Gröbnerbasen in gewöhnlichen differentiellen Polynomringen

Holger Bluhm

Dissertation
zur Erlangung des Grades
eines Doktors der Naturwissenschaften

Der Fakultät für Mathematik
der Technischen Universität Dortmund
vorgelegt im April 2008

Tag der mündlichen Prüfung:	28. Juli 2008
Erstgutachter:	Prof. Dr. Martin Kreuzer
Zweitgutachter:	Prof. Dr. Hans–Michael Möller
Dritter Prüfer:	HD Dr. Walter Gubler
Vorsitzender:	Prof. Dr. Heribert Blum

Inhaltsverzeichnis

Einleitung

Die Theorie der Gröbnerbasen ist ohne Zweifel das Fundament der Computeralgebra. Mit ihrer Hilfe lassen sich viele Probleme aus der kommutativen Algebra bewältigen. Ist K ein Körper und $P = K[y_1, \ldots, y_n]$ der Polynomring in den Unbestimmten $y_1, \ldots, y_n$ über K, so ist zum Beispiel entscheidbar, ob ein Polynom $f \in P$ in einem Ideal I von P enthalten ist. Ist dies der Fall, so kann f zudem auf eindeutige Weise in den Elementen einer Gröbnerbasis von I dargestellt werden. Neben solchen rein algebraischen Eigenschaften existieren auch Anwendungen in anderen Gebieten der Mathematik. So finden Gröbnerbasen auch Einsatz in der Kryptographie und Geometrie, etwa bei der Bestimmung des Verschwindungsideals einer Punktmenge.

Aufgrund ihrer vielfältigen Eigenschaften und der zur Verfügung stehenden Algorithmen besteht natürlich die Motivation, auch auf anderen algebraischen Strukturen eine Gröbnerbasistheorie zu entwickeln. So wollen wir in dieser Arbeit die Gröbnerbasistheorie auf eine Struktur erweitern, die eher analytischer Natur ist, den *differentiellen Polynomring*. Dazu versehen wir P mit einer sogenannten *Derivation*, d.h. mit einer Abbildung $\partial : P \longrightarrow P$, so dass für Polynome $f, g \in P$ die Regeln $\partial(f + g) = \partial(f) + \partial(g)$ und $\partial(fg) = \partial(f)g + f\partial(g)$ erfüllt sind. Für jedes $k \geq 0$ fassen wir dabei die Bilder von $y_1, \ldots, y_n$ unter ∂^k als zusätzliche Unbestimmte auf und schreiben $\partial^k(y_i) = y_i^{(k)}$. Wir erhalten mit $D = K[y_i^{(k)} \mid i = 1, \ldots, n,\ k \in \mathbb{N}_0]$ einen differentiellen Ring, der auch als $K\{y_1, \ldots, y_n\}$ notiert wird. Auf diese Weise lässt sich u.a. jede gewöhnliche polynomielle Differentialgleichung mit einem Element in D identifizieren. Das Vorhandensein einer Derivation erzwingt nun aber zunächst einen neuen Idealbegriff, um die Verträglich mit ∂ zu gewährleisten. Hierzu wird an ein Ideal I zusätzlich die Bedingung gestellt, dass es bzgl. ∂ abgeschlossen ist, d.h. dass mit jedem Polynom $f \in I$ auch $\partial(f)$ ein Element von I ist. Auf diese Weise erhalten wir mit I ein sogenanntes *differentielles Ideal*. Das Studium solcher Ideale aus algebraischer Sicht begann Mitte des letzten Jahrhunderts. J. Ritt war hierbei einer der Mitbegründer der Theorie der *charakteristischen Mengen* von differentiellen Idealen. Neben Ritt lieferte vor allem Kolchin in [13] die Grundlagen aller späteren Untersuchungen.

Bei der Entwicklung einer *differentiellen Gröbnerbasistheorie* werden wir u.a. den folgenden Fragen nachgehen:

- Was ist eine differentielle Gröbnerbasis eines differentiellen Ideals?
- Besitzt jedes differentielle Ideal eine differentielle Gröbnerbasis oder sogar eine endliche?

- Lassen sich alle Eigenschaften einer algebraischen Gröbnerbasis auf differentielle Gröbnerbasen übertragen?
- Wie kann eine differentielle Gröbnerbasis berechnet werden?
- Welche Anwendungen gibt es speziell für differentielle Gröbnerbasen?

Für die Beantwortung der obigen Fragen werden wir thematisch wie folgt vorgehen: In Kapitel 1 fassen wir zunächst die wesentlichen Grundlagen der differentiellen Algebra zusammen. Besonderes Augenmerk fällt dabei auf die bereits angesprochene Theorie der charakteristischen Mengen und die Dimensionstheorie für differentielle Faktorringe des differentiellen Polynomrings D.

Im zweiten Kapitel studieren wir dann die Theorie der differentiellen Gröbnerbasen. Dies beinhaltet die Betrachtung differentieller Termordnungen sowie deren zugehörige Termersetzungssysteme. Für die Berechnung differentieller Gröbnerbasen geben wir schließlich eine differentielle Version des Buchberger-Algorithmus an.

Zum Abschluss stellen wir in Kapitel 3 ausgewählte Anwendungen der differentiellen Gröbnerbasistheorie dar. Dies umfasst Aussagen zur Eliminationstheorie und eine Berechnungsmethode für den Kern differentieller Algebrenhomomorphismen. Darüber hinaus befassen wir uns mit differentiellen Gleichungssystemen und Verschwindungsidealen endlicher Punktmengen. Letzteres werden wir auch unter numerischen Aspekten betrachten, um auch für gestörte Daten sinnvolle Ergebnisse zu erzielen.

Nach der kurzen Darstellung des Verlaufs dieser Arbeit wollen wir nun noch detaillierter auf unsere Ergebnisse eingehen. Hierzu ist es zunächst sinnvoll, den bisherigen Forschungsstand auf dem Gebiet der differentiellen Polynomringe anzusprechen. Grundlage dessen sind zumeist sogenannte *Rankings*, also Ordnungen auf der Menge der Derivate $\mathbb{D}^n = \{y_i^{(k)} \mid i = 1, \ldots, n,\ k \geq 0\}$, die mit der Derivation ∂ des differentiellen Polynomrings D verträglich sind. Letzteres ist erfüllt, falls für Derivate $u, v \in \mathbb{D}^n$ mit $u < v$ auch $\partial(u) < \partial(v)$ gilt. Mit Hilfe solcher Rankings definiert Ritt eine Pseudo-Reduktion auf D. Für zwei Polynome $f, g \in D$ heißt dabei f pseudo-reduzibel bzgl. g, falls für ein $k \in \mathbb{N}_0$ die k-te Derivation des bzgl. eines Rankings größten Derivats in g, den sogenannten *Leader* von g, in f vorkommt. In diesem Fall ergibt sich für geeignete $f_1, f_2 \in D$ ein Polynom $f_1 f - f_2 \partial^k(g)$, dessen Leader kleiner oder gleich dem Leader von f ist, wobei im Falle der Gleichheit der Leader zu einer echt kleineren Potenz vorkommt.

