we also use $\operatorname{pdpredas}(q, P)$ *to denote* $\operatorname{pdpreds}(q, P)$ *, and* $\operatorname{dpredas}(q, P)$ *to denote* $\operatorname{dpreds}(q, P)$ *.*

Definition 5.9 (Differential characteristic set)**.** *[compare 1, Theorem 6.2, page 100] Let $P \subseteq F\{Y\}$. An autoreduced subset A of P is called a differential characteristic set of P if and only if*

$$\nexists\, p \in P : p \neq 0 \wedge \operatorname{dpredas}(p, A) \,. \tag{120}$$

An equivalent (e.g.: [1, Theorem 6.2, page 100]), alternative definition of a differential characteristic set bases itself on a ranking of autoreduced sets (e.g.: [1, Definition 3.25, page 58]). The lowest ranking autoreduced set among all possible autoreduced sets of some set P is a differential characteristic set of P (e.g.: [1, Definition 3.26, page 59]). In this thesis, we however spare introducing a ranking on autoreduced sets, and therefore also spare the definition of differential characteristic sets basing on such a ranking. Nevertheless, this equivalent definition of differential characteristic sets provides an easy proof for the existence of differential characteristic sets.

Theorem 5.10 (Existence of characteristic sets). *[compare 1, Theorem 3.28, page 60] Let $P \subseteq F\{Y\}$. P has a differential characteristic set.*

When simply trying to check whether some autoreduced set A of a finite set $P \subseteq F\{Y\}$ is a differential characteristic set of P, Definition 5.9 suffices. However, when trying to actually compute a differential characteristic set, Definition 5.9 serves only as motivation, and does not actually contribute to the computation. Instead of only checking for being differentially pseudo-reduced, it is more advantageous to actually compute differential pseudo-remainders. Therefore, we now relate differential pseudo-remainders and differential characteristic sets in Section 5.2.

5.2 Pseudo-remainders and differential characteristic sets

In relation to Gröbner bases, which are typically computed for a specific ideal, also differential characteristic sets are typically computed for a specific differential ideal. Hence, an interesting special case of Definition 5.9 is, when P is a differential ideal. Then several equivalences between differential characteristic sets and differential pseudo-reduction can be established. First, we work towards presenting differential pseudo-remainders and finally relate them to differential characteristic sets in Theorem 5.15 and Theorem 5.17.

Differential characteristic set literature presents differential pseudo-remainders in several different variants. While those approaches are all in the same spirit, they bear considerable differences, which are described for example in [1, Chapter 11.5, pages 206–212]. We adapt the notions of differential pseudo-remainders presented in [1, Chapter 5, pages 77–98], which is a first step to unifying those different formulations. However, we replace the drem in the kernel of the specification names of [1] by dprem[21]. Hence for example, we would use dpremraikras in this thesis to denote the specification dremraikras of [1]. Furthermore, if the differential pseudo-remainder is with respect to a polynomial instead of an autoreduced set, we add a trailing p to the name of the specification. For example dpremdip in this thesis refers to the specification dremdi of [1].

While [1] presents 64 different specifications of differential pseudo-reduction, we do not attempt to reproduce all of those specifications and explain their differences. Due to the renaming, we give the defining properties of all 64 specifications in Appendix A, but

[21] While this renaming is certainly cumbersome and confusing, the naming scheme for the specifications of [1] has been devised having solely differentially characteristic sets and therefore solely differential pseudo-reduction in mind, and in differential characteristic set literature, it is not common to add the "p" for differential pseudo-reduction to the name of a program or specification. Indeed, from the 26 differential pseudo-reduction presentations compared in [1, Chapter 11.5, pages 206–212], only three carry the "p".

Nevertheless, by the need to also consider reduction besides pseudo-reduction in this thesis, the naming convention of [1] seems unfortunate, as drem seems more appropriate for a "differential remainder" than for a "differential pseudo-remainder."

The most convincing solution to naming different approaches to reduction is to replace drem in the names of the specifications of [1] by dprem.

for now resort to only presenting the properties of the classes dpremas, and dpremras, which we need to relate differential pseudo-remainders to differential characteristic sets.

After introducing initials and separants and sets thereof, we present the classes dpremas, and dpremras of specifications of differential pseudo-reduction and relate them to characteristic sets. Finally, we present characterizable ideals and refine the relation between differential pseudo-reduction and characteristic sets in this context.

When reducing a polynomial p with respect to another polynomial (or set thereof), p is considered and terms of it are eliminated. For pseudo-reduction, not p, but hp is considered and again terms of it are eliminated. h is a premultiplication polynomial arising from the polynomial(s) to pseudo-reduce by. Typically, h is product of initials and/or separants of the the polynomial(s) to pseudo-reduce by. Hence, before the first variant of a specification of pseudo-reduction in Definition 5.13, we introduce notions towards separants and initials.

Definition 5.11 (Initial and separant of a differential polynomial)**.** *[compare 22, § 3.1, page 11] Let* $p \in F\{Y\}$. *If* $p \notin F$, *we choose* $d = \deg_{\mathrm{lead}(p)}(p)$ *and for all* $k \in \{0, 1, \ldots, d\}$ *we choose* $c_k \in F\left[(y_{i,\theta})_{i \in I, \theta \in \Theta, y_{i,\theta} \neq \mathrm{lead}(p)}\right]$ *such that*

$$p = \sum_{k=0}^{d} c_k \big(\,\mathrm{lead}(p)\,\big)^k. \tag{121}$$

Using this notation, we define the initial *of* p *(denoted by* $\mathrm{init}(p)$*) as*[22]

$$\mathrm{init}(p) := \begin{cases} 0 & \textit{if } p \textit{ is a constant,} \\ c_d & \textit{otherwise,} \end{cases} \tag{122}$$

and the separant *of* p *(denoted by* $\mathrm{sep}(p)$*) as*

$$\mathrm{sep}(p) := \begin{cases} 0 & \textit{if } p \textit{ is a constant,} \\ \sum_{k=1}^{d} k c_k \big(\,\mathrm{lead}(p)\,\big)^{k-1} & \textit{otherwise.} \end{cases} \tag{123}$$

Definition 5.12 (Sets of initials and separants)**.** *[compare 22, § 3.2, page 13] Let* $P \subseteq F\{Y\}$. *We use,*

$$I_P := \{q \in F\{Y\} \mid \exists p \in P : q = \mathrm{init}(p)\}\,, \tag{124}$$

$$S_P := \{q \in F\{Y\} \mid \exists p \in P : q = \mathrm{sep}(p)\}\,, \textit{and} \tag{125}$$

$$H_P := I_P \cup S_P. \tag{126}$$

Using the notation around separants and initials, we introduce dpremras and dpremas.

[22] The term "initial" is not without problems in elimination theory. Besides the presented notion from characteristic set theory, "initial" is sometimes used in Gröbner bases theory to denote $\mathrm{lc}\,(p)\mathrm{ltp}\,(p)$ for a non-zero p (e.g.: [45, Definition 8.2.2, page 181]).

We base our presentation of Gröbner bases solely on leading terms instead of "initial"s and therefore use "initial" exclusively in the characteristic set theory meaning of (122).

Definition 5.13 (Respectful differential pseudo-reduction with respect to an autoreduced set)**.** *We use* dpremras *to denote any predicate for triples* (p, A, q) *with* $p, q \in F\{Y\}$ *and* A *be an autoreduced set in* $F\{Y\}$ *implying*

$$\text{dpredas}(q, A)\,, \tag{127}$$
$$\text{dpredas}(p, A) \wedge p \neq 0 \implies q \neq 0, \tag{128}$$

and

$$\exists h \in H_A^\infty : \; hp \equiv q \pmod{[A]}\,. \tag{129}$$

If dpremras(p, A, q) *holds, we call* q *a* respectful differential pseudo-remainder *of* p *with respect to* A.

Dropping (128) from Definition 5.13, we still obtain a variant of pseudo-reduction, however no longer a *respectful* pseudo-reduction.

Definition 5.14 (Differential pseudo-reduction with respect to an autoreduced set)**.** *We use* dpremas *to denote any predicate for triples* (p, A, q) *with* $p, q \in F\{Y\}$ *and* A *be an an autoreduced set in* $F\{Y\}$ *implying*

$$\text{dpredas}(q, A)\,, \tag{130}$$

and

$$\exists h \in H_A^\infty : \; hp \equiv q \pmod{[A]}\,. \tag{131}$$

If dpremas(p, A, q) *holds, we call* q *a* differential pseudo-remainder *of* p *with respect to* A.

If differential pseudo-reduction (respectful or not) with respect to an autoreduced set of an ideal *forces* all elements of the ideal to 0, the autoreduced set is a characteristic set. Similarly, if *respectful* pseudo-reduction with respect to an autoreduced set of an ideal *allows* to take the ideal's elements to 0, the autoreduced set is a characteristic set. These implications are actually equivalences.

Theorem 5.15 (Differential characteristic sets and differential pseudo-reduction)**.** *[compare 1, Chapter 6.1, pages 99–105] Let* J *be a differential ideal in* $F\{Y\}$*, and let* A *be an autoreduced set of* J*. Then the following statements are equivalent:*

- *A is a differential characteristic set of J.*
- $\nexists\, j \in J : j \neq 0 \wedge \text{dpredas}(j, A)\,.$ (132)
- $\forall j \in J\, \forall p \in F\{Y\} : \text{dpremas}(j, A, p) \implies p = 0.$ (133)
- $\forall j \in J : \text{dpremras}(j, A, 0)\,.$ (134)

Just as for Gröbner basis in Theorem 4.12, we reproduced the defining equation of differential characteristic sets (i.e.: (120)) in Theorem 5.15 as (132) to have all relevant properties of differential characteristic sets next to each other.

For a further, final relation, we need to specialize to characterizable ideals.

Definition 5.16 (Characterizable differential ideal)**.** *[compare 22, Definition 5.1, page 24] Let J be a differential ideal in $F\{Y\}$. J is* characterizable *if and only if there is a differential characteristic set C of J such that*

$$J = [C] : H_C^\infty . \tag{135}$$

Such a differential characteristic set C is said to characterize J .

Theorem 5.17 (Characterizable differential ideals and differential pseudo-reduction)**.** *[compare 22, § 5.1, pages 24–25] Let J be a characterizable differential ideal in $F\{Y\}$ and C be an autoreduced set of J characterizing J. Choosing such a differential characteristic set C, we obtain*

$$\forall p \in F\{Y\} : p \in J \iff \operatorname{dpremas}(p, C, 0)\,. \tag{136}$$

Hence for characterizable differential ideals, differential characteristic sets actually solve the membership problem.

For Gröbner bases, we saw on page 39 that their definitions allow to come up with simple methods to obtain them. Trying to translate those methods to differential pseudo-reduction and a differential setting, we do not arrive at differential characteristic sets. We only arrive at coherent sets, which we present in Section 5.3. Nevertheless, coherent sets constitute an important intermediate goal in the computation of differential characteristic sets, as we illustrate in Section 5.4, where we briefly exhibit computation of differential characteristic sets.

5.3 Coherence

When computing Gröbner bases, reduction of S-polynomials to zero plays an important role. The S-polynomials model cancellation of *leading terms* of two polynomials by *multiplying monomials* to the polynomials. Δ-polynomials[23] are a similar concept for differential characteristic set computations modelling cancellation of *leaders* by *applying derivations*. However, while being able to reduce all S-polynomials to zero leads to a Gröbner basis, being able to pseudo-reduce all Δ-polynomials to zero only leads to coherence (Definition 5.22), which however is a prerequisite for a being differential characteristic set. Additionally, coherence is a crucial property of a set of differential polynomials, as it allows to defer further computations from differential rings to purely algebraic rings.

[23] Some papers (e.g.: [32]) use Δ within text as an abbreviation for "differential", which would turn "Δ-polynomial" into "differential polynomial". We do not use such an abbreviation and follow the notation of [22].

We introduce Δ-polynomials via the intermediate notion of pseudo-S-polynomials, which helps to relate S-polynomials and Δ-polynomials. Afterwards, we define coherence and relate it to differential characteristic sets.

Definition 5.18 (Pseudo-S-polynomial)**.** *[compare 34, Definition 3.5] Let $p, q \in F\{Y\}$. If p and q are both not constants, then we define the* pseudo-S-polynomial *of p and q (or* $\operatorname{pseudoS}(p, q)$*) to be*

$$\operatorname{init}(q)\, z^{\deg_z(q)-d} p - \operatorname{init}(p)\, z^{\deg_z(p)-d} q, \tag{137}$$

where $z = \max\{\operatorname{lead}(p), \operatorname{lead}(q)\}$*, and* $d := \min\left\{\deg_z(p), \deg_z(q)\right\}$*. Otherwise, we choose* $\operatorname{pseudoS}(p, q) := 0$*.*

The pseudo-S-polynomial of two non-constant polynomials p and q within $F\{Y\}$ differs from the the S-polynomial of p and q within the univariate algebraic polynomial ring $F\left[(y_{i,\theta})_{i\in I,\theta\in\Theta}\setminus\{z\}\right][z]$, where $z = \max\{\operatorname{lead}(p), \operatorname{lead}(q)\}$ only by a constant factor. This constant factor is due to the fact that S-polynomial divides by the leading coefficients, while the pseudo-S-polynomial multiplies with the initials.

Before defining Δ-polynomials in Definition 5.21, we introduce "least common derivatives" which are to derivatives what "least common multiples" are to terms.

Definition 5.19 (Least common derivative)**.** *[compare 22, § 4.1, paragraph before Definition 4.1, page 18] Let $z_1, z_2 \in (y_{i,\theta})_{i\in I,\theta\in\Theta}$. Using*

$$Z := \left(\overline{\{z_1\}}^{\Theta} \cap \overline{\{z_2\}}^{\Theta}\right), \tag{138}$$

we use the least common derivative *of z_1 and z_2 (or* $\operatorname{lcd}_D(z_1, z_2)$*) to denote* $\min Z$[24]*, if Z is not empty. Otherwise, the least common derivative of z_1, and z_2 does not exist.*

Definition 5.20 (Least common derivative for differential polynomials)**.** *Let $p, q \in F\{Y\}$. The* least common derivative *of p and q (or* $\operatorname{lcd}_P(p, q)$*) is*

$$\operatorname{lcd}_D(\operatorname{lead}(p), \operatorname{lead}(q)), \tag{139}$$

if neither p nor q is constant and (139) *exists. Otherwise, the least common derivative of p and q does not exist.*

Definition 5.21 (Δ-polynomial)**.** *[compare 34, Definition 4.2] Let $p, q \in F\{Y\}$. If* $\operatorname{lcd}_P(p, q)$ *exists, choose $\theta, \theta' \in \Theta$ such that*

$$\operatorname{lcd}_P(p, q) = \theta(\operatorname{lead}(p)) = \theta'(\operatorname{lead}(q)). \tag{140}$$

Then the Δ-polynomial *of p and q (or $\Delta(p, q)$) is*

$$\operatorname{pseudoS}(\theta(p), \theta'(q)) \tag{141}$$

Otherwise, $\Delta(p, q) := 0$.

[24]Note that $Z \subseteq (y_{i,\theta})_{i\in I,\theta\in\Theta}$, hence min refers to the minimum with respect to the chosen ranking.

With the notion of Δ-polynomials, we can introduce coherence. While coherence is typically established by trying to pseudo-reduce all Δ-polynomials to zero, its formulation is free of pseudo-reduction.

Definition 5.22 (Coherent autoreduced set). *[compare 39, page 397] An autoreduced set A in $F\{Y\}$ is called* coherent *if and only if for all non-constant $a, a' \in A$, for which $\mathrm{lcd}_P(a, a')$ exists and $a \neq a'$ holds, also*

$$\Delta(a, a') \in \left\langle \overline{A}^{\Theta,<z} \right\rangle : H_A{}^{\infty} \tag{142}$$

holds, where we use z to denote $\mathrm{lcd}_P(a, a')$, and $\overline{A}^{\Theta,<z}$ to denote

$$\{p \in \overline{A}^{\Theta} \mid \forall z' \in \mathfrak{D}(\{p\}) : z' < z\}. \tag{143}$$

The motivation for computing coherent autoreduced sets is three-fold. Firstly, coherence is a prerequisite for a characteristic set.

Theorem 5.23 (Characteristic sets of ideals are coherent). *[compare 21, Lemma 6.1, page 14] Let J be a differential ideal in $F\{Y\}$. Furthermore, let $C \subseteq J$ be a differential characteristic set of J[25]. Then C is coherent.*

The second motivation to compute coherent autoreduced sets is the Rosenfeld lemma, which asserts the Rosenfeld property to coherent autoreduced sets.

Definition 5.24 (Rosenfeld property). *[compare 1, Definition 7.11, page 129] Let A be an autoreduced set in $F\{Y\}$. A has the* Rosenfeld property *if and only if*

$$\forall p \in F\{Y\} : \mathrm{pdpredas}(p, A) \implies \left(p \in [A] : H_A^{\infty} \iff p \in \langle A \rangle : H_A^{\infty}\right). \tag{144}$$

Theorem 5.25 (Rosenfeld lemma). *[compare 1, Theorem 7.13, page 129] Let A be a coherent autoreduced set in $F\{Y\}$. Then A has the Rosenfeld property.*

By the Rosenfeld property, the membership problem of a differential polynomial in $[A] : H_A^{\infty}$ can be decided purely algebraic after partial differential pseudo-reduction of the differential polynomial.

Finally, coherent autoreduced sets (again via the Rosenfeld property) yield radical ideals, which is crucial for the decomposition described in Section 5.4.

Theorem 5.26 (Ideals having Rosenfeld property are radical). *[compare 1, Theorem 7.16, page 136]) Let A be an autoreduced set in $F\{Y\}$ having the Rosenfeld property. Then $[A] : H_A^{\infty}$ is a radical differential ideal.*

We continue to present an overview of how to compute differential characteristic sets in Section 5.4. There, we identify two separate stages within the computation. The first of those two stages covers obtaining coherent autoreduced sets and is motivated by Theorem 5.23, Theorem 5.25, and Theorem 5.26.

[25] Note that $J = [C] : H_C^{\infty}$ need not hold. We do not require J to be characterizable.

5.4 Characteristic decomposition

On page 39, we paraphrased Buchberger's algorithm of computing Gröbner bases, by trying to reduce all S-polynomials to zero again and again, while collecting the non-zero remainders. Although differential characteristic sets and Gröbner bases share some aspects, applying Buchberger's algorithm using differential pseudo-reduction instead of algebraic reduction does not lead to differential characteristic sets in general—even when additionally considering the Δ-polynomials. Due to the *pseudo*-reduction, the resulting autoreduced sets relate to saturated ideals and not to the original ideals.

Although each differential ideal has a differential characteristic set (Theorem 5.10), differential characteristic set methods typically do not attempt to compute such a differential characteristic set. Instead, starting with a finitely generated, radical differential ideal, characteristic set methods arrive at differential characteristic sets for other characterizable differential ideals, whose intersection yields the original ideal. Starting with some finite $P \subseteq F\{Y\}$, differential characteristic set methods obtain a finite set $\mathbb{B}$ of autoreduced sets, such that

$$[\![P]\!] = \bigcap_{C \in \mathbb{B}} [C] : H_C^\infty, \tag{145}$$

and each $C \in \mathbb{B}$ is a characteristic set of the characterizable ideal $[C] : H_C^\infty$. Using such a characteristic decomposition, we can solve for example the membership problem of $[\![P]\!]$, by delegating it to the membership problem in the ideals $[C] : H_C^\infty$. The membership problem in each $[C] : H_C^\infty$ is easily solved via Theorem 5.17.

Obtaining a decomposition in spirit of (145) is typically a two step process. A differential step is followed by a purely algebraic step. The inner workings of each of these two steps are rather involved, while not contributing to the understanding of the relations between (differential) Gröbner bases and differential characteristic sets. Hence, we only present the essential aspects of the two steps in the following paragraphs and leave a discussion of the details to literature (e.g.: [1] for the differential stage, and [21], and [23] for the algebraic stage).

The differential step operates in the differential ring $F\{Y\}$ and decomposes $[\![P]\!]$ into finitely many ideals generated by regular systems (see Definition 5.27):

$$[\![P]\!] = \bigcap_{(A,H) \in \mathbb{A}} [A] : H^\infty, \tag{146}$$

where $\mathbb{A}$ is a finite set of regular systems depending on P. As each of the A in (146) is coherent, the differential ideals $[A] : H^\infty$ are radical. A detailed treatment of the differential stage can be found for example in [1, Sections 8–10, pages 137–195].

Definition 5.27 (Regular system)**.** *[compare 3, Définition 14, page 36] Let $A, H \subseteq F\{Y\}$, such that A is a coherent autoreduced set,*

$$H_A \subseteq H^\infty, \text{ and} \tag{147}$$

$$\forall h \in H : \operatorname{pdpredas}(h, A)\,. \tag{148}$$

Then (A, H) is a called regular system

The second, purely algebraic step completes the decomposition by turning each $[A] : H^\infty$ of (146) into an intersection of finitely many characterizable ideals $[C] : H_C^\infty$ such that

$$[A] : H^\infty = \bigcap_{C \in \mathbb{B}_{(A,H)}} [C] : H_C^\infty, \tag{149}$$

where $\mathbb{B}_{(A,H)}$ depends on A and H. Each $C \in \mathbb{B}_{(A,H)}$ of (149) denotes a differential characteristic set of $[C] : H_C^\infty$. This second stage of the decomposition is typically carried out in purely algebraic rings[26]. For details about this algebraic stage, we again refer to literature (e.g.: [21], or [23]).

Combining the differential stage (146) and the algebraic stage (149), we arrive at the desired decomposition (145).

After this exposure of differential characteristic sets, we present formulations of differential Gröbner basis in Section 6, followed by a comparison of the presented concepts in Section 7.

[26]Assuming A does not contain constants (otherwise $[A] : H^\infty = F\{Y\}$ and the decomposition is trivial), this algebraic decomposition is typically computed in $F\left[\mathfrak{D}\left(A \cup H\right) \setminus \mathfrak{L}\left(A\right)\right]\left[\mathfrak{L}\left(A\right)\right]$.

6 Differential Gröbner bases

When trying to translating Gröbner basis theory to differential polynomial rings, there are basically two hurdles. The first problem is that the differential structure has to be considered. This differential structure requires revisiting the notion of admissible orderings, reduction and also considering S-polynomials arising from applying derivations. The second problem is more fundamental: The precondition to Hilbert's basis theorem (Theorem 2.1) does not hold in typical differential rings ($m \geq 1 \wedge n \geq 1$), only the Ritt Raudenbush basis theorem (Theorem 2.11) holds. Hence, the differential analogues of ways to compute Gröbner bases need not terminate; the resulting bases need not be finite.

Literature provides two ways of addressing those problems. The first approach is due to Carrà Ferro [8] and Ollivier [37]. This approach incorporates the differential structure into the admissible ordering, into reduction, and also adapts the use of S-polynomials. However, applicability depends on the termination of the used methods and the finiteness of the computed bases. We present this approach in Section 6.1. The second approach to addressing the problems of the switch to a differential setting is due to Mansfield [31]. This approach trades reduction for differential *pseudo*-reduction and in general connects ideas from Gröbner bases and differential characteristic sets. Due to the change in the used reduction paradigm, termination can be shown. However, some identities of usual Gröbner bases get lost. This approach is discussed in Section 6.2.

Although the given original references for both approaches are already roughly 20 years old, we nevertheless tried to refer to those papers as much as possible, while of course incorporating recent results.

6.1 Differential Gröbner bases following Carrà Ferro and Ollivier

In this part we present the approach to differential Gröbner bases taken in [8], and [37], which received a exhaustive round up in [10]. While in our treatment we sometimes have to criticize [10], we are well aware of the fact, that the author died before being able to revise the paper. We want to point out that our intention is not to lessen the contribution of [10]. On the contrary. We think that the contribution of [10] is an important step for differential Gröbner bases, even though the printed version comes with some problems.

When trying to lift the concept of Gröbner bases to the differential setting according to [8], and [37], the first difference to the purely algebraic formulation is a refinement of an admissible order to an differentially admissible order.

Definition 6.1 (Differentially admissible ordering)**.** *[compare 49, § 2.2, O1–O3, page 2] We call a total order* $<$ *on* $\mathrm{ComMonoid}\left((y_{i,\theta})_{i\in I,\theta\in\Theta}\right)$ differentially admissible order *on* $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ *if and only if both*

- $<$ *is an admissible order on* $(y_{i,\theta})_{i\in I,\theta\in\Theta}$*, and*
- $<|_{\left((y_{i,\theta})_{i\in I,\theta\in\Theta}\times(y_{i,\theta})_{i\in I,\theta\in\Theta}\right)}$ *is a ranking on* $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Literature presents several different variants in spirit of Definition 6.1. All those variants refine an admissible order on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$. However, the nature of those refinements is quite diverse. In the original paper by Carrà Ferro an orderly ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ (Definition B.6) is required ([8, Section 4, second definition on page 135]). The original paper by Ollivier refines admissible orders by the requirements

$$t \neq 1 \implies t < f_\delta(t) \tag{150}$$
$$t < s \implies f_\delta(t) < f_\delta(s) \tag{151}$$

for all $t, s \in \operatorname{ComMonoid}\left((y_{i,\theta})_{i\in I,\theta\in\Theta}\right)$, and $\delta \in \Delta$, where

$$\begin{array}{rccl} f_\delta: & \operatorname{ComMonoid}\left((y_{i,\theta})_{i\in I,\theta\in\Theta}\right) & \to & \operatorname{ComMonoid}\left((y_{i,\theta})_{i\in I,\theta\in\Theta}\right) \\ & u & \mapsto & \begin{cases} \operatorname{ltp}(\delta(u)) & \text{if } u \neq 1, \\ 1 & \text{otherwise.} \end{cases} \end{array}$$

In [44, Section 2, Definition 2.1, page 247], we find an even more complicated refinement of admissible orders.

[10, Section 4, pages 85–92] relates the different refinements among each other[27], and it turns out that each such set of refinements of admissible orders is a special case of an differentially admissible order, as also noted for example in [47, Section 3, pages 210–212]. Hence, we base our presentation of differential Gröbner bases on differentially admissible orders.

For Section 6.1, let $<$ denote an arbitrary but fixed differentially admissible order.

As $<$ is an admissible order, the notion of "leading terms" can be used, and we obtain a first characterization of differential Gröbner bases in spirit of (101).

Definition 6.2 (Differential Gröbner basis)**.** *[compare 10, Definition 5.2, page 92]*[28] *Let J be a differential ideal in $F\{Y\}$, and $G \subseteq F\{Y\}$. G is called* differential Gröbner basis *of J if and only if* $0 \notin G$, $G \subseteq J$[29]*, and*

$$\langle \operatorname{lts}(J)\rangle = \left\langle \operatorname{lts}\left(\overline{G}^{\Theta}\right)\right\rangle. \tag{152}$$

[27] Sadly enough, this part of [10] contains a considerable amount of formal (e.g.: not quantifying θ' in [10, Equation (4.22), page 90] and additionally dropping the condition $\theta \neq \theta'$) or minor errors (e.g.: not excluding $\theta = 1$ in [10, Equation (4.21), page 89]), and hence requires great alertness when reading it and constant comparison with the cited literature. Nevertheless, we refer to this part as its elaboration on the relations of the refinements is excellent and invaluable.