In diesem Zusammenhang nennen wir eine Teilmenge G eines differentiellen Ideals $I \subseteq D$ eine *differentielle Pseudo-Gröbnerbasis* von I, falls jedes Element von I bzgl. eines Polynoms $g \in G$ pseudo-reduzibel ist. Fordern wir zusätzlich, dass jedes $g_1 \in G$ bzgl. jedem $g_2 \in G \backslash \{g_1\}$ nicht pseudo-reduzibel ist, so erhalten wir Ritts Begriff der charakteristischen Menge. Bestimmen lassen sich solche Mengen bisher nur für differentielle Prim- und Radikalideale von D. Mit ihnen kann algorithmisch die Radikalzugehörigkeit getestet werden, aber weitere typische Eigenschaften einer Gröbnerbasis weisen sie nicht auf. Charakteristische Mengen sind weder Erzeugendensysteme der Ideale, noch liefern sie eine eindeutige Darstellung der Elemente von I. Ritts Ansatz ist für unsere Ziele daher nicht geeignet.

Im Jahre 1987 gab Carrà-Ferro eine erste konkrete Definition einer differentiellen Gröbnerbasis an (siehe [5]). Sie beschränkte sich dabei jedoch auf lexikographische Termordnungen. Allgemeinere Ansätze lieferten dagegen Ollivier (1990) und Zobnin (2005). Entscheidend für eine sinnvolle Definition einer differentiellen Gröbnerbasis sind die Bedingungen, die an *differentielle Termordnungen* gestellt werden, also an geeignete Termordnungen auf der Menge der Terme $\mathbb{T}^n$ in D. Wir fordern hier lediglich, dass die Einschränkung der Termordnung auf $\mathbb{D}^n$ zusätzlich ein Ranking definiert, und erhalten auf diese Weise eine Verallgemeinerung der Termordnungsbegriffe in [18] und [29]. Jede solche differentielle Termordnung σ liefert bereits eine Wohlordnung auf $\mathbb{T}^n$ und damit zu jeder Polynommenge $G \subseteq D\backslash\{0\}$ ein Termersetzungssystem. Existiert zu einem Polynom $f \in D$ ein $g \in G$ und ein $k \in \mathbb{N}_0$, so dass der Leitterm von $\partial^k(g)$ ein Teiler des Leitterms $\mathrm{LT}_\sigma(f)$ von f ist, so heißt f reduzibel bzgl. g und wir erhalten mit $f - ct\partial^k(g)$ für ein geeignetes $c \in K$ und einen Term $t \in \mathbb{T}^n$ ein Restpolynom mit einem echt kleineren Leitterm als f. Da jedes solche Termersetzungssystem noethersch ist, kann jedem Polynom f eine Normalform zugeordnet werden, also ein Polynom, das bzgl. G nicht weiter reduziert werden kann. Diese Normalform ist aber im Allgemeinen nicht eindeutig. Für eine Teilmenge G eines differentiellen Ideals ist die Eindeutigkeit nun gerade dann garantiert, wenn die Menge der Leitterme der Polynome $\partial^k(g)$ mit $g \in G$ und $k \in \mathbb{N}_0$ das Leittermideal $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I\backslash\{0\}\rangle$ von I erzeugt. Die letzte Bedingung an G kommt formal der Definition einer algebraischen Gröbnerbasis sehr nahe. Ein solches G erfüllt also mit der Eindeutigkeit der Normalform bereits eine der typischen Eigenschaften einer Gröbnerbasis, und daher nennen wir in diesem Fall G eine *differentielle Gröbnerbasis* von I. Dass diese Definition auch berechtigt ist, zeigt eine Verallgemeinerung des Begriffs der Standardbasis für Ideale bzgl. einer Filtrierung auf D (siehe Abschnitt 2.3). Für die Gröbner-Filtrierung liefert diese gerade unsere Definition einer differentiellen Gröbnerbasis.

In Abschnitt 2.4 weisen wir weiter nach, dass bzgl. einer differentiellen Gröbnerbasis G eines differentiellen Ideals $I \subseteq D$ ein Polynom $f \in D$ genau dann zu Null reduziert, wenn es ein Element von I ist. Damit lässt sich für ein Polynom die Idealzugehörigkeit entscheiden und im Fall $f \in I$ eine eindeutige Darstellung in den Elementen $\partial^k(g)$ mit $g \in G$ und $k \in \mathbb{N}_0$ angeben. Für eine solche Darstellung $f = \sum_{i=1}^s f_i \partial^{k_i}(g_i)$ mit $f_i \in D$, $g_i \in G$ und $k_i \in \mathbb{N}_0$ für $i = 1, \ldots, s$ gilt insbesondere $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(f_i \partial^{k_i}(g_i))$ für jedes $i \in \{1, \ldots, s\}$.

Bis auf eine sind also alle wesentlichen Eigenschaften einer Gröbnerbasis erfüllt. Eine differentielle Gröbnerbasis eines differentiellen Ideals ist zwar immer zugleich ein differentielles Erzeugendensystem des Ideals, jedoch ist zunächst unklar, ob es auch stets eine endliche gibt. Leider lässt sich die generelle Existenz einer endlichen differentiellen Gröbnerbasis direkt ausschließen, da der differentielle Polynomring nicht noethersch ist und damit nicht jedes differentielle Ideal von D ein endliches differentielles Erzeugendensystem besitzt. Daher beschränken wir uns hier auf endlich erzeugte differentielle Ideale, auch hinsichtlich des Einsatzes von Computeralgebrasystemen, in denen nur mit endlichen Mengen gearbeitet werden kann. Aber auch für solche Ideale ist die Existenz einer endlichen differentiellen Gröbnerbasis nicht gesichert. Nichts desto trotz können wir ein differentielles Analogon zum Buchberger-Algorithmus angeben, das von ausgewählten S-Polynomen die Normalform bestimmt und diese ggf. zum aktuellen Erzeugendensystem hinzufügt. Dabei liefert für $G = \{g_1, \ldots, g_s\}$ jedes Paar $((i,k),(j,l)) \in (\{1,\ldots,n\} \times \mathbb{N}_0)^2$ mit $(i,k) \neq (j,l)$ das zugehörige S-Polynom $\frac{t_{(i,k),(j,l)}}{\mathrm{LM}_\sigma(\partial^k(g_i))}\,\partial^k(g_i) - \frac{t_{(i,k),(j,l)}}{\mathrm{LM}_\sigma(\partial^l(g_j))}\,\partial^l(g_j)$, wobei $t_{(i,k),(j,l)} = \mathrm{kgV}(\mathrm{LT}_\sigma(\partial^k(g_i)), \mathrm{LT}_\sigma(\partial^l(g_j)))$ und $\mathrm{LM}_\sigma(f)$ für jedes $f \in D\backslash\{0\}$ das Leitmonom von f bezeichnet. Das Buchberger-Kriterium besagt nun, dass G genau dann eine differentielle Gröbnerbasis von I ist, wenn jedes solche S-Polynom bzgl. G zu Null reduziert. Da es aber unendlich viele S-Polynome gibt, die im Allgemeinen auch nicht durch die üblichen Kriterien vermieden werden können, terminiert der oben beschriebene Algorithmus nur in besonders günstigen Fällen.