[28] While the original reference for this definition is [8, Section 4, second definition on page 135] and while this formulation is the same as in our presentation, we nevertheless refer to the more recent work [10], as the original work [8] uses a very restrictive order on the terms.

[29] While the cited definition does not require $[G] \subseteq J$, requirements in this spirit can be found in the original papers in this field ([8, Section 4, second definition on page 135] requires $[G] = J$, which seems stronger. However, as $[G] \supseteq J$ follows from (152) with $G \subseteq J$, it is equivalent to our setting. [37, Section 1.3, Definition 3, page 8] explicitly requires $G \subseteq J$). Finally, a differential Gröbner basis need not be a *basis* of J without the requirement $G \subseteq J$.

For the same arguments as made after Definition 4.7, we forbid 0 within differential Gröbner bases. However, this restriction is not crucial for the concept of a differential Gröbner basis.

Besides the more theoretic characterization of differential Gröbner bases in Definition 6.2, reduction again allows to establish many equivalences. We begin by introducing the concept of "differentially reduced" and afterwards present literature's two most common approaches to differential reduction. Finally, we elaborate on equivalences between differential Gröbner bases and properties using differential reduction.

The concept of differentially reduced polynomials naturally lifts itself from the notion of (algebraically) reduced polynomials via introducing θ within (155)

Definition 6.3 (Differentially reduced polynomials)**.** *[compare 10, Definition 5.6, page 93] Let $P \subseteq F\{Y\}$, and $p, q \in F\{Y\}$. We say that p is* differentially reduced *with respect to the polynomial q (or* $\operatorname{dredp}(p,q)$*) if and only if*[30]

$$\forall \theta \in \Theta : \operatorname{aredp}(p, \theta(q)). \tag{155}$$

We use p is differentially reduced *with respect to the set P (or* $\operatorname{dreds}(p,P)$*) to denote*

$$\forall p' \in P : \operatorname{dredp}(p, p'). \tag{156}$$

Using the notion of differentially reduced polynomials, we introduce differential reduction. We present two different approaches. The first approach (Definition 6.4) is more general and holds the differential reduction equivalent to the differential *pseudo*-reduction specification dpremdias. The second approach (Definition 6.5) lifts algebraic stepwise reduction to the differential setting. Both approaches are found in literature and allow to obtain differential Gröbner bases. However, the second variant seems to be the variant typically intended, as can be seen from the difference in equivalences to differential Gröbner bases (Theorem 6.6, and Theorem 6.7).

Definition 6.4 (Differential pseudo-reduction with respect to generated differential ideal)**.** *[compare 10, Remark 5.8, page 93] Let $p, q \in F\{Y\}$, and $P \subseteq F\{Y\}$. We say that q is a* differential remainder *of p with respect to the differential ideal generated by the set P (or* $\operatorname{dremdis}(p,P,q)$*) if and only if*

$$\operatorname{dreds}(q,P), \textit{ and} \tag{157}$$

$$p \equiv q \pmod{[P]}. \tag{158}$$

[30]Using the notation of Definition 2.6, we may rephrase (155) as

$$\operatorname{areds}\left(p, \overline{\{q\}}^{\Theta}\right), \tag{153}$$

and (156) as

$$\operatorname{areds}\left(p, \overline{P}^{\Theta}\right). \tag{154}$$

While this notation is certainly more compact, and takes better advantage of the notation already developed for purely algebraic reduction, such a formulation does not highlight Θ as much as (155) does and it does not put as much focus on bottom-up construction of predicates as (155), and (156) do. Furthermore, (155) and (156) are closer to the formulation used in [10, Definition 5.6, page 93]. Therefore, we decided to use the more verbose formulations within Definition 6.3.

Definition 6.5 (Differential stepwise reduction)**.** *[compare 37, Section 1.2, Definition 7, page 6] Let $P \subseteq F\{Y\}$, and $p, q \in F\{Y\}$. We say that q is a* d̲ifferential s̲tepw̲ise r̲e̲m̲ainder *of p with respect to the s̲et P (or* dremsws (p, P, q)*) if and only if*

$$\operatorname{dreds}(q, P), \ \textit{and} \tag{159}$$

$$\operatorname{aremsws}\left(p, \overline{P}^{\Theta}, q\right). \tag{160}$$

While (157) and (159) agree, the difference between dremdis and dremsws is between (158), and (160).

We now present the equivalent formulations to being a differential Gröbner bases using above notions of differential reduction. Again, we incorporate the defining condition (i.e.: (152)) into the list of equivalent conditions (see (161)), to collect all equivalent formulations in one place.

Theorem 6.6 (Differential Gröbner bases equivalences)**.** *[compare 37, Section 1.3, Theorem 4, page 8] Let J be a differential ideal in $F\{Y\}$, and $P \subseteq J \setminus \{0\}$. Then the following statements are equivalent:*

- *P is a Gröbner basis for J.*
- $\langle \operatorname{lts}(J) \rangle = \left\langle \operatorname{lts}\left(\overline{P}^{\Theta}\right) \right\rangle.$ (161)
- $\nexists\, j \in J : j \neq 0 \wedge \operatorname{dreds}(j, P).$ (162)
- $\forall j \in J \, \forall p \in F\{Y\} : \operatorname{dremsws}(j, P, p) \implies p = 0.$ (163)
- $\forall j \in J : \operatorname{dremsws}(j, P, 0).$ (164)
- $\forall p \in F\{Y\} : p \in J \iff \operatorname{dremsws}(p, P, 0).$ (165)
- $[P] \supseteq J \wedge \forall p, q \in \overline{P}^{\Theta} : \operatorname{dremsws}(\mathrm{S}(p, q), P, 0).$ (166)
- $\forall j \in J \, \forall p \in F\{Y\} : \operatorname{dremdis}(j, P, p) \implies p = 0.$ (167)

Theorem 6.7 (Properties using dremdis)**.** *Let J be a differential ideal in $F\{Y\}$, and $P \subseteq F\{Y\}$ with $[P] = J$. Then the following statements hold:*

- $\forall j \in J : \operatorname{dremdis}(j, P, 0).$ (168)
- $\forall p \in F\{Y\} : p \in J \iff \operatorname{dremdis}(p, P, 0).$ (169)
- $\forall p, q \in \overline{P}^{\Theta} : \operatorname{dremdis}(\mathrm{S}(p, q), P, 0).$ (170)

We want to point out, that in Theorem 6.7, P is an arbitrary subset of $F\{Y\}$ with $[P] = J$. P *need not* be a or relate to a differential Gröbner basis in any way. The chosen setting alone already *implies* (168), (169), and (170).

In fact, Theorem 6.7 is a contradiction to some formulations in literature. For example in [10, Section 5.1, Proposition 5.9, page 93] claims that (170) is equivalent to P being a differential Gröbner basis of J[31]. In Example 6.8, we give a counter-example to this claim.

[31] When closely scrutinizing the settings of Theorem 6.7 and [10, Section 5.1, Proposition 5.9, page

Example 6.8 (S-polynomial reduction by dremdis does not yield differential Gröbner bases)**.** *Let* $F = \mathbb{R}, I = \{1, 2\}$, *and* $\Delta = \{\delta\}$. *We choose a differentially admissible order that is an elimination ranking on* $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ *(Definition B.8) with* $y_1 < y_2$. *We choose*

$$p_1 := y_2, \qquad\qquad p_2 := y_{2,\delta} + y_1. \tag{171}$$

Using $P := \{p_1, p_2\}$, *and* $J := [P]$, *we see that* P *is* not *a differential Gröbner basis for* J*, due to* (152) *of Definition 6.2. For example,* $y_1 \in \langle \operatorname{lts}(J) \rangle$, *as* $y_1 = \operatorname{ltp}(p_2 - \delta(p_1))$, *but* $y_1 \notin \left\langle \operatorname{lts}\left(\overline{P}^{\Theta}\right) \right\rangle$, *as*

$$\left\langle \operatorname{lts}\left(\overline{P}^{\Theta}\right) \right\rangle = \left\langle \overline{\{y_2\}}^{\Theta} \right\rangle = [y_2]\,. \tag{172}$$

On the other hand, we see (170). *Let* $p, q \in \overline{P}^{\Theta}$. *We use* p_S *to denote* $\mathrm{S}(p, q)$. *To establish* $\operatorname{dremdis}(p_S, P, 0)$, *we have to show*

$$\operatorname{dreds}(0, P), \textit{ and} \tag{173}$$

$$p_S \equiv 0 \pmod{[P]}\,. \tag{174}$$

(173) *holds as* 0 *is reduced with respect to any polynomial. As we obtain* $p_S \in [P]$ *from the construction of* p_S, (174) *follows. Hence,* $\operatorname{dremdis}(p_S, P, 0)$, *and we see* (170).

Although P *is not a differential Gröbner basis for* J, (170) *holds. Hence, [10, Section 5.1, Proposition 5.9, page 93] does not hold.*

We devote the rest of Section 6.1 to establish a theorem similar to Theorem 4.14 in the differential setting.

Definition 6.9 (Differentially reduced sets)**.** *[compare 8, Section 4, definition on page 134] Let* $P \subseteq F\{Y\}$. *Then* P *is called* differentially reduced *if and only if*

$$\forall p, q \in P : p \neq q \implies \operatorname{dredp}(p, q). \tag{175}$$

Some variants of differential Gröbner bases require the basis to be differentially reduced (e.g.: [8, Section 4, Second definition on page 135]). We find this requirement too limiting, and follow definitions not employing such a restriction.

Combining "differentially reduced" and "normed" of Definition 4.13, we can bring Theorem 4.14 to the differential setting.

93], we see that there is a slight mismatch. Theorem 6.7 requires $[P] = J$, while this requirement is absent from [10, Section 5.1, Proposition 5.9, page 93].

Interpreting [10, Section 5.1, Proposition 5.9, page 93] literally (without $[P] = J$), we would immediately obtain that $\{1\}$ is a differential Gröbner bases for any differential ideal in $F\{Y\}$, as it allows to reduce any element to 0 and therefore can also take any S-polynomial to 0. However, 1 being a differential Gröbner bases would contradict [10, Section 5.1, Definition 5.2, page 92].

This counter-example renders [10] inconsistent, when interpreting [10, Section 5.1, Proposition 5.9, page 93] literally (without $[P] = J$). The requirement $[P] = J$ is natural and it is a typical requirement it Gröbner basis theory. Hence, we implicitly and silently add $[P] = J$ whenever referring to [10, Section 5.1, Proposition 5.9, page 93].

Theorem 6.10 (Every ideal has a unique normed, differentially reduced differential Gröbner basis). *Let J be an ideal in $F\{Y\}$. There exists a unique normed differentially reduced differential Gröbner basis for J.*

Unfortunately, there is no equivalent of Theorem 4.15 in the differential setting, as the precondition to Hilbert's basis theorem (Theorem 2.1) is violated, and hence such a finite basis need not exist. Nevertheless, there are formulations of differential Gröbner bases requiring finiteness (e.g.: [8, Section 4, Second definition on page 135]). Using such an alternative formulation, there are ideals without differential Gröbner bases. Using our formulation, every ideal has a differential Gröbner basis. Some papers use the finiteness of the basis as distinguishing property between differential Gröbner bases and differential standard bases (e.g.: [10, Definition 5.2, page 92]).

In Section 6.2 we continue, by presenting a second approach to bringing Gröbner bases to differential polynomial rings. This second approach does not replace the algebraic reduction of purely algebraic Gröbner bases by differential reduction, but by differential *pseudo*-reduction.

6.2 Differential Gröbner bases following Mansfield

While the approach to differential Gröbner bases presented in Section 6.2 may yield *infinite* sets, the approach to differential Gröbner bases of [31, Section 2, pages 25–68] tries to circumvent this issue by shifting from differential reduction to differential *pseudo*-reduction. Although the setting of [31] does not exactly agree with the setting of our thesis, we nevertheless choose to present it in our setting (after discussing the differences), as the theory also works in our setting and this rebasing improves comparability to our presentation of (differential) Gröbner basis and differential characteristic sets.

The main mismatch in setting is the notion of differential polynomial rings given in [31, Section 2.1, pages 27]. Besides obvious minor issues (e.g.: the indeterminates are algebraically dependent in [31]), the main differences are the restriction to partial derivations and the requirement of the partial derivations' coordinates to act as indeterminates of the polynomial ring. Our setting does not restrict itself to partial derivations, but allows any derivation. However, our setting does not allow coordinates of partial derivations to occur as indeterminates of the final polynomial ring structure. Instead, our setting forces those coordinates into the ground field, which can typically be modelled by an algebraic extension of the ground field by the coordinates of the partial derivations[32].

[32] For example using the field $\mathbb{R}$, $R_{1,1} = \mathbb{R}[x_1, u^1, p^1_{(0)}, p^1_{(1)}, p^1_{(2)}, \ldots]$ in the notation of [31] corresponds to $\mathbb{R}(x_1)\{Y\}$ in our notation. Although we can of course clear denominators for x_1 in our differential ring, the same set of polynomials may give rise to different ideals in the two notations. For example, the ideal generated by x_1 does not contain 1 in the formulation of [31], while it does contain 1 using our notation, as x_1 is in the coefficient domain (which is the field $\mathbb{R}(x_1)$) of our interpretation of differential polynomial rings. Such ideals however do not seem to be considered in [31], as [31, Section 2.1, last paragraph, page 27] restricts itself to "ideals whose elements contain derivative terms [Ann: i.e.: some p^j_α, which corresponds to $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ in our notation]." Nevertheless, we are not completely sure how to interpret this restriction, as in several places, elements of $\mathbb{R}$ occur in ideals of [31] (e.g.: 0 in [31, Section 2.7, Definition 9, page 46], or 1 in [31, Section 2.7, Property two, pages 46–47]).

As the approach to differential Gröbner bases of [31] however also works in our interpretation of differential polynomial rings and ideals, we chose to present the concepts of [31] in our setting.

A second issue is the chosen approach to orders in [31]. [31, Section 2.2, pages 27–32] begins by giving the defining property of the orders, followed by four examples for orders on derivatives and finally the cited section closes by a procedure to lift the orders on derivatives to orders on differential polynomials. However, lifting any of those four exemplary orders on derivatives to orders on differential polynomials, the required defining property does not hold[33]. As an order on the derivatives is sufficient for pseudo-reduction, and definitions of [31] only rely on pseudo-reduction, it is tempting, to ignore the defining property for orders on polynomials and build the theory with just the four exemplary definitions of orders on derivatives—trying to extract a sound defining property from those four presented examples. However, the last of the four variants does not allow to build meaningful pseudo-reduction without further restrictions on the used weights[34]. Hence, we chose to rebase the differential Gröbner bases approach of [31] not only in terms of the differential ring as illustrated above, but also in terms of the used order. Our presentation relies on a ranking on the derivatives. This approach covers the first three of the four presented orders[35] of [31] completely and additionally covers the fourth variant for meaningful weights.

Hence, for Section 6.2, let $<$ denote a ranking.

Having clarified the basic setting, we present a further coefficient notation, the basic pseudo-reduction step, followed by stepwise differential pseudo-reduction, and finally Mansfield differential Gröbner bases.

[33] To observe the contradiction, we begin by discussing the defining property. In [31, Section 2.2, last paragraph of page 27], we find that "[a] compatible ordering is desired, that is

$$f_1 > f_2 \implies D_i(f_1) > D_i(f_2) \text{ and } f.f_1 > f.f_2 \tag{176}$$

for all i and all [differential polynomials] f."

Sadly enough, this definition leaves f_1, and f_2 unquantified. Assuming the order $>$ within (176) should be an order on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$, $f.f_1$ and $f.f_2$ need not be comparable, as neither of them needs to be in $(y_{i,\theta})_{i\in I,\theta\in\Theta}$. Assuming the order $>$ within (176) should be an order on terms built from $(y_{i,\theta})_{i\in I,\theta\in\Theta}$, $D_i(f_1)$ and $D_i(f_2)$ need not be comparable, as neither of them needs to be a term built from $(y_{i,\theta})_{i\in I,\theta\in\Theta}$. Finally, assuming the order $>$ within (176) should be an order on the differential polynomial ring, seems most plausible from the context and the used notation. However, when using this assumption, (176) does not hold for the orders given in [31, Section 2.2, pages 27–32], which we show with the help of the following example.

Using the notation of [31], we choose $R_{0,3}$ over $\mathbb{R}$ with any order on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ such that $u^3 > u^2 > u^1$. We lift this order using the description of [31, Section 2.2, last two paragraphs, page 32], and consider

$$f_1 := u^3 + u^2 \qquad\qquad f_2 := u^3 + u^1 \tag{177}$$

We observe $f_1 > f_2$, as $\mathrm{HDT}(f_1) = u^3 = \mathrm{HDT}(f_2)$, $\mathrm{Hp}(f_1) = 1 = \mathrm{Hp}(f_2)$, $\mathrm{Hcoeff}(f_1) = 1 = \mathrm{Hcoeff}(f_2)$ (By a very rigorous interpretation, the Hcoeffs would not be comparable at all, as they have no HDTs), and finally $\mathrm{HDT}(f_1 - \mathrm{Head}(f_1)) = u^2 > u^1 = \mathrm{HDT}(f_2 - \mathrm{Head}(f_2))$. Hence, the precondition of (176) is met.

However, for $f := u^3 - u^2$, we obtain $ff_1 < ff_2$ as $\mathrm{HDT}(ff_1) = u^3 = \mathrm{HDT}(ff_2)$, $\mathrm{Hp}(f_1) = 2 = \mathrm{Hp}(f_2)$, $\mathrm{Hcoeff}(ff_1) = 1 = \mathrm{Hcoeff}(ff_2)$, and finally $\mathrm{HDT}(ff_1 - \mathrm{Head}(ff_1)) = u^2 < u^3 = \mathrm{HDT}(ff_2 - \mathrm{Head}(ff_2))$. Hence, (176) does not hold.

[34] Consider negative $w_h(x_i)$ in relevant rules, which thereby do not honor the differential structure. Or in $R_{1,2}$ over $\mathbb{R}$, for $s = 1$, consider $w_1(u^1) = w_1(u^2) = w_1(x_1) = 1$, which does not allow to resolve ties between p^1_1, and p^2_0.

[35] Those three orders satisfy the even stronger requirements of an elimination ranking (Definition B.8).

Definition 6.11 (Coefficients with respect to an indeterminate)**.** *Let* $p \in F[X]$, $z \in X$, *and* $d \in \mathbb{N}_0$. *We may then (unambiguously) choose* $c_k \in F[X] \setminus \{z\}$ *for all* $k \in \{0, 1, \ldots, \deg_z(p)\}$, *such that*

$$p = \sum_{k=0}^{\deg_z(p)} c_k z^k. \tag{178}$$

We use $\operatorname{coeff_I}(p, z, d)$ *to refer to the coefficient of* p *in the indeterminate* z *to the power* d*:*

$$\operatorname{coeff_I}(p, z, d) := \begin{cases} c_d & \text{if } d \leq \deg_z(p) \\ 0 & \text{otherwise.} \end{cases} \tag{179}$$

Note that $\operatorname{coeff_I}(p, z, d)$ is different from $\operatorname{coeff_T}(p, z^d)$. On page 17, we provide examples illustrating the difference.

Definition 6.12 (Differential pseudo-reduction Mansfield step)**.** *[compare 31, Section 2.5, page 36] Let* $p, q \in F\{Y\}$.

For $p' \in F\{Y\}$ *and* $\theta' \in \Theta$, *we say* q *is the result of a single* differential pseudo-remainder Mansfield step *of* p *with respect to the derivative operator* θ' *and the polynomial* p' *(or* $\operatorname{dpremMstepd}(p, p', \theta', q)$*) to denote*

$$\neg \operatorname{apredp}(p, \theta'(p')) \wedge q = \begin{cases} \frac{\operatorname{init}(\theta'(p'))}{c} p - \frac{\operatorname{coeff_I}(p,z,d)}{c} z^{\deg_z(p)-d} \theta'(p') & \text{if } \theta'(p') \notin F, \\ 0 & \text{otherwise,} \end{cases} \tag{180}$$

where we use $z := \operatorname{lead}(\theta'(p'))$, $d := \deg_z(\theta'(p'))$, *and* $c := \gcd(\operatorname{init}(\theta'(p')), \operatorname{coeff_I}(p, z, d))$.

For $p' \in F\{Y\}$, *we say* q *is the result of a single* differential pseudo-remainder Mansfield step *of* p *with respect to the polynomial* p' *(or* $\operatorname{dpremMstepp}(p, p', q)$*) to denote*

$$\exists\, \theta' \in \Theta : \operatorname{dpremMstepd}(p, p', \theta', q). \tag{181}$$

Finally, for $P \subseteq F\{Y\}$, *we say* q *is the result of a single* differential pseudo-remainder Mansfield step *of* p *with respect to the set* P *(or* $\operatorname{dpremMsteps}(p, P, q)$*) if and only if*

$$\exists\, p' \in P : \operatorname{dpremMstepp}(p, p', q). \tag{182}$$

Note that the fractions within (180) are purely formal due to the construction of c. Those fractions do *not* require to translate the setting to a localization of $F\{Y\}$ at c.

Furthermore, it is noteworthy that in the "otherwise" branch of (180), not only $\theta'(p') \in F$, but even $\theta'(p') \in F \setminus \{0\}$ holds. To observe this, first assume $\theta'(p') \in F$. As $\neg \operatorname{apredp}(p, \theta'(p'))$ has to hold, we see that $\theta'(p')$ cannot be zero. From $\theta'(p') \in F \setminus \{0\}$, we observe $\langle \theta'(p') \rangle = F\{Y\}$, which motivates requiring $q = 0$ for the "otherwise" branch.

Taking differential pseudo-remainder Mansfield steps again and again, we eventually arrive at a differentially pseudo-reduced polynomial.

Definition 6.13 (Stepwise differential pseudo-reduction by Mansfield steps)**.** *[compare 31, Section 2.5, second paragraph on page 37] Let $P \subseteq F\{Y\}$, and $p, q \in F\{Y\}$. We say that q is a* differential stepwise pseudo-remainder *of p with respect to Mansfield steps and the set P (or* dpremMsws (p, P, q)*) if and only if*

$$\mathrm{dpreds}(q, P)\,, \textit{and} \tag{183}$$

$$\exists k \in \mathbb{N}_0 : \mathrm{dpremMc}\,(p, P, q, k), \tag{184}$$

where

$$\mathrm{dpremMc}\,(p, P, q, 0) :\Longleftrightarrow p = q, \tag{185}$$
$$\mathrm{dpremMc}\,(p, P, q, 1) :\Longleftrightarrow \mathrm{dpremMsteps}\,(p, P, q), \textit{ and} \tag{186}$$
$$\begin{aligned}\mathrm{dpremMc}\,(p, P, q, k) :\Longleftrightarrow \exists p' \in F\{Y\} : \mathrm{dpremMc}\,(p, P, p', 1)\ \wedge \\ \wedge\ \mathrm{dpremMc}\,(p', P, q, k-1).\end{aligned} \tag{187}$$

A Mansfield differential Gröbner bases for a differential ideal is a set generating this ideal, while allowing to pseudo-reduce the ideal's elements to zero.

Definition 6.14 (Mansfield differential Gröbner basis)**.** *[compare 31, Definition 9, page 49] Let J be a differential ideal in $F\{Y\}$, and $G \subseteq F\{Y\}$. G is called* Mansfield differential Gröbner basis *of J if and only if $0 \notin G$, $[G] = J$, and*

$$\forall j \in J\, \forall p \in F\{Y\} : \mathrm{dpremMsws}\,(j, G, p) \implies p = 0. \tag{188}$$

The given reference for Definition 6.14 does not forbid 0 in Mansfield differential Gröbner bases. We nevertheless forbid it for the same arguments as made after Definition 4.7.

In the upcoming list of equivalent formulations towards Mansfield differential Gröbner basis, we again adjoin the defining condition (i.e.: (188)) to collect all conditions in a single theorem.

Theorem 6.15 (Mansfield differential Gröbner bases equivalences)**.** *Let J be a differential ideal in $F\{Y\}$, and $P \subseteq F\{Y\} \setminus \{0\}$ with $[P] = J$. Then the following statements are equivalent:*

- *P is a Mansfield differential Gröbner basis for J.*
- $\forall j \in J\, \forall p \in F\{Y\} : \mathrm{dpremMsws}\,(j, P, p) \implies p = 0.$ (189)
- $\nexists\, j \in J : j \neq 0 \wedge \mathrm{dpreds}(j, P)\,.$ (190)
- $\forall j \in J : \mathrm{dpremMsws}\,(j, P, 0).$ (191)

Having introduced Gröbner bases, differential characteristic sets, differential Gröbner bases, and Mansfield differential Gröbner bases, we now compare those notions in Section 7

7 Comparing Gröbner bases and characteristic set methodology

In this section we compare Gröbner bases (Section 4), differential characteristic sets (Section 5), differential Gröbner bases (Section 6.1, and Section 6.2).

We begin by a classification of the different methods, followed by comparison of equivalences. Finally, we briefly discuss the availability of software packages implementing the different approaches.

7.1 Classification of different approaches

In Figure 7.1, we present a classification of the elimination methods basing themselves on (pseudo-)reduction.

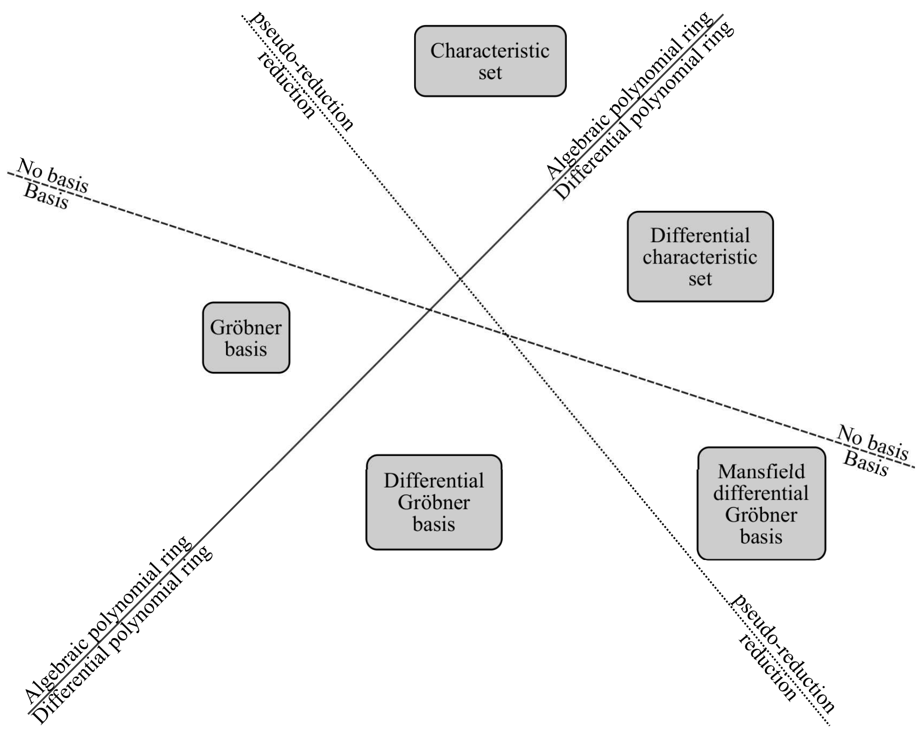

Figure 7.1: Classification of elimination methods based on (pseudo-)reduction

Each box represents an elimination method, while each line represents a border between different values of a classification criterion.