Für *strikt stabile* differentielle Termordnungen lassen sich hingegen genauere Aussagen über die Existenz endlicher differentieller Gröbnerbasen treffen. Hierzu fordern wir wie in [18] und [29] zusätzlich, dass für Terme $t_1, t_2 \in \mathbb{T}^n$ mit $t_1 <_\sigma t_2$ auch $\mathrm{LT}_\sigma(\partial(t_1)) <_\sigma \mathrm{LT}_\sigma(\partial(t_2))$ erfüllt ist. Für solche Termordnungen zeigen wir, dass sich für differentielle Ideale I, die eine endlich differentielle Gröbnerbasis besitzen, genau $n - \dim(D/I)$ Polynome in I finden lassen, deren Leitterme Derivate von paarweise verschiedenen differentiellen Unbestimmten sind. Hierbei bezeichnet die Zahl $\dim(D/I)$ die Dimension des differentiellen Faktorrings D/I, die sich algorithmisch mit Hilfe differentieller Pseudo-Gröbnerbasen berechnen lässt (siehe Abschnitt 1.8). Für differentielle Ideale I mit $\dim(D/I) = 0$ gilt sogar die Umkehrung der obigen Folgerung. D.h. existieren in I genau n solcher Polynome, so auch eine endliche differentielle Gröbnerbasis.

Auch für die praktische Berechnung von differentiellen Gröbnerbasen bringt die Verwendung strikt stabiler differentieller Termordnungen Vorteile mit sich. So ist es vor allem nicht notwendig, alle S-Polynome zu bestimmen. Es genügt die Betrachtung der S-Polynome zu sogenannten *fundamentalen* Paaren, d.h. zu Paaren $((i,k),(j,l))$, so dass für alle $\tilde{k}, \tilde{l}, m \in \mathbb{N}_0$ der Term $\partial^m(t_{(i,\tilde{k}),(j,\tilde{l})})$ kein Teiler von $t_{(i,k),(j,l)}$ ist. Es stellt sich dabei heraus, dass es zwischen zwei Polynomen entweder unendlich viele oder genau ein fundamentales Paar gibt. Zudem finden wir weitere Kriterien zur Vermeidung unnötiger fundamentaler Paare, die in einer neuen Version des differentiellen Buchberger-Algorithmus zur Anwendung kommen. Mit dieser sind wir in der Lage, für jedes null-dimensionale differentielle Ideal in endlich vielen Schritten eine endliche differentielle Gröbnerbasis zu bestimmen, falls eine solche existiert. Für höhere Dimensionen berechnet die Prozedur zwar eine differentielle Gröbnerbasis, es fehlt jedoch ein geeignetes Abbruchkriterium. In diesem Zusammenhang klassifizieren wir die differentiellen Ideale, für die unsere Prozedur terminiert, anhand der Gestalt ihrer reduzierten differentiellen Gröbnerbasis.

In Abschnitt 3.1 beschreiben wir, wie mit differentiellen Gröbnerbasen differentielle Eliminationsideale bestimmt werden können. Hierzu verwenden wir sogenannte *differentielle Eliminationsordnungen*, d.h. differentielle Termordnungen σ, die für eine bestimmte Menge L von differentiellen Unbestimmten stets $y >_\sigma \tilde{y}$ erfüllt, falls $y \in L$ und $\tilde{y} \notin L$ ist. Die differentielle Version des Hauptsatzes der Eliminationstheorie besagt dann, dass für eine differentielle Gröbnerbasis G von I bzgl. einer differentiellen Eliminationsordnung für $L \subseteq \{y_1, \dots, y_n\}$ die Menge $G \cap K\{y_i \mid i = 1, \dots, n, y_i \notin L\}$ eine differentielle Gröbnerbasis des Ideals $I \cap K\{y_i \mid i = 1, \dots, n, y_i \notin L\}$ bildet. Für ausgewählte σ und L können wir mit dem differentiellen Buchberger-Algorithmus sogar eine solche differentielle Gröbnerbasis berechnen, falls diese endlich ist.

Mit den obigen Überlegungen lässt sich auch der Kern eines differentiellen K-Algebrenhomomorphismus φ bestimmen. Da jede endlich erzeugte differentielle K-Algebra von der Form $K\{y_1, \dots, y_n\}/I$ für ein differentielles Ideal I ist, können wir φ auffassen als $\varphi : K\{y_1, \dots, y_n\}/I_1 \longrightarrow K\{z_1, \dots, z_m\}/I_2$ mit differentiellen Idealen I_1, I_2 und mit $\varphi(y_i + I_1) = f_i + I_2$ für $i = 1, \dots, n$ und gewissen $f_1, \dots, f_n \in K\{z_1, \dots, z_m\}$. Ist J das von $\{y_1 - f_1, \dots, y_n - f_n\}$ und I_2 differentiell erzeugte Ideal, so erhalten wir mit dem Bild von $J \cap K\{y_1, \dots, y_n\}$ in $K\{y_1, \dots, y_n\}/I_1$ den Kern von φ. Zur Bestimmung des Ideals $J \cap K\{y_1, \dots, y_n\}$ können wir dabei eine differentielle Eliminationsordnung für $L = \{z_1, \dots, z_m\}$ verwenden. Auf diese Weise lassen sich z.B. alle differentiellen Relationen zwischen Polynomen aus $K[z_1, \dots, z_m]$ berechnen.

Um für eine gegebene Polynommenge $\{f_1, \dots, f_s\} \subseteq D$ bzw. für das von $\{f_1, \dots, f_s\}$ differentiell erzeugte Ideal I alle gemeinsamen Nullstellen $a \in K^n$ zu bestimmen, wobei wir hier auch $\partial^k(f_i)(a) = 0$ für alle $k \geq 0$ fordern, genügt es, alle Nullstellen des Ideals $I \cap K[y_1, \dots, y_n]$ zu berechnen und diese zu testen. Dies ist aber nur dann möglich, wenn es endlich viele solcher Nullstellen gibt. Und Letzteres ist genau dann der Fall, wenn I null-dimensional ist und Ordnung Null besitzt (siehe Abschnitt 3.3).