To eliminate unoccupied regions in the charted space, we also added characteristic sets, which are only briefly mentioned in Section 3. Just as Gröbner bases are a specialization for $\Delta = \emptyset$ of differential Gröbner bases via dremsws, characteristic sets are a specialization for $\Delta = \emptyset$ of differential characteristic sets. We refer the interested reader to the in-depth treatment of purely algebraic characteristic sets in [21], [23], and [42].

Methods below the solid line in Figure 7.1 (differential Gröbner bases, Mansfield differential Gröbner bases, differential characteristic sets) operate in differential polynomial rings, while those above the solid line (Gröbner bases, characteristic sets) operate in algebraic polynomial rings. Methods below the dashed line (Gröbner bases, differential Gröbner bases, Mansfield differential Gröbner bases) provide a basis for the ideal, while those above the dashed line (characteristic sets, differential characteristic sets) need not yield a basis. Methods above the dotted line (characteristic sets, differential characteristic sets, Mansfield differential Gröbner bases) take advantage of pseudo-reduction, while those below the dotted line (Gröbner bases, differential Gröbner bases) base themselves on reduction.

We observe that the center and the top-left regions are unoccupied: There is no elimination method based on reduction that does not also yield a basis of the relevant ideal.

While the three classification criteria give rise to eight distinct regions, the projection presented in Figure 7.1 can only show seven of those regions. The missing region corresponds to "pseudo-reduction" in "algebraic polynomial rings" yielding a "basis" for the ideal. No method is known to us that occupies this region. However, when restricting Mansfield differential Gröbner bases to the algebraic setting, we would obtain a method in this region.

Figure 7.1 nicely shows that Mansfield differential Gröbner bases act as connector between classical Gröbner bases notions and characteristic sets. And indeed Mansfield differential Gröbner bases blur the distinction between those two approaches. Mansfield differential Gröbner bases base themselves on pseudo-reduction, while yielding a basis and calling themselves Gröbner bases. This approach mixes the crucial aspects of both characteristic sets and Gröbner bases. In discussions often the impression arises that the distinction between characteristic sets and Gröbner bases is whether reduction or pseudo-reduction is used. Using Figure 7.1, we see that the distinction is rather whether or not the resulting set is a basis for the ideal.

After this comparison of the methodological differences, Section 7.2 tries to identify relations between the formulated equivalences for the different approaches to elimination.

7.2 Comparison of equivalences

In Table 7.1 we compare the equivalences for the different approaches to elimination presented in this thesis.

The table is divided into nine columns. The first column presents the name of the elimination method. The second and third column give the requirements on $<$, and further, general requirements. On top of columns four to nine we find expressions depending on Set, $Pred$, or both.

The table cells relate the names of elimination methods on the left to the expressions on top. If an expression is equivalent to P being a Gröbner basis, ... for J, we find appropriate values in for Set, $Pred$, or (if applicable) both in the corresponding table

				$\langle \mathrm{lts}(J)\rangle = \langle \mathrm{lts}(Set)\rangle$		$\nexists\, j \in J : j \neq 0 \wedge Pred(j, P)$		$\forall j \in J\, \forall p \in F\{Y\} : Pred(j, P, p) \implies p = 0$		$\forall j \in J : Pred(j, P, 0)$		$\forall p \in F\{Y\} : p \in J \iff Pred(p, P, 0)$		$[P] \supseteq J \wedge \forall p, q \in Set : Pred(\mathrm{S}(p, q), P, 0)$		
	Name	$<$	Requirements	*Set*	Eq#	*Pred*	Eq#	*Pred*	Eq#	*Pred*	Eq#	*Pred*	Eq#	*Set*	*Pred*	Eq#
1:	Gröbner basis	admissible order	$\Delta = \emptyset$	P	(101)	areds	(102)	aremsws	(103)	aremsws	(104)	aremsws	(105)	P	aremsws	(100)
2:	Differential Gröbner basis via dremsws	differentially admissible ordering		$\overline{P}^{\Theta}$	(161)	dreds	(162)	dremsws	(163)	dremsws	(164)	dremsws	(165)	$\overline{P}^{\Theta}$	dremsws	(166)
3:	Differential Gröbner basis via dremdis	differentially admissible ordering		$\overline{P}^{\Theta}$	(161)	dreds	(162)	dremdis	(167)	–	–	–	–	–	–	–
4:	Mansfield differential Gröbner basis	ranking	$[P] \supseteq J$	–	–	dpreds	(190)	dpremMsws	(189)	dpremMsws	(191)	–	–	–	–	–
5:	Differential characteristic set	ranking	P is autoreduced	–	–	dpredas	(132)	dpremas	(133)	dpremras	(134)	–	–	–	–	–
6:	Differential characteristic set	ranking	P characterizes J	–	–	dpredas	(132)	dpremas	(133)	dpremras	(134)	dpremas	(136)	–	–	–

Table 7.1: Comparison of equivalences for different elimination techniques

cell and additionally the equation number (Eq#), where this equivalence occurs in a theorem. If there is no such equivalence between the elimination method and the expression on top, the table cell lists "–".

In Table 7.1, J denotes an arbitrary differential ideal in $F\{Y\}$, and P denotes an arbitrary subset of $J\backslash\{0\}$.

To clarify the information contained in Table 7.1, consider the fifth cell in row 4 (i.e.: the cell containing (190) in the "Eq#" field). This cell states that if $[P] = J$[36] holds, then P being a Mansfield differential Gröbner basis of J is equivalent to J containing no non-zero differentially pseudo-reduced polynomial with respect to P.

The last cell of row 5 serves as second example. The "–" in this cell indicate that there is no equivalence between an autoreduced set P being a differential characteristic set of J and reduction of S-polynomials.

For row 1, we restrict ourselves to $\Delta = \emptyset$. In this setting we may identify $F\{Y\}$ and $F[X]$ for a finite X and thereby describe the properties of Gröbner basis using the differential formulations in the expressions on top Table 7.1. This approach also shows nicely that Gröbner bases are the algebraic counterpart to differential Gröbner bases via dremsws (row 2). $\overline{P}^{\Theta}$ becomes P and dremsws becomes aremsws when switching from the differential to the algebraic setting.

The difference between Gröbner basis via dremsws (row 2) and Gröbner basis via dremdis (row 3) is already apparent when looking at Theorem 6.6 and Theorem 6.7. However, in the direct comparison within Table 7.1, we clearly see that Gröbner basis via dremdis is not an appropriate differential counterpart to purely algebraic Gröbner basis, as for example the S-polynomial criterion (last column) gets lost.

Similarly, the relation between Gröbner basis and Mansfield differential Gröbner basis is exposed when comparing row 1 to row 4. We see that the equivalences of the leading term ideal (first column with expression on top), ideal membership problem (last but one column), and the S-polynomial criterion (last column) do not carry over. The reason is the switch from reduction to pseudo-reduction. Keeping this switch in mind and comparing row 4 with differential characteristic sets (row 5) suggests a stronger relation between Mansfield differential Gröbner bases and differential characteristic sets than between Mansfield differential Gröbner bases and Gröbner bases. Nevertheless, the crucial distinction between Mansfield differential Gröbner bases and differential characteristic sets is that Mansfield differential Gröbner bases need to be a basis for J, while this is not the case for differential characteristic sets. This observation warrants the term "basis" within "Mansfield differential Gröbner basis ". Furthermore, differential characteristic sets need to be autoreduced sets, while neither Gröbner bases nor Mansfield differential Gröbner bases need to be autoreduced sets.

The only difference between the last two rows of Table 7.1 is the additional requirement for P to characterize J (and thereby requiring P to be a differential characteristic set of J), which allows to solve the ideal membership problem (last but one column). While

[36] $P \subseteq J\backslash\{0\}$ is the general assumption on P as presented in the paragraph above. $[P] \supseteq J$ is coming from the "Requirements" column. Hence, combining those two, we obtain the requirement $[P] = J$.

the requirement of P to characterize J is a strong requirement, we nevertheless present row 6, as the ideal membership problem is crucial to elimination theory.

Finally, we want to point out that in row 5, and row 6 the last but two column contains dremras, while the other reduction specifications in those rows contain dremas—without the "r".

Inspecting the overall patterns of Table 7.1, the correlation between the loss of the leading term ideal equivalence (first column with expression on top) and the switch from admissible orders to a ranking may appear relevant. However, this loss is inherent, as for rankings there is no meaning for leading terms[37]. More intriguing is the fact that all formulations of elimination methods provide the criterion that J contains no non-zero reduced (either with respect to reduction or with respect to pseudo-reduction) polynomials (second column with expression on top), and also the criterion which forces reduction (again either with respect to reduction or pseudo-reduction) to zero (third column with expression on top). Finally, the table seems to demote the importance of the S-polynomial criterion (last column). However, this criterion is obviously crucial to Gröbner bases as it allows a simple (although typically not especially efficient) method to compute Gröbner bases. Furthermore—although this aspect is not and cannot be visible in the table—reducing (a special variant of) S-polynomials to zero is crucial when trying to obtain differential characteristic sets and leads to the concept of coherence (Section 5.3), which asserts that the generated ideals are radical and allows to conduct further computations in *purely algebraic* polynomial rings.

We close Section 7 by a brief survey of implementations of the various elimination methods in computer algebra systems.

7.3 Integration into computer algebra systems

One important aspect of methods in elimination theory is certainly their applicability in modern computer algebra systems. In general, the purely algebraic methods found their way into computer algebra systems, while differential methods are still on the verge of being implemented and included in computer algebra systems. While some of the methods provide native implementations that can be used without a computer algebra system, we only focus on implementations usable from within computer algebra system, as those implementations typically are easier accessible. We only provide links for packages not shipped with the respective computer algebra systems.

Most computer algebra systems naturally provide means to obtain Gröbner bases given a finite basis of an ideal. Computer algebra systems do not distinguish them for providing a Gröbner basis, but for providing especially efficient Gröbner basis implementations for various benchmarks.

For differential Gröbner bases the situation is fundamentally different. The main problem is that the resulting sets need not be finite and are therefore not well suited for

[37]Trying to base a notion of leading terms on recursively collecting leaders to their respective powers does not allow to reclaim equivalences.

today's computer algebra systems. We do not know implementations computing differential Gröbner bases in the general case. Nevertheless, there are several packages available in this direction (e.g.: the Rif package of Maple) or research trying to obtain differential Gröbner bases, if they are finite (e.g.: [48]).

Methods to obtain Mansfield differential Gröbner bases for certain classes of systems have been implemented in the diffgrob2 package for Maple. This package has not been shipped with Maple and is no longer publicly available. We do not know any other implementation of Mansfield differential Gröbner bases.

Characteristic set methods found their way into Maple in various packages (e.g.: the RegularChains and the epsilon package [43]). For Mathematica, the WuRitt-Solva package [30] is available. However, most computer algebra systems do not ship with methods to explicitly compute characteristic sets.

Among the major computer algebra systems, only Maple allows to compute differential characteristic sets. Besides the shipped DifferentialAlgebra package (which is a connector between Maple and the BLAD library [4]), there is the diffalg package [5] for general settings, and the epsilon package [43] for the case $\Delta = 1$.

When trying to apply the presented elimination methods using computer algebra systems, there is not a broad choice. While Gröbner bases are ubiquitously available, other methods typically require the use of Maple. However, Maple provides an extensive toolbox of mature implementations of different elimination methods.

We close this thesis, be summing up its contributions in Section 8

8 Conclusion

While especially Gröbner bases but also differential characteristic sets, and to some extend differential Gröbner bases received a considerable amount of research on their own, there is not much research comparing those related approaches. We presented such a comparison in this thesis.

After introducing the significant concepts for each of the approaches, we gave the relevant definitions and equivalences. For this presentation we used a common notation system and thereby ease comparability.

Finally, we presented relations among the methods both from a methodological, and also from a property oriented perspective. Thereby, we not only explored the connections and distinctions between the presented approaches, but also provide a basis to tie in further research in terms of additional elimination methods and also in terms of further criteria.

Purely algebraic characteristic sets serve as example for further elimination methods that can be integrated into the comparison.

Examples for further criteria are the commutativity of $F\{Y\}$ (e.g.: non-commutative rings, or commutative rings with non-commuting derivations) or the characteristic of F (e.g.: characteristic two, or positive characteristic in general). For both Gröbner basis and differential characteristic sets, there is research in both of the mentioned directions.

Additionally, it might be intriguing, to also add both algebraic and differential resultant based methods into the comparison, although their approach to elimination is a bit different.

Finally, further elaborating on the notions towards saturation will certainly allow to merge the pseudo-reduction notions used for differential characteristic set, and Mansfield differential Gröbner basis computations and find common generalizations.

A Differential pseudo-reduction

For describing different approaches to differential pseudo-reduction, [1] presents an expressive notation framework, which bases its names on drem. As [1] only discusses differential pseudo-remainders, this naming seems adequate. In our thesis, we however present differential remainders (Section 6.1) besides differential *pseudo*-remainders (Section 5), hence this naming convention may lead to confusion.