Umgekehrt ist auch von Interesse, zu einer gegebenen endlichen Punktmenge diejenigen Polynome $f \in D$ zu bestimmen, für die $\partial^k(f)$ für jedes $k \geq 0$ an allen Punkten verschwindet. Eine direkte Übertragung des Buchberger-Möller-Algorithmus auf den differentiellen Fall liefert dazu das gewünschte Ergebnis. In diesem Zusammenhang befassen wir uns auch mit der folgenden Fragestellung: Sind die Werte von unendlich oft differenzierbaren, reellen Funktionen $\varphi_1, \dots, \varphi_n$ an Stellen $x_1, \dots, x_s \in \mathbb{R}$ bis zu einer festen Ordnung $N \in \mathbb{N}_0$ bekannt, wie kann dann das Verschwindungsideal von $\varphi_1, \dots, \varphi_n$ aus diesen Daten bestmöglich approximiert werden? Dazu passen wir den differentiellen Buchberger-Möller-Algorithmus geeignet an und berechnen so für jedes $m \in \mathbb{N}_0$ mit $m \leq N$ alle Polynome $f \in K[y_i^{(j)} \mid i = 1, \dots, n, 0 \leq j \leq m]$, für die $f, \partial(f), \dots, \partial^{N-m}(f)$ an den gegebenen Punkten verschwinden.

Schließlich betrachten wir die beschriebene Problemstellung unter dem Gesichtspunkt, dass es sich bei den gegebenen Werten um gestörte, also nicht exakte Daten handelt. Unter Verwendung verschiedener numerischer Methoden geben wir dazu Algorithmen an, die möglichst einfache Relationen liefern, die an den gestörten Daten „beinahe“ verschwinden.

An dieser Stelle möchte ich mich vor allem bei Herrn Prof. Dr. M. Kreuzer für die sehr gute Betreuung und die interessanten Diskussionen bedanken.

Außerdem danke ich meiner Familie, insbesondere meiner Frau Ina, die mir in der arbeitsreichen Zeit stets liebevoll und unterstützend zur Seite stand.

Kapitel 1

Grundlagen

In diesem Kapitel befassen wir uns mit den Grundlagen der *differentiellen Algebra*. Diese beschäftigt sich mit algebraischen Strukturen, die unter einer Derivation abgeschlossen sind. Der Schwerpunkt liegt dabei auf der Theorie der differentiellen Polynomringe und deren Ideale.

Ihre Anfänge hatte die differentielle Algebra zu Beginn des 20. Jahrhunderts. So lieferte Riquier 1910 als Erster einen algebraischen Ansatz für die Untersuchung von Systemen partieller Differentialgleichungen. Dazu wird eine Differentialgleichung als ein Element eines Polynomrings aufgefasst, in dem für jede Unbestimmte auch deren Derivationen definiert sind, sogenannte *Derivate*. Auf diese Weise lässt sich die Lösungsmenge eines Systems als Nullstellenmenge eines Ideals interpretieren. Dies war Motivation genug, solche Ideale umfassend zu studieren. Als Standardwerke gelten hierbei die Arbeiten von Kolchin ([13]) und Ritt ([21]). Diese beschäftigen sich insbesondere mit der Theorie der *charakteristischen Mengen*, die als ein differentielles Analogon zur Gröbnerbasistheorie angesehen werden kann. Aktuelle Forschungsergebnisse hierzu finden sich in [1] bzw. [2] sowie in [11] und [24].

Wir beginnen zunächst mit einer Darstellung der grundlegenden Aussagen über differentielle Ringe und Ideale, bevor wir im zweiten Abschnitt speziell auf differentielle Polynomringe eingehen. Hierauf folgt ein kurzer Einblick in die differentielle Geometrie, insbesondere die differentielle Version des Hilbertschen Nullstellensatzes.

Im vierten Abschnitt widmen wir uns dann speziellen Ordnungen auf der Menge der Derivate, den sogenannten *Rankings*. Diese bilden die Grundlage für die Einführung eines Pseudo-Reduktionssystems im darauffolgenden Abschnitt, welches wiederum zum Begriff der differentiellen Pseudo-Gröbnerbasis führt. Letzerer kann als eine sinnvolle Verallgemeinerung des Begriffs der charakteristischen Menge angesehen werden, wobei sich die Eigenschaften größtenteils übertragen lassen. Hierzu zählen u.a. der Radikalzugehörigkeitstest und die Berechnung von Eliminationsidealen für differentielle Primideale.

Der letzte Abschnitt befasst sich schließlich mit der Dimension eines differentiellen Faktorrings und deren algorithmische Berechnung.

1.1 Differentielle Ringe

In diesem Abschnitt wollen wir kurz die wichtigsten Fakten aus der differentiellen Ringtheorie darlegen, die wir für unsere folgenden Untersuchungen benötigen. Wir beginnen dabei mit einer algebraischen Definition einer Derivation, einem Begriff, der ursprünglich nur im Gebiet der Analysis vorzufinden ist. In Ringen, die mit einer solchen Abbildung versehen sind, werden dann im Wesentlichen Ideale studiert, die bzgl. der Derivation abgeschlossen sind, sogenannte *differentielle Ideale*. Für diese Ideale lassen sich nun analoge Aussagen zu denen der klassischen Algebra treffen.

Im Folgenden bezeichnen R, S stets Ringe, I, J Ideale und K, L Körper. Dabei verstehen wir unter einem Ring immer einen kommutativen Ring mit Eins.

Definition 1.1.1. Sei R ein Ring. Eine Abbildung $\partial : R \longrightarrow R$ heißt *Derivation*, falls für alle $a, b \in R$ gilt

i) $\partial(a + b) = \partial(a) + \partial(b)$,
ii) $\partial(a \cdot b) = a \cdot \partial(b) + \partial(a) \cdot b$.

Für die k-fache Konkatenation

$$\partial^k(a) = (\underbrace{\partial \circ \ldots \circ \partial}_{k})(a)$$

schreiben wir auch kurz $\partial^k a$ oder $a^{(k)}$, wobei k eine nicht-negative ganze Zahl ist. Dabei sei $a^{(0)} = a$.

Für die algebraischen Strukturen Ring und Körper lassen sich nun entsprechende differentielle Strukturen definieren. Hierfür benötigen wir lediglich die Existenz einer geeigneten Derivation.

Definition 1.1.2. Sei R ein Ring und $\partial : R \longrightarrow R$ eine Derivation.

1) Das Paar (R, ∂) heißt ein *differentieller Ring*. Ist klar, welche Derivation gemeint ist, so schreiben wir auch einfach R. Ein Teilring $S \subseteq R$ heißt *differentieller Teilring* von (R, ∂), falls $\partial(s) \in S$ gilt für alle $s \in S$.
2) Ist K ein Körper und $\delta : K \longrightarrow K$ eine Derivation, so heißt (K, δ) ein *differentieller Körper*. Ein Teilkörper $L \subseteq K$ heißt *differentieller Teilkörper* von K, falls L ein differentieller Teilring von K ist. Dann heißt K auch *differentieller Oberkörper* oder *differentielle Körpererweiterung* von L.
3) Ein Element a eines differentiellen Rings (R, ∂), das die Gleichung $\partial(a) = 0$ erfüllt, heißt *Konstante*. Die Menge aller Konstanten von R bezeichnen wir mit R_0.

Der Begriff des differentiellen Rings kann auch als Verallgemeinerung des Ringbegriffs angesehen werden. Denn wählen wir als Derivation die Nullabbildung, die die Bedingungen aus Definition 1.1.1 trivialerweise erfüllt, so wird jeder Ring zu einem differentiellen Ring.

Bemerkung 1.1.3. Sei R ein differentieller Ring und K ein differentieller Körper.

a) Die Menge R_0 aller Konstanten von R bildet einen differentiellen Teilring von R. Denn für Elemente $a, b \in R_0$ gilt $\partial(a+b) = \partial a + \partial b = 0$ bzw. $\partial(ab) = a\partial b + b\partial a = 0$. Entsprechend ist K_0 ein differentieller Teilkörper von K.
b) Der Teilkörper $K_0 \subseteq K$ umfasst wegen $\partial(1) = \partial(1 \cdot 1) = 1 \cdot \partial(1) + \partial(1) \cdot 1 = 2\partial(1)$ stets den Primkörper von K.

Beispiel 1.1.4. Die $\mathbb{Q}$-lineare Abbildung $\partial : \mathbb{Q}[t] \longrightarrow \mathbb{Q}[t]$ mit $\partial t = 1$ ist eine Derivation. Also ist $(\mathbb{Q}[t], \partial)$ ein differentieller Ring mit $\mathbb{Q}[t]_0 = \mathbb{Q}$.

Definition 1.1.5. Sei (R, ∂) ein differentieller Ring.

1) Ein Ideal $I \subseteq R$ heißt *differentielles Ideal* von R, falls für jedes $f \in I$ auch ∂f ein Element von I ist.
2) Für eine Teilmenge $G \subseteq R$ bezeichne

$$\langle G \rangle_\partial = \{ \sum_{g \in G} \sum_{i \in \mathbb{N}_0} f_{gi} g^{(i)} \mid \text{ nur endlich viele } f_{gi} \in R \text{ ungleich Null} \}$$

das von G *differentiell erzeugte* differentielle Ideal von R. Ist I ein differentielles Ideal von R und gilt $\langle G \rangle_\partial = I$, so heißt G ein *differentielles Erzeugendensystem* von I.

Ist I ein differentielles Ideal von (R, ∂), so induziert ∂ durch $\partial(r + I) = \partial(r) + I$ eine Derivation auf dem zugehörigen Faktorring R/I. Damit ist auch R/I ein differentieller Ring.

Ein differentielles Ideal, welches zudem ein Primideal bzw. maximales Ideal ist, heißt differentielles Primideal bzw. maximales differentielles Ideal. Auch die üblichen Idealoperation lassen sich problemlos übertragen.

Satz 1.1.6. *Seien I, J differentielle Ideale von R und $h \in R$.*

a) Die Mengen $I + J$ und $I \cap J$ bilden differentielle Ideale von R.
b) Gilt $\mathbb{Q} \subseteq R$, so ist das Radikal von I ein differentielles Ideal von R.
c) Ist I ein differentielles Primideal, so gilt $\sqrt{I} = I$.
d) Der Durchschnitt beliebig vieler differentieller Radikalideale von R ist wieder ein differentielles Radikalideal von R.
e) Die Mengen $I : J$, $I : J^\infty$ und $I : h^\infty$ sind differentielle Ideale von R.

Beweis. In a) ist nur zu zeigen, dass die Mengen mit jedem Element auch dessen Derivation enthält. Für $I \cap J$ ist dies offensichtlich erfüllt. Sei also $f \in I + J$, d.h. $f = g + h$ für ein $g \in I$ und ein $h \in J$. Wegen $\partial g \in I$ und $\partial h \in J$ folgt direkt $\partial f = \partial g + \partial h \in I + J$.

Für den Beweis von b) sei $f^i \in I$ für ein $f \in R$ und ein $i \in \mathbb{N}$. Wir zeigen zunächst mit Induktion nach j, dass für $j \in \{1, \ldots, i\}$ das Element $f^{i-j}(\partial f)^{2j-1}$ in I enthalten ist. Für $j = i$ folgt dann $(\partial f)^{2i-1} \in I$, also $\partial f \in \sqrt{I}$. Für $j = 1$ ergibt sich direkt

$f^{i-1}\partial f = \frac{1}{i}\partial f^i \in I$. Sei jetzt $j > 1$ und die Behauptung für $k = j-1$ erfüllt. Durch Derivation und Multiplikation mit ∂f erhalten wir mit

$$\partial(f)\partial(f^{i-(j-1)}(\partial f)^{2(j-1)-1}) = (i-j+1)f^{i-j}(\partial f)^{2j-1} + (2j-3)f^{i-(j-1)}(\partial f)^{2(j-1)-1}\partial^2 f$$

ein Element von I. Da der rechte Summand nach Induktionsvoraussetzung in I liegt, gilt dies auch für den ersten.

Um e) zu zeigen, sei zunächst $f \in I : J$, d.h. für jedes $g \in J$ gilt $fg \in I$. Dann liegt auch $\partial(f)g = \partial(fg) - f\partial g$ in I und damit ∂f in $I : J$. Analog folgt aus $fg^i \in I$ für ein $i \geq 0$ sofort $\partial(f)g^{i+1} = \partial(fg^i)g - ifg^i\partial g \in I$.

Die Beweise der Aussagen c) und d) verlaufen analog zu denen aus der kommutativen Algebra unter Verwendung von a). □

Lemma 1.1.7. *Sei R ein differentieller Ring mit $\mathbb{Q} \subseteq R$, $I \subseteq R$ ein differentielles Ideal und seien $f_1, \ldots, f_m \in R$.*

a) Gilt $f_1f_2 \in \sqrt{I}$, so folgt $f_1^{(k_1)}f_2^{(k_2)} \in \sqrt{I}$ für alle $k_1, k_2 \in \mathbb{N}_0$.
b) Es gilt $\sqrt{I + \langle f_1 \cdots f_m\rangle_\partial} = \sqrt{I + \langle f_1\rangle_\partial} \cap \cdots \cap \sqrt{I + \langle f_m\rangle_\partial}$.