It turned out to be more appropriate to base names for differential pseudo-remainders around dprem and use drem solely for differential remainders.

This necessary difference in notation between [1] and our thesis renders [1, Appendix A, pages 281–287], which explicitly presents required properties for different formulations of differential pseudo-reduction, unusable and confusing even for simple look ups. Hence, we now reproduce [1, Appendix A, pages 281–287] with our improved naming convention.

In Table A.1, we present the requirements of differential pseudo-reduction specifications with respect to autoreduced sets. The "Requirements" columns explicitly show which specification of differential pseudo-reduction with respect to an autoreduced set carries what requirements on the triple (p, A, q) . Additionally, Table A.1 illustrates in the "Classes of reductions" columns, which specification of differential pseudo-reduction is allowed or forbidden in which class of specifications of differential pseudo-reduction. For a given specification and class of specification, "$*$" denotes that the specification can be used for the corresponding class of specifications. The absence of "$*$" denotes that the specification must not be used for the corresponding class.

For example, dpremraikas may be used for dpremas but must not be used for dpremras.

In Table A.2, we present the requirements of reduction specifications with respect to a differential polynomial. The "Requirements" columns explicitly show which specification of differential pseudo-reduction with respect to a differential polynomial carries what requirements on the triple (p, p', q) .

Table A.2 is essentially Table A.1, when setting A to $\{p'\}$, and replacing "as" from the specification names by "p". Nevertheless, we give both tables to avoid vagueness and allow easier reference.

In the formulas referenced in both Table A.1 and Table A.2, sometimes curly relation operators occur. As those relation operators are not relevant for the results of this thesis, we did not introduce them. For the use of the curly relation operator as superscript to sets with an overline (e.g.: M, and G below (195)) [1, Definition 11.5, page 202] provides a definition, while the use as binary relation of two differential polynomials (e.g.: (202)) is defined for example in [1, Definition 3.17, page 54].

	Requirements			Classes of reductions							
	reduced	congruence	additional	pdpremas	dpremas	dpremras	dpremkas	dpremndias	dpremndikas	dpremnsaias	dpremnsaikas
dpremraikras	(192)	(194)	(202), (203)	∗	∗	∗	∗	∗	∗	∗	∗
dpremraikas	(192)	(194)	(202)	∗	∗		∗	∗	∗	∗	∗
dpremrairas	(192)	(194)	(203)	∗	∗	∗		∗		∗	
dpremraias	(192)	(194)		∗	∗			∗		∗	
dpremlaikras	(192)	(196)	(202), (203)	∗	∗	∗	∗	∗	∗	∗	∗
dpremlaikas	(192)	(196)	(202)	∗	∗		∗	∗	∗	∗	∗
dpremlairas	(192)	(196)	(203)	∗	∗	∗		∗		∗	
dpremlaias	(192)	(196)		∗	∗			∗		∗	
dpremsaikras	(192)	(198)	(202), (203)	∗	∗	∗	∗	∗	∗		
dpremsaikas	(192)	(198)	(202)	∗	∗		∗	∗	∗		
dpremsairas	(192)	(198)	(203)	∗	∗	∗		∗			
dpremsaias	(192)	(198)		∗	∗			∗			
dpremdikras	(192)	(200)	(202), (203)	∗	∗	∗	∗				
dpremdikas	(192)	(200)	(202)	∗	∗		∗				
dpremdiras	(192)	(200)	(203)	∗	∗	∗					
dpremdias	(192)	(200)		∗	∗						
pdpremraikras	(193)	(195)	(202), (204)	∗							
pdpremraikas	(193)	(195)	(202)	∗							
pdpremrairas	(193)	(195)	(204)	∗							
pdpremraias	(193)	(195)		∗							
pdpremlaikras	(193)	(197)	(202), (204)	∗							
pdpremlaikas	(193)	(197)	(202)	∗							
pdpremlairas	(193)	(197)	(204)	∗							
pdpremlaias	(193)	(197)		∗							
pdpremsaikras	(193)	(199)	(202), (204)	∗							
pdpremsaikas	(193)	(199)	(202)	∗							
pdpremsairas	(193)	(199)	(204)	∗							
pdpremsaias	(193)	(199)		∗							
pdpremdikras	(193)	(201)	(202), (204)	∗							
pdpremdikas	(193)	(201)	(202)	∗							
pdpremdiras	(193)	(201)	(204)	∗							
pdpremdias	(193)	(201)		∗							

Table A.1: Specifications of differential pseudo-reductions with respect to autoreduced sets and classes thereof

Differential pseudo-reduction of p to q with respect to A

Requirements on being reduced:

- Being fully differentially pseudo-reduced:
$$\operatorname{dpredas}(q, A) \tag{192}$$
- Being partially differentially pseudo-reduced:
$$\operatorname{pdpredas}(q, A) \tag{193}$$

Congruence relation requirements:

- Congruences via rank restriction and an algebraic ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{194}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{195}$$
where $M = \overline{A}^{\precsim p}$ and $G = \begin{cases} \overline{A}^{\Theta, \precsim p} & \text{if } p \notin F, \\ A \cap F & \text{otherwise.} \end{cases}$
- Congruences via leader restriction and an algebraic ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{196}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{197}$$
where $M = \begin{cases} \overline{A}^{\leq \operatorname{lead}(p)} & \text{if } p \notin F, \\ A \cap F & \text{otherwise} \end{cases}$ and $G = \begin{cases} \overline{A}^{\Theta, \leq \operatorname{lead}(p)} & \text{if } p \notin F, \\ A \cap F & \text{otherwise.} \end{cases}$
- Congruences via leader semi restriction and an algebraic ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{198}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{199}$$
where $M = A$ and $G = \begin{cases} \overline{A}^{\Theta, \leq \operatorname{lead}(p)} & \text{if } p \notin F, \\ A \cap \ F & \text{otherwise.} \end{cases}$
- Congruences via a differential ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{[G]}, \tag{200}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{[G]}, \tag{201}$$
where $M = A$ and $G = A$.

Additional requirements:

- Rank bounded:
$$p \succsim q \tag{202}$$
- Respectful for full differential pseudo-reduction:
$$\operatorname{dpredas}(p, A) \wedge p \neq 0 \implies q \neq 0 \tag{203}$$
- Respectful for partial differential pseudo-reduction:
$$\operatorname{pdpredas}(p, A) \wedge p \neq 0 \implies q \neq 0 \tag{204}$$

	Requirements		
	reduced	congruence	additional
dpremraikrp	(205)	(207)	(215), (216)
dpremraikp	(205)	(207)	(215)
dpremrairp	(205)	(207)	(216)
dpremraip	(205)	(207)	
dpremlaikrp	(205)	(209)	(215), (216)
dpremlaikp	(205)	(209)	(215)
dpremlairp	(205)	(209)	(216)
dpremlaip	(205)	(209)	
dpremsaikrp	(205)	(211)	(215), (216)
dpremsaikp	(205)	(211)	(215)
dpremsairp	(205)	(211)	(216)
dpremsaip	(205)	(211)	
dpremdikrp	(205)	(213)	(215), (216)
dpremdikp	(205)	(213)	(215)
dpremdirp	(205)	(213)	(216)
dpremdip	(205)	(213)	
pdpremraikrp	(206)	(208)	(215), (217)
pdpremraikp	(206)	(208)	(215)
pdpremrairp	(206)	(208)	(217)
pdpremraip	(206)	(208)	
pdpremlaikrp	(206)	(210)	(215), (217)
pdpremlaikp	(206)	(210)	(215)
pdpremlairp	(206)	(210)	(217)
pdpremlaip	(206)	(210)	
pdpremsaikrp	(206)	(212)	(215), (217)
pdpremsaikp	(206)	(212)	(215)
pdpremsairp	(206)	(212)	(217)
pdpremsaip	(206)	(212)	
pdpremdikrp	(206)	(214)	(215), (217)
pdpremdikp	(206)	(214)	(215)
pdpremdirp	(206)	(214)	(217)
pdpremdip	(206)	(214)	

Table A.2: Specifications of differential pseudo-reductions with respect to a differential polynomial

Requirements on being reduced:

- Being fully differentially pseudo-reduced:
$$\operatorname{dpredp}(q, p') \tag{205}$$
- Being partially differentially pseudo-reduced:
$$\operatorname{pdpredp}(q, p') \tag{206}$$

Congruence relation requirements:

- Congruences via rank restriction and an algebraic ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{207}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{208}$$
where $M = \overline{\{p'\}}^{\precsim p}$ and $G = \begin{cases} \overline{\{p'\}}^{\Theta, \precsim p} & \text{if } p \notin F, \\ \{p'\} \cap F & \text{otherwise.} \end{cases}$
- Congruences via leader restriction and an algebraic ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{209}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{210}$$
where $M = \begin{cases} \overline{\{p'\}}^{\leq \operatorname{lead}(p)} & \text{if } p \notin F, \\ \{p'\} \cap F & \text{otherwise} \end{cases}$ and $G = \begin{cases} \overline{\{p'\}}^{\Theta, \leq \operatorname{lead}(p)} & \text{if } p \notin F, \\ \{p'\} \cap F & \text{otherwise.} \end{cases}$
- Congruences via leader semi restriction and an algebraic ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{211}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{\langle G \rangle}, \tag{212}$$
where $M = \{p'\}$ and $G = \begin{cases} \overline{\{p'\}}^{\Theta, \leq \operatorname{lead}(p)} & \text{if } p \notin F, \\ \{p'\} \cap F & \text{otherwise.} \end{cases}$
- Congruences via a differential ideal:
$$\exists h \in H_M^\infty : \ hp \equiv q \pmod{[G]}, \tag{213}$$
$$\exists h \in S_M^\infty : \ hp \equiv q \pmod{[G]}, \tag{214}$$
where $M = \{p'\}$ and $G = \{p'\}$.

Additional requirements:

- Rank bounded:
$$p \succsim q \tag{215}$$
- Respectful for full differential pseudo-reduction:
$$\operatorname{dpredp}(p, p') \wedge p \neq 0 \implies q \neq 0 \tag{216}$$
- Respectful for partial differential pseudo-reduction:
$$\operatorname{pdpredp}(p, p') \wedge p \neq 0 \implies q \neq 0 \tag{217}$$

B Refinements of rankings

In this section we present the refinements of rankings found in literature.

Several parts of this thesis refer to this section, when requiring special kinds of rankings, although giving their definition directly there would distract too much from the main arguments (e.g.: orderly ranking in the first paragraph after Definition 6.1).

After some introductory remarks and definitions, we define each of the five refinements of rankings along with examples. At the end of this section, we relate the different refinements graphically.

For the examples (and only for the examples) of this section, we choose I as some subset of $\mathbb{N}_0$. Therefore, the addition of elements of I and $\mathbb{N}_0$ is well-defined. With the help of the usual total order on $\mathbb{N}_0$, we may additionally compare the elements of I.

Before actually giving the definitions of the refinements, we introduce the concept of orders for derivative operators.

Definition B.1 (Order of derivative operators)**.** *[compare 28, I, 1, third paragraph on page 59] Let $\theta \in \Theta$. We may then (unambiguously) choose $d_\delta \in \mathbb{N}_0$ for each $\delta \in \Delta$, such that*

$$\theta = \prod_{\delta \in \Delta} \delta^{d_\delta}. \tag{218}$$

By the order *of θ (or $\operatorname{ord}(\theta)$), we refer to $\sum_{\delta \in \Delta} d_\delta$.*

For any $\delta \in \Delta$, we use order *of θ* with respect to δ *(or $\operatorname{ord}_\delta(\theta)$) to denote d_δ.*

The notion of orders on derivative operators leads to the orderly rankings, which we introduce by specializing integrated rankings to sequential rankings, which we in turn specialize to orderly rankings.

Definition B.2 (Integrated ranking)**.** *[compare 28, I, 8, page 75] A ranking $<$ on $(y_{i,\theta})_{i \in I, \theta \in \Theta}$ is called* integrated ranking *if and only if*

$$\forall \theta, \theta' \in \Theta \;\; \forall i, i' \in I \; : \; y_{i,\theta} < y_{i',\theta'} \implies \exists \phi \in \Theta \;\; : y_{i',\theta'} < y_{i,\theta\phi}. \tag{219}$$

Integrated rankings are rankings where derivatives stemming from different elements of I are interwoven.

In most algebraic settings (i.e.: $m = 0 \wedge n > 1$), no ranking can be integrated, as there are i, i', θ, θ' such that the precondition of the implication in (219) holds, while conclusion cannot hold as $\Theta = \{1\}$.

Example B.3 (Integrated ranking). *Let $I = \{1, 2\}$, and $\Delta = \{\delta_1, \delta_2, \delta_3\}$. By choosing $<$ such that*[38]

$$\begin{aligned}&\forall \theta, \theta' \in \Theta \;\; \forall i, i' \in I \;:\; y_{i,\theta} < y_{i',\theta'} :\Longleftrightarrow \\ &\quad (i + \operatorname{ord}_{\delta_3}(\theta), i, \operatorname{ord}_{\delta_{3-i}}(\theta), \operatorname{ord}(\theta)) <_{lex} (i' + \operatorname{ord}_{\delta_3}(\theta'), i', \operatorname{ord}_{\delta_{3-i}}(\theta'), \operatorname{ord}(\theta')), \end{aligned} \tag{220}$$

we see that $<$ is an integrated ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Writing down the derivatives increasingly, we obtain

$$\begin{aligned}&y_1 < y_{1,\delta_1} < y_{1,\delta_1^2} < \cdots < y_{1,\delta_2} < y_{1,\delta_1\delta_2} < y_{1,\delta_1^2\delta_2} < \cdots < y_{1,\delta_3} < y_{1,\delta_1\delta_3} < \cdots \\ &\quad \cdots < y_{1,\delta_2\delta_3} < y_{1,\delta_1\delta_2\delta_3} < \cdots < y_2 < y_{2,\delta_2} < y_{2,\delta_2^2} < \cdots < y_{2,\delta_1} < y_{2,\delta_1\delta_2} < \cdots \\ &\qquad \cdots < y_{1,\delta_3^2} < \cdots < y_{2,\delta_3} < \cdots < y_{1,\delta_3^3} < \cdots < y_{2,\delta_3^2} < \cdots . \end{aligned} \tag{221}$$

As can be seen in Example B.3, there are integrated rankings where derivatives may have infinitely many derivatives below them (e.g.: y_2, as can be seen in (221)). Refining integrated rankings to avoid such cases, we arrive at sequential rankings.

Definition B.4 (Sequential ranking). *[compare 28, I, 8, page 75] A ranking $<$ on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ is called* sequential ranking *if and only if*

$$\forall z \in (y_{i,\theta})_{i\in I,\theta\in\Theta} : \left| \{ z' \in (y_{i,\theta})_{i\in I,\theta\in\Theta} \mid z' < z \} \right| \in \mathbb{N}_0. \tag{222}$$

For sequential rankings, any derivative has only finitely many lower ranking derivatives. If the setting allows an integrated ranking (i.e.: $m > 0 \;\vee\; (m = 0 \wedge n \leq 1)$), then any sequential ranking is integrated. The converse does not hold as Example B.3 gives a ranking that is integrated, but is not sequential.

Example B.5 (Sequential ranking). *Let $I = \{1, 2\}$, and $\Delta = \{\delta_1, \delta_2\}$. By choosing $<$ such that*

$$\begin{aligned}&\forall \theta, \theta' \in \Theta \;\; \forall i, i' \in I \;:\; y_{i,\theta} < y_{i',\theta'} :\Longleftrightarrow \\ &\qquad (i + \operatorname{ord}(\theta), i, \operatorname{ord}_{\delta_{3-i}}(\theta)) <_{lex} (i' + \operatorname{ord}(\theta'), i', \operatorname{ord}_{\delta_{3-i}}(\theta')), \end{aligned} \tag{223}$$

we see that $<$ is a sequential ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Writing down the derivatives increasingly, we obtain

$$y_1 < y_{1,\delta_1} < y_{1,\delta_2} < y_2 < y_{1,\delta_1^2} < y_{1,\delta_1\delta_2} < y_{1,\delta_2^2} < y_{2,\delta_2} < y_{2,\delta_1} < \cdots . \tag{224}$$

For applications some sequential rankings are especially interesting: rankings, where sequences of increasing derivatives provide non-decreasing orders, allow to simplify (e.g.: using differential characteristic set computations) systems of differential equations by reducing their order. Therefore, such rankings are called orderly.

[38] The δ_{3-i} in the third slot of the tuples in (220) is used to select δ_2, if $i = 1$, and δ_1, if $i = 2$. Thereby, the chosen order switches with different i. This cumbersome formulation allows to arrive at a ranking that is not a Riquier ranking (Definition B.10).

Note that slots three and four are only relevant for the comparison if the first two slots agree. Hence $i = i'$. Therefore, our use of δ_{3-i} does not hurt the ranking properties.

Definition B.6 (Orderly ranking). *[compare 28, I, 8, page 75] A ranking $<$ on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ is called* orderly ranking *if and only if*

$$\forall\theta,\theta'\in\Theta\ \forall i,i'\in I : \operatorname{ord}(\theta)<\operatorname{ord}(\theta') \implies y_{i,\theta} < y_{i',\theta'}. \tag{225}$$

Although any orderly ranking is sequential, the converse cannot hold, as the ranking of Example B.5 is sequential but not orderly..

Example B.7 (Orderly ranking). *Let $I=\{1,2\}$, and $\Delta=\{\delta_1,\delta_2\}$. By choosing $<$ such that*

$$\begin{aligned}\forall\theta,\theta'\in\Theta\ \ \forall i,i'\in I\ :\ y_{i,\theta} < y_{i',\theta'} :\iff&\\ (\operatorname{ord}(\theta), i, \operatorname{ord}_{\delta_{3-i}}(\theta)) &<_{lex} (\operatorname{ord}(\theta'), i', \operatorname{ord}_{\delta_{3-i}}(\theta')),\end{aligned} \tag{226}$$

we see that $<$ is an orderly ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Writing down the derivatives increasingly, we obtain

$$\begin{aligned}y_1 < y_2 < y_{1,\delta_1} < y_{1,\delta_2} < y_{2,\delta_2} < y_{2,\delta_1} <&\\ < y_{1,\delta_1^2} < y_{1,\delta_1\delta_2} < y_{1,\delta_2^2} < y_{2,\delta_2^2} &< y_{2,\delta_1\delta_2} < y_{2,\delta_1^2} < \cdots.\end{aligned} \tag{227}$$

The remaining two refinements of rankings are not directly connected to the first three. We begin by presenting elimination rankings, which in contrast to orderly rankings do not focus on lowering the order, but on grouping derivatives by the element of I they are built from. In differential characteristic set computations, elimination rankings are used to decouple differential equations.

Definition B.8 (Elimination ranking). *[compare 22, § 3.1, last but one paragraph on page 10] A ranking $<$ on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ is called* elimination ranking *if and only if*

$$\forall\theta\in\Theta\ \ \forall i,i'\in I\ :\ y_i < y_{i'} \implies y_{i,\theta} < y_{i'}. \tag{228}$$

When writing down all the derivatives increasingly, an elimination ranking results in n blocks, where each block only contains derivatives stemming from the same element of I.

Example B.9 (Eliminiation ranking). *Let $I=\{1,2\}$, and $\Delta=\{\delta_1,\delta_2\}$. By choosing $<$ such that*

$$\begin{aligned}\forall\theta,\theta'\in\Theta\ \ \forall i,i'\in I\ :\ y_{i,\theta} < y_{i',\theta'} :\iff&\\ (i, \operatorname{ord}_{\delta_{3-i}}(\theta), \operatorname{ord}(\theta)) &<_{lex} (i', \operatorname{ord}_{\delta_{3-i}}(\theta'), \operatorname{ord}(\theta')),\end{aligned} \tag{229}$$

we see that $<$ is an elimination ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Writing down the derivatives increasingly, we obtain

$$\begin{aligned}y_1 < y_{1,\delta_1} < y_{1,\delta_1^2} < \cdots < y_{1,\delta_2} < y_{1,\delta_1\delta_2} < y_{1,\delta_1^2\delta_2} < \cdots < y_{1,\delta_2^2} < \cdots&\\ \cdots < y_2 < y_{2,\delta_2} < y_{2,\delta_2^2} < \cdots < y_{2,\delta_1} < y_{2,\delta_1\delta_2} < y_{2,\delta_1\delta_2^2} &< \cdots < y_{2,\delta_1^2} < \cdots.\end{aligned} \tag{230}$$

The final refinement of rankings are Riquier rankings, which state that structure of derivatives coming from the same element of I corresponds the structure of derivatives coming from any other element of I.

Definition B.10 (Riquier ranking)**.** *[compare 40, § 3, Theorem 7, page 5] A ranking $<$ on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$ is called* Riquier ranking *if and only if*

$$\forall \theta,\theta' \in \Theta \;\; \forall i,i' \in I \;:\; y_{i,\theta} < y_{i,\theta'} \iff y_{i',\theta} < y_{i',\theta'}. \tag{231}$$

Whether or not a ranking is a Riquier ranking is independent from whether or not the ranking meets the requirements of any of the previous four refinements.

Example B.11 (Riquier ranking)**.** *Let $I = \{1,2,3\}$, and $\Delta = \{\delta_1, \delta_2\}$. By choosing $<$ such that*

$$\begin{aligned}
&\forall \theta,\theta' \in \Theta \;\; \forall i,i' \in I \;:\; y_{i,\theta} < y_{i',\theta'} :\iff \\
&\begin{cases}
(\operatorname{ord}(\theta), \operatorname{ord}_{\delta_2}(\theta), i) <_{lex} (\operatorname{ord}(\theta'), \operatorname{ord}_{\delta_2}(\theta'), i') & \text{if } i \in \{1,2\} \wedge i' \in \{1,2\} \\
(\operatorname{ord}(\theta), \operatorname{ord}_{\delta_2}(\theta)) <_{lex} (\operatorname{ord}(\theta'), \operatorname{ord}_{\delta_2}(\theta')) & \text{if } i = i' = 3 \\
i < i' & \text{otherwise,}
\end{cases}
\end{aligned} \tag{232}$$

we see that $<$ is a Riquier ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$.

Writing down the derivatives increasingly, we obtain

$$\begin{aligned}
y_1 < y_2 < y_{1,\delta_1} < y_{2,\delta_1} < y_{1,\delta_2} < y_{2,\delta_2} < y_{1,\delta_1^2} < y_{2,\delta_1^2} < y_{1,\delta_1\delta_2} < y_{2,\delta_1\delta_2} < \\
< y_{1,\delta_2^2} < y_{2,\delta_2^2} < \cdots < y_3 < y_{3,\delta_1} < y_{3,\delta_2} < y_{3,\delta_1^2} < y_{3,\delta_1\delta_2} < y_{3,\delta_2^2}.
\end{aligned} \tag{233}$$

While the ranking in Example B.11 does not meet the requirements of any of the first four refinements of rankings, we see that it is an orderly ranking on $(y_{i,\theta})_{i\in\{1,2\},\theta\in\Theta}$, and an elimination ranking on both $(y_{i,\theta})_{i\in\{1,3\},\theta\in\Theta}$, and also on $(y_{i,\theta})_{i\in\{2,3\},\theta\in\Theta}$.

Note however, that the given examples do not represent all possible constellations of refinements for the non-degenerate case (i.e.: $m > 0 \wedge n > 1$). The rankings given in any of the first four examples can be modified to additionally meet the Riquier ranking requirements by substituting δ_1 for δ_{3-i}. Finally, there are of course also rankings meeting none of the presented refinements, as illustrated by the following example.

Example B.12 (General ranking)**.** *Let $I = \{1,2,3\}$, and $\Delta = \{\delta_1, \delta_2, \delta_3\}$. By choosing $<$ such that*

$$\begin{aligned}
&\forall \theta,\theta' \in \Theta \;\; \forall i,i' \in I \;:\; y_{i,\theta} < y_{i',\theta'} :\iff \\
&\begin{cases}
(i + \operatorname{ord}_{\delta_3}(\theta), i, \operatorname{ord}_{\delta_{3-i}}(\theta), \operatorname{ord}(\theta)) <_{lex} & \\
\qquad <_{lex} (i' + \operatorname{ord}_{\delta_3}(\theta'), i', \operatorname{ord}_{\delta_{3-i}}(\theta'), \operatorname{ord}(\theta')) & \text{if } i \in \{1,2\} \wedge i' \in \{1,2\} \\
(\operatorname{ord}(\theta), \operatorname{ord}_{\delta_3}(\theta), \operatorname{ord}_{\delta_2}(\theta)) <_{lex} & \\
\qquad <_{lex} (\operatorname{ord}(\theta'), \operatorname{ord}_{\delta_3}(\theta'), \operatorname{ord}_{\delta_2}(\theta')) & \text{if } i = i' = 3 \\
i < i' & \text{otherwise,}
\end{cases}
\end{aligned} \tag{234}$$

we see that $<$ is ranking on $(y_{i,\theta})_{i\in I,\theta\in\Theta}$, while meeting none of the presented refinements. Below, we give counter-examples for each refinement.

Writing down the derivatives increasingly, we obtain

$$\begin{gathered} y_1 < y_{1,\delta_1} < y_{1,\delta_1^2} < \cdots < y_{1,\delta_2} < y_{1,\delta_1\delta_2} < y_{1,\delta_1^2\delta_2} < \cdots < y_{1,\delta_3} < y_{1,\delta_1\delta_3} < \cdots \\ \cdots < y_{1,\delta_2\delta_3} < y_{1,\delta_1\delta_2\delta_3} < \cdots < y_2 < y_{2,\delta_2} < y_{2,\delta_2^2} < \cdots < y_{2,\delta_1} < y_{2,\delta_1\delta_2} < \cdots \\ \cdots < y_{1,\delta_3^2} < \cdots < y_{2,\delta_3} < \cdots < y_{1,\delta_3^3} < \cdots < y_{2,\delta_3^2} < \cdots . \\ \cdots < y_3 < y_{3,\delta_1} < y_{3,\delta_2} < y_{3,\delta_3} < y_{3,\delta_1^2} < y_{3,\delta_1\delta_2} < y_{3,\delta_2^2} < y_{3,\delta_1\delta_3} < y_{3,\delta_2\delta_3} < \cdots . \end{gathered} \tag{235}$$

The ranking is not integrated, as $y_1 < y_3$, while there is no $\phi \in \Theta$ such that $y_3 < y_{1,\phi}$.

The ranking is not sequential, as there are infinitely many elements below y_3.

The ranking is not orderly, as $y_{1,\delta_1} < y_3$.

The ranking is not an elimination ranking, as $y_1 < y_2$, although $y_2 < y_{1,\delta_3^2}$,

The ranking is not a Riquier ranking, as $y_{1,\delta_1} < y_{1,\delta_2}$ holds, while $y_{2,\delta_1} < y_{2,\delta_2}$ does not hold.

Having presented all the definitions and examples for refinements of rankings, we collect the example's properties in Table B.1.