Beweis. Für den Beweis von a) sei $f_1f_2 \in \sqrt{I}$. Da $\sqrt{I}$ ein differentielles Ideal ist, ist auch $f_1\partial(f_1f_2) = f_1f_1^{(1)}f_2 + f_1^2f_2^{(1)}$ ein Element in $\sqrt{I}$, also $f_1^2f_2^{(1)} \in \sqrt{I}$. Dann enthält $\sqrt{I}$ auch das Element $f_1^2(f_2^{(1)})^2$ und damit $f_1f_2^{(1)}$, woraus direkt $f_1^{(1)}f_2 = \partial(f_1f_2) - f_1f_2^{(1)} \in \sqrt{I}$ folgt. Für $\tilde{f}_2 = f_2^{(1)}$ lässt sich nun die obige Überlegung auf das Element $f_1\tilde{f}_2$ anwenden, und wir erhalten $f_1f_2^{(2)} \in \sqrt{I}$. Sukzessive ergibt sich demnach $f_1f_2^{(k_1)} \in \sqrt{I}$. Damit ist auch $f_1^{(1)}f_2^{(k_1)}$ im Radikal von I und schließlich $f_1^{(k_1)}f_2^{(k_2)} \in \sqrt{I}$.

Um b) zu zeigen, genügt es den Fall $m = 2$ zu betrachten. Offensichtlich ist die Inklusion $\subseteq$ erfüllt. Sei also $f \in \sqrt{I + \langle f_1\rangle_\partial} \cap \sqrt{I + \langle f_2\rangle_\partial}$. Dann existieren Elemente $g_1, g_2 \in I$, $\tilde{f}_1 \in \langle f_1\rangle_\partial$, $\tilde{f}_2 \in \langle f_2\rangle_\partial$ und $i_1, i_2 \in \mathbb{N}$ mit $f^{i_1} = g_1 + \tilde{f}_1$ und $f^{i_2} = g_2 + \tilde{f}_2$. Die Elemente $\tilde{f}_1$ und $\tilde{f}_2$ lassen sich nun schreiben als $\tilde{f}_1 = \sum_{i=0}^{k_1} h_i f_1^{(i)}$ bzw. $\tilde{f}_2 = \sum_{i=0}^{k_2} \tilde{h}_i f_2^{(i)}$ für gewisse $h_1, \ldots, h_{k_1}, \tilde{h}_1, \ldots, \tilde{h}_{k_2} \in R$ und $k_1, k_2 \in \mathbb{N}_0$. Mit a) ergibt sich für das Produkt

$$\tilde{f}_1\tilde{f}_2 = \sum_{\substack{i=0,\ldots,k_1 \\ j=0,\ldots,k_2}} h_i\tilde{h}_j f_1^{(i)}f_2^{(j)} \in \sqrt{\langle f_1f_2\rangle_\partial}.$$

Es gilt nun $f^{i_1+i_2} = g_1g_2 + g_1\tilde{f}_2 + g_2\tilde{f}_1 + \tilde{f}_1\tilde{f}_2 \in I + \sqrt{\langle f_1f_2\rangle_\partial} \subseteq \sqrt{I + \langle f_1f_2\rangle_\partial}$. Dann ist aber auch $f \in \sqrt{I + \langle f_1f_2\rangle_\partial}$ und die Behauptung bewiesen. □

Abschließend gilt es noch, Homomorphismen zwischen differentiellen Ringen zu erklären. Ein differentieller Ringhomomorphismus sollte natürlich die differentielle Struktur eines differentiellen Rings erhalten, d.h. eine Verträglichkeit mit der entsprechenden Derivation gewährleisten.

Definition 1.1.8. Seien (R, ∂) und (S, δ) differentielle Ringe. Ein Ringhomomorphismus $\varphi : R \longrightarrow S$ heißt *differentieller Ringhomomorphismus*, falls für alle $r \in R$ die Bedingung $\varphi(\partial r) = \delta(\varphi(r))$ erfüllt ist.

Der Kern eines differentiellen Ringhomomorpismus $\varphi : R \longrightarrow S$ ist als Teilmenge von R_0 offensichtlich ein differentielles Ideal von R und das Bild von φ ein differentieller Unterring von S.

1.2 Der differentielle Polynomring

Nachdem die grundlegenden Begriffe aus der differentiellen Algebra erklärt wurden, wollen wir uns nun mit Polynomringen über differentiellen Körpern beschäftigen. Diese sollten in natürlicher Weise wieder differentielle Ringe ergeben. In Folge dessen ist auch für jede Unbestimmte eine Derivation zu erklären. Dabei ist es wiederum vernünftig zu verlangen, dass auch die Elemente der Menge $\{\partial^k y \mid k \geq 0, y \text{ ist Unbestimmte}\}$ wieder algebraisch unabhängig über dem Grundkörper sind. Ein solcher *differentieller Polynomring* entspricht also einem Polynomring mit unendlich vielen Unbestimmten.

In [13] und [21] wurde bereits eine umfassende Theorie über differentielle Ideale von differentiellen Polynomringen entwickelt. Einige der wesentlichen Aussagen werden wir hier aufführen. Dazu gehört zum Beispiel die Existenz einer Primidealzerlegung von differentiellen Radikalidealen oder auch Raudenbushs Basissatz. Letzterer ist vergleichbar mit dem Hilbertschen Basissatz aus der klassischen Algebra. Er besagt, dass für jedes differentielle Ideal I eines differentiellen Polynomrings endlich viele Polynome existieren, deren differentielles Erzeugnis das gleiche Radikale wie I besitzt. Leider ist eine stärkere Aussage hier nicht möglich, da der differentielle Polynomring nicht noethersch ist.

Im Folgenden sei K stets ein differentieller Körper der Charakteristik Null mit Derivation ∂.

Definition 1.2.1. Seien $y_1, \ldots, y_n$ Unbestimmte mit $n \in \mathbb{N}$ und die Elemente der Menge $\mathbb{D}^n = \{y_i^{(k)} \mid i \in \{1, \ldots, n\}, k \in \mathbb{N}_0\}$ algebraisch unabhängig über K. Dann lässt sich die Derivation ∂ auf den Polynomring $K[\mathbb{D}^n]$ durch $\partial(y_i^{(k)}) = y_i^{(k+1)}$ fortsetzen.