			Presented ranking is				
	Example	Substitution	integrated	sequential	orderly	elimination	Riquier
1:	B.3		$*$				
2:	B.3	$\delta_{3-i} \to \delta_1$	$*$				$*$
3:	B.5		$*$	$*$			
4:	B.5	$\delta_{3-i} \to \delta_1$	$*$	$*$			$*$
5:	B.7		$*$	$*$	$*$		
6:	B.7	$\delta_{3-i} \to \delta_1$	$*$	$*$	$*$		$*$
7:	B.9					$*$	
8:	B.9	$\delta_{3-i} \to \delta_1$				$*$	$*$
9:	B.11						$*$
10:	B.12						

Table B.1: Relations between refinements of rankings and the examples of Appendix B

Each row of Table B.1 gives the properties of a ranking mentioned in this section. The first column gives the reference to the relevant example. The second column gives the substitutions that are to apply. Columns three to seven give the defined refinements of rankings. If a refinement is met by an row's ranking, the corresponding cell is marked by $*$. Otherwise, the cell is left empty.

For example, row 3 describes the ranking given in Example B.5 (without applying any substitutions). This ranking is integrated and sequential, but neither orderly, nor an elimination ranking, nor a Riquier ranking.

Row 8 deals with the ranking given in Example B.9. Substituting δ_1 for every occurring δ_{3-i} in this rankings definition, we arrive at an elimination ranking that is additionally a Riquier ranking. The ranking is however neither integrated, nor sequential, nor orderly.

We collect the structure of the possible relations between the ranking refinements for the non-degenerate case in Figure B.1.

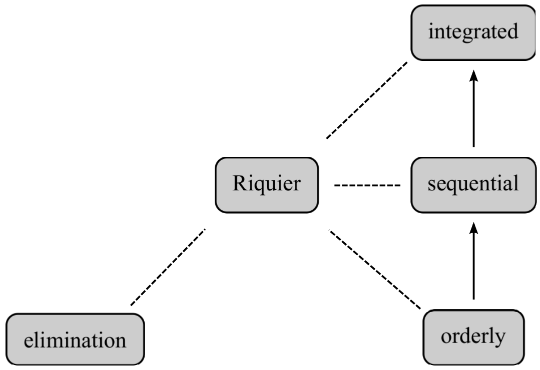

Figure B.1: Relations of ranking refinements for $m > 0 \wedge n > 1$.

Each box in Figure B.1 represents a ranking refinement. Solid arrows point towards the more general notion. Dashed lines connect non contradicting refinements where however none of the two refinements is more general than the other.

Up to now, the discussion focused on the non-degenerate setting. We close this section by briefly exhibiting the degenerate cases.

If $n \leq 1$, any ranking is integrated, and additionally an elimination, and a Riquier ranking. Rankings may or may not be sequential or orderly. However, if furthermore $m \leq 1$, then *the*[39] ranking is also sequential, and orderly.

For algebraic settings (i.e.: $m = 0$, but no restriction on n), any ranking is sequential, orderly, and also an elimination, and a Riquier ranking. Rankings need not be integrated.

[39] In those cases there is only a single ranking possible.

List of Definitions

List of Theorems

List of Examples

List of Figures

List of Tables

References

[1] C. Aistleitner. *Differential aspects of differential characteristic set computations.* PhD thesis, Johannes Kepler Universität, Linz, 2010.

[2] T. Becker and V. Weispfenning. *Gröbner Bases — A computational approach to commutative algebra.* Springer Verlag, Wien, 1993. ISBN 0-387-97971-9. In cooperation with Heinz Kredel.

[3] F. Boulier. *Étude et implantation de quelques algorithmes en algèbre différentielle.* PhD thesis, Université Lille I, June 1994. URL `http://tel.archives-ouvertes.fr/docs/00/13/78/66/PDF/these.pdf` (last seen on 2010-03-03).

[4] F. Boulier. BLAD. *Internet.* URL `http://www2.lifl.fr/~boulier/BLAD/index.html` (last seen on 2010-04-07).

[5] F. Boulier and E. Hubert. diffalg. *Internet.* URL `http://www-sop.inria.fr/cafe/Evelyne.Hubert/diffalg/` (last seen on 2005-12-06).

[6] M. Brickenstein. Slimgb: Gröbner Bases with Slim Polynomials. In *Reports On Computer Algebra*, number 35. Centre for Computer Algebra, University of Kaiserslautern, September 2005. URL `http://www.mathematik.uni-kl.de/~zca/Reports_on_ca/35/paper_35_full.ps.gz` (last seen on 2010-08-24).

[7] B. Buchberger and A. Zapletal. Gröbner bases bibliography. *Internet.* URL `http://www.ricam.oeaw.ac.at/Groebner-Bases-Bibliography/` (last seen on 2010-11-30).

[8] G. Carrà Ferro. Gröbner bases and differential algebra. In L. Huguet and A. Poli, editors, *Proceedings of the 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 356 of *Lecture Notes in Computer Science*, pages 131–140. Springer, 1987. ISBN 3-540-51082-6.

[9] G. Carrà Ferro. A resultant theory for ordinary algebraic differential equations. In T. Mora and H. F. Mattson, editors, *Proceedings of the 12th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1255 of *Lecture Notes in Computer Science*, pages 55–65. Springer, 1997. ISBN 3-540-63163-1.

[10] G. Carrà Ferro. *A survey on differential Gröbner bases*, pages 77–108. Number 2 in Radon Series on Computational and Applied Mathematics. Walter de Gruyter, 2007. ISBN 978-3-11-019323-7.

[11] M. Chardin. Differential resultants and subresultants. In L. Budach, editor, *Proceedings of the 1991 Fundamentals of Computation Theory*, volume 529 of *Lecture Notes in Computer Science*, pages 180–189. Springer, 1993. ISBN 3-540-54458-5.

[12] D. A. Cox, J. B. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Springer, 3. edition, 2007. ISBN 978-0-387-35650-1.

[13] Emacs. *Internet.* URL `http://www.gnu.org/software/emacs/emacs.html` (last seen on 2010-05-27).

[14] J.-C. Faugère. A new efficient algorithm for computing gröbner bases (F4). *Journal of Pure and Applied Algebra*, 139(1–3):61–88, 1999. doi: 10.1016/S0022-4049(99)00005-5. URL `http://www-calfor.lip6.fr/~jcf/Papers/F99a.pdf` (last seen on 2010-08-24).

[15] J.-C. Faugère. A new efficient algorithm for computing gröbner bases without reduction to zero (F5). In T. Mora, editor, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, pages 55–62. ACM Press, 2001. ISBN 1-58113-484-3. URL `http://www-calfor.lip6.fr/~jcf/Papers/F02a.pdf` (last seen on 2010-08-24).

[16] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants and multidimensional determinants*. Mathematics: theory & applications. Birkhäuser GmbH, 1994. ISBN 0-8176-3660-9.

[17] Gentoo linux. *Internet*. URL `http://www.gentoo.org/` (last seen on 2010-05-27).

[18] The GNU operating system. *Internet*. URL `http://www.gnu.org/` (last seen on 2010-05-27).

[19] O. Golubitsky, M. Kondratieva, M. Moreno Maza, and A. Ovchinnikov. A bound for the Rosenfeld Groebner algorithm. *Journal of Symbolic Computation*, 43(8): 582–610, August 2008. doi: 10.1016/j.jsc.2007.12.002.

[20] Graphviz. *Internet*. URL `http://www.graphviz.org/` (last seen on 2010-05-27).

[21] E. Hubert. Factorization free decomposition algorithms in differential algebra. *Journal of Symbolic Computation*, 29(4–5):641–662, 2000. doi: 10.1006/jsco.1999.0344.

[22] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms II: Differential systems. In F. Winkler and U. Langer, editors, *SNSC*, volume 2630 of *Lecture Notes in Computer Science*. Springer, 2003. ISBN 3-540-40554-2. URL `http://www-sop.inria.fr/members/Evelyne.Hubert/publications/sncsd.pdf` (last seen on 2010-03-03).

[23] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms I: Polynomial systems. In F. Winkler and U. Langer, editors, *SNSC*, volume 2630 of *Lecture Notes in Computer Science*. Springer, 2003. ISBN 3-540-40554-2. URL `http://www-sop.inria.fr/members/Evelyne.Hubert/publications/sncsp.pdf` (last seen on 2010-03-03).

[24] E. Hubert. Differential algebra for derivations with nontrivial commutation rules. *Journal of Pure and Applied Algebra*, 200:163–190, 2005. doi: 10.1016/j.jpaa.2004.12.034.

[25] K. Iima and Y. Yoshino. Gröbner bases for the polynomial ring with infinite variables and their applications. *Communications in Algebra*, 37(10):3424–3437, 2009. URL `http://www.math.okayama-u.ac.jp/~yoshino/pdffiles/Groebner7.pdf` (last seen on 2010-08-26).

[26] Inkscape. *Internet*. URL `http://inkscape.org/` (last seen on 2010-12-02).

[27] I. Kaplansky. *An introduction to differential algebra*. Hermann, Paris, 1957.

[28] E. R. Kolchin. *Differential Algebra and Algebraic Groups*, volume 54 of *Pure and Applied Mathematics*. Academic Press, 1973.

[29] Linux. *Internet*. URL `http://kernel.org/` (last seen on 2010-05-27).

[30] H.-S. Liu. WuRittSolva: Implementation of Wu-Ritt Characteristic Set Method. *Internet*. URL `http://library.wolfram.com/infocenter/MathSource/5716/` (last seen on 2005-12-06).

[31] E. Mansfield. *Differential Gröbner bases*. PhD thesis, University of Sydney, 1991. URL `http://www.kent.ac.uk/ims/personal/elm2/liz/papers/thesis.pdf.gz` (last seen on 2010-03-31).

[32] M. Minzlaff and J. Calmet. A new definition for passivity and its relation to coherence. In *8th International Conference on Artificial Intelligence and Symbolic Computation*, 2006. doi: 10.1007/11856290_10. URL `http://www.math.tu-berlin.de/~minzlaff/publications/mc-06-ndp.pdf` (last seen on 2010-01-07).

[33] F. Mora. Gröbner bases for non-commutative polynomial rings. In J. Calmet, editor, *Proceedings of the 3rd International Symposium on Algebraic Algorithms and Error-Correcting Codes*, volume 229 of *Lecture Notes in Computer Science*, pages 353–362. Springer, 1986. ISBN 3-540-16776-5. doi: 10.1007/3-540-16776-5_740.

[34] S. Morrison. The differential ideal $[P] : M^\infty$. *Journal of Symbolic Computation*, 28(4–5):631–656, Oct./Nov. 1999. ISSN 0747-7171. doi: 10.1006/jsco.1999.0318.

[35] n. n. JKU Linz. URL `http://www.jku.at/zv/stpa/tndok.htm` (last seen on 2007-07-18).

[36] A. Neubauer. Deckblatt für Dissertationen an der TNF der JKU Linz, 2009. URL `http://www.jku.at/STA/content/e4426/e4269/e3904/e3903/e3902/e49235/coversheet-tnf_ger.zip` (last seen on 2010-05-24).

[37] F. Ollivier. Standard bases of differential ideals. In S. Sakata, editor, *Proceedings of the 8th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 508 of *Lecture Notes in Computer Science*, pages 304–321. Springer, 1991. ISBN 3-540-54195-0. doi: 10.1007/3-540-54195-0_60.

[38] J. F. Ritt. *Differential Algebra*, volume 33 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, 1950. URL `http://www.ams.org/online_bks/coll33/` (last seen on 2004-09-03).

[39] A. Rosenfeld. Specializations in differential algebra. *Transactions of the Mathematical Society*, 90(3):394–407, March 1959.

[40] C. J. Rust and G. J. Reid. Rankings of partial derivatives. In W. Küchlin, editor, *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, pages 9–16. ACM Press, 1997. ISBN 0-89791-875-4. URL `http://oldweb.cecm.sfu.ca/~reid/Rust/RustReidIssac97.dvi.gz` (last seen on 2006-08-04).

[41] TeX Live. *Internet*. URL `http://tug.org/texlive/` (last seen on 2010-05-27).

[42] D. Wang. *Elimination Methods*. Springer, 2001. ISBN 3-211-83241-6.

[43] D. Wang. Epsilon. *Internet*. URL `http://www-calfor.lip6.fr/~wang/epsilon/` (last seen on 2005-12-06).

[44] V. Weispfenning. Differential term-orders. In M. Bronstein, editor, *Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation*, page 245–253. ACM Press, 1993. ISBN 0-89791-604-2.

[45] F. Winkler. *Polynomial algorithms in computer algebra*. Springer, 1996. ISBN 3-211-82759-5.

[46] Xfig. *Internet*. URL `http://www.xfig.org/` (last seen on 2010-05-27).

[47] A. I. Zobnin. Essential properties of admissible orderings and rankings. In I. Chajda, K. Denecke, G. Eigenthaler, M. Goldstern, W. B. Müller, and R. Pöschl, editors, *Contributions to General Algebra 14*, page 205–221. Verlag Johannes Heyn, Klagenfurt, 2004. ISBN 3-7084-0116-6. Proceedings of the Olomouc Workshop 2002 on General Algebra, Potsdam Workshop 2003 on General Algebra.

[48] A. I. Zobnin. Admissible orderings and finiteness criteria for differential standard bases. In M. Kauers, editor, *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation*, pages 365–372. ACM Press, 2005. ISBN 1-59593-095-7.

[49] A. I. Zobnin. On standard bases in rings of differential polynomials. *Journal of Mathematical Sciences*, 135(5):3327–3335, 2006. doi: 10.1007/s10958-006-161-3.

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit 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. [35]

Linz, Dezember 2010