1) Der differentielle Ring $K[\mathbb{D}^n]$ heißt der *gewöhnliche differentielle Polynomring* über K in den *differentiellen Unbestimmten* $y_1, \ldots, y_n$ und wird mit D notiert. Seine Elemente heißen *differentielle Polynome*, die Elemente von $\mathbb{D}^n$ *Derivate*.
2) Ein differentielles Polynom t der Form $t = u_1^{k_1} \cdots u_m^{k_m}$ mit $u_1, \ldots, u_m \in \mathbb{D}^n$ und $k_1, \ldots, k_m \in \mathbb{N}$ heißt *differentieller Term*. Die Menge aller differentiellen Terme sei mit $\mathbb{T}^n$ bezeichnet.
3) Ist $f \in D \backslash \{0\}$ ein differentielles Polynom mit der Darstellung $f = \sum_{i=1}^m c_i t_i$, wobei $c_i \in K \backslash \{0\}$ und $t_i \in \mathbb{T}^n$ für $i = 1, \ldots, m$, so heißt die Menge $\{t_1, \ldots, t_m\}$ der *Träger* von f und wird mit $\operatorname{Supp}(f)$ notiert. Als *differentiellen Träger* von f bezeichnen wir die Menge $\mathbb{D}(f) = \{u \in \mathbb{D}^n \mid u \text{ teilt } t \text{ für ein } t \in \operatorname{Supp}(f)\}$.

Der Begriff „gewöhnlich“ dient hierbei der Unterscheidung von D und dem Polynomring $K[y_1, \ldots, y_n]$ versehen mit den partiellen Derivationen $\frac{\partial}{\partial y_1}, \ldots, \frac{\partial}{\partial y_n}$. Da letzterer in dieser Arbeit keine weitere Erwähnung findet, sprechen wir im Weiteren nur noch vom differentiellen Polynomring D.

Definition 1.2.2. Sei $t = u_1^{k_1} \cdots u_m^{k_m}$ ein differentieller Term mit $u_1, \ldots, u_m \in \mathbb{D}^n$ und $k_1, \ldots, k_m \in \mathbb{N}$. Weiter sei $f \in D\backslash\{0\}$ ein differentielles Polynom mit der Darstellung $f = \sum_{i=1}^m c_i t_i$, wobei $c_i \in K\backslash\{0\}$ und $t_i \in \mathbb{T}^n$ für $i = 1, \ldots, m$.

1) Für ein Derivat $y_i^{(k)} \in \mathbb{D}^n$ mit $i \in \{1, \ldots, n\}$ und $k \geq 0$ heißt die Zahl $\operatorname{ord}(y_i^{(k)}) = k$ die *Ordnung* von $y_i^{(k)}$. Die Zahl $\operatorname{ord}(f) = \max\{\operatorname{ord}(u) \mid u \in \mathbb{D}(f)\}$ heißt dann die *Ordnung* von f. Für eine Teilmenge $G \subseteq D$ und ein $k \in \mathbb{N}_0$ bezeichne G_k die Menge aller Elemente von G mit Ordnung kleiner oder gleich k.
2) Die Zahl $w(t) = \operatorname{ord}(u_1)k_1 + \cdots + \operatorname{ord}(u_m)k_m$ heißt das *Gewicht* von t und entsprechend $w(f) = \max\{w(t) \mid t \in \operatorname{Supp}(f)\}$ heißt das *Gewicht* von f.
3) Die Zahl $\deg(t) = k_1 + \cdots + k_m$ heißt wie üblich der *Grad* von t und entsprechend $\deg(f) = \max\{\deg(t_i) \mid i = 1, \ldots, m\}$ der *Grad* von f.

Für jedes Polynom $f \in D\backslash K$ besitzen f und ∂f offensichtlich denselben Grad. Das Gewicht hingegen erhöht sich bei Derivation. Genauer lassen sich folgende Eigenschaften festhalten.

Lemma 1.2.3. *Sei $t \in \mathbb{T}^n$ ein differentieller Term und $f \in D\backslash K$ ein differentielles Polynom.*

a) Es ist $\partial f \in D\backslash K$.
b) Alle differentiellen Terme in $\operatorname{Supp}(\partial t)$ haben dasselbe Gewicht, und für jeden differentiellen Term $\tilde{t} \in \operatorname{Supp}(\partial t)$ gilt $w(\tilde{t}) = w(t) + 1$.
c) Es gilt $w(\partial f) = w(f) + 1$.

Beweis. Für den Beweis von a) sei $y_i^{(k)} \in \mathbb{D}(f)$ mit $i \in \{1, \ldots, n\}$. Dabei sei $k \in \mathbb{N}_0$ maximal gewählt, d.h. y_i kommt in f höchstens zur Ordnung k vor. Wir schreiben nun f als Polynom in $y_i^{(k)}$ mit Koeffizienten, die y_i höchstens zur Ordnung $k-1$ enthalten, d.h. $f = \sum_{j=0}^d f_j (y_i^{(k)})^j$ mit $f_0, \ldots, f_d \in D$ und $f_d \neq 0$. Dann ist $df_d \neq 0$ der Koeffizient von $(y_i^{(k)})^{d-1} y_i^{(k+1)}$ in ∂f, also $\partial f \notin K$.

Jeder differentielle Term $\tilde{t}$ aus dem Träger von ∂t ergibt sich durch Streichen eines Derivats $u \in \mathbb{D}(t)$ in t und Multiplikation von ∂u. Daher erhalten wir für das Gewicht von $\tilde{t}$ den Wert $w(\tilde{t}) = w(t) - \operatorname{ord}(u) + \operatorname{ord}(\partial u) = w(t) + 1$ und damit b).

Um c) zu zeigen, schreiben wir f als $f = f_1 + f_2$ mit $f_1, f_2 \in D$, wobei f_1 genau die differentiellen Terme von f mit Gewicht $w(f)$ umfasst. Nach a) gilt nun $\partial f_1 \notin K$ und mit b) folgt $w(\partial f_1) = w(f_1) + 1 = w(f) + 1$. Wegen $w(\partial f) = w(\partial f_1)$ ergibt sich daraus die Behauptung. □

Im Weiteren wollen wir uns detaillierter mit differentiellen Idealen des differentiellen Polynomrings D beschäftigen. Dabei stellt sich zunächst die Frage, ob in unserer Situation ein Analogon zum Hilbertschen Basissatz existiert, d.h. ob jedes solche Ideal ein endliches differentielles Erzeugendensystem besitzt. Wie wir bereits erwähnt haben, ist dies leider nicht der Fall. Betrachten wir zum Beispiel das von $\{y^2, (\partial y)^2, (\partial^2 y)^2, \ldots\}$ differentiell erzeugte Ideal I von $\mathbb{Q}\{y\}$, so kann es für I wegen $(\partial^k y)^2 \notin \langle y^2, \ldots, (\partial^{k-1} y)^2 \rangle_\partial$

für jedes $k \geq 1$ kein endliches differentielles Erzeugendensystem geben. Einen Ausweg liefert schließlich ein anderer Erzeugendenbegriff.

Definition 1.2.4. Sei $I \subseteq D$ ein differentielles Ideal. Eine Teilmenge $F \subseteq I$ heißt *differentielles Radikalerzeugendensystem* von I, falls gilt $\sqrt{I} = \sqrt{\langle F \rangle_\partial}$.

Jedes differentielle Ideal $I \subseteq D$ besitzt offensichtlich ein differentielles Radikalerzeugendensystem, denn $F = I$ erfüllt trivialerweise die obige Bedingung. Dass jedoch stets ein endliches differentielles Radikalerzeugendensystem existiert, besagt der nun folgende Basissatz.

Theorem 1.2.5 (Raudenbushs Basissatz)**.**
Jedes differentielle Ideal von D besitzt ein endliches differentielles Radikalerzeugendensystem.

Beweis. Siehe [21], Kapitel I.12. □

Eine typische Folgerung des obigen Basissatzes ist hingegen die Aussage, dass eine aufsteigende Kette entsprechender Ideale stets stationär wird.

Korollar 1.2.6. *Jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq \cdots$ von differentiellen Radikalidealen von D wird stationär.*

Beweis. Sei $I_1 \subseteq I_2 \subseteq \cdots$ eine aufsteigende Kette von differentiellen Radikalidealen von D. Dann ist $I = \bigcup_{i \in \mathbb{N}} I_i$ offensichtlich wieder ein differentielles Radikalideal von D, welches nach obigem Theorem ein endliches differentielles Radikalerzeugendensystem $F \subseteq I$ besitzt. Da F endlich ist, existiert ein Index $j \in \mathbb{N}$, so dass für alle $k \geq j$ die Polynommenge F in I_k enthalten ist. Dann gilt $F \subseteq I_k \subseteq I = \sqrt{\langle F \rangle_\partial}$ und, da I_k ein Radikalideal ist, sogar $I_k = \sqrt{\langle F \rangle_\partial}$. Die Kette der Ideale wird also stationär. □

Schließlich existiert für jedes differentielle Radikalideal I auch eine Primidealzerlegung, d.h. es gibt differentielle Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ von D, so dass gilt $I = \bigcap_{i=1}^r \mathfrak{p}_i$.

Theorem 1.2.7 (Primidealzerlegung differentieller Radikalideale)**.**
Jedes differentielle Radikalideal $I \subseteq D$ ist Durchschnitt endlich vieler differentieller Primideale von D.

Beweis. Sei $I \subseteq D$ ein differentielles Radikalideal. Angenommen, I besitzt keine Zerlegung in differentielle Primideale. Dann ist I insbesondere kein Primideal, d.h. es existieren differentielle Polynome $f, g \in D \backslash I$ mit $fg \in I$. Nach Lemma 1.1.7 b) ist das differentielle Ideal I also der Durchschnitt der differentiellen Radikalideale $I_1 = \sqrt{I + \langle f \rangle_\partial}$ und $J_1 = \sqrt{I + \langle g \rangle_\partial}$. Nach Voraussetzung können nun nicht beide Ideale eine Zerlegung wie oben besitzen. O.B.d.A. besitze I_1 keine solche Zerlegung. Da auch I_1 demnach nicht prim ist, ist es wieder der Durchschnitt zweier Radikalideale, von denen mindestens eines nicht in Primideale zerlegbar ist. Wir erhalten auf diese Weise eine unendliche, echt aufsteigende Kette $I \subset I_1 \subset I_2 \subset \cdots$ von differentiellen Idealen von D im Widerspruch zu Korollar 1.2.6. □

1.3 Der differentielle Nullstellensatz

In diesem Abschnitt wollen wir einen kurzen Einblick in die Grundlagen der *differentiellen Geometrie* geben. Wie die algebraische beschäftigt sich auch die differentielle Geometrie mit Nullstellenmengen von Polynomen und Idealen, jedoch unter Berücksichtigung der zugrundeliegenden Derivation. Hierbei verstehen wir unter einer Nullstelle eines Polynoms $f \in K\{y_1, \ldots, y_n\}$ ein Element $(a_1, \ldots, a_n) \in L^n$ für einen differentiellen Oberkörper L von K, so dass f im Kern des differentiellen Einsetzhomomorphismus $D \longrightarrow L$, $y_i \mapsto a_i$ liegt. Es wird also jedes Derivat $y_i^{(k)} \in \mathbb{D}(f)$ durch das entsprechende Element $a^{(k)}$ ersetzt.

Umgekehrt lässt sich für eine Menge $\mathbb{X}$ von Punkten aus L^n auch das zugehörige Verschwindungsideal studieren. Dabei macht es Sinn, von einem differentiellen Ideal zu sprechen, da mit jeder Komponente eines Punktes aus $\mathbb{X}$ auch deren Derivationen gegeben sind.

Zu den zentralen Aussagen zählt schließlich auch der Nullstellensatz für differentielle Ideale, der exakt dem algebraischen Resultat entspricht.

Definition 1.3.1. Sei $K \subseteq L$ eine differentielle Körpererweiterung.

1) Ein Element $(a_1, \ldots, a_n) \in L^n$ heißt eine *Nullstelle* eines differentiellen Polynoms $f \in D$ in L^n, falls $f(a_1, \ldots, a_n) = 0$ gilt. Die Menge aller Nullstellen von f in L^n sei mit $\mathcal{Z}_L(f)$ bezeichnet. Für die Menge aller Nullstellen von f in allen möglichen differentiellen Erweiterungen L von K schreiben wir $\mathcal{Z}(f)$.
2) Ist $F \subseteq D$ ein Menge von Polynomen, so ist die *Nullstellenmenge* von F in L^n definiert als die Menge

$$\mathcal{Z}_L(F) = \{(a_1, \ldots, a_n) \in L^n \mid f(a_1, \ldots, a_n) = 0 \text{ für alle } f \in F\}.$$

   Für die Vereinigung aller Nullstellenmengen von F in allen möglichen differentiellen Erweiterungen L von K schreiben wir $\mathcal{Z}(F)$.
3) Ist $\mathbb{X}$ eine Teilmenge von K^n, so heißt das differentielle Ideal

$$\mathcal{I}(\mathbb{X}) = \{f \in D \mid f(a) = 0 \text{ für alle } a \in \mathbb{X}\}$$

   das *Verschwindungsideal* von $\mathbb{X}$.

Das Verschwindungsideal von $\mathbb{X} \subseteq K^n$ ist in der Tat ein differentielles Ideal, denn für jedes Polynom $f \in D$ mit $f(a) = 0$ gilt auch $(\partial f)(a) = \partial(f(a)) = 0$.

Bemerkung 1.3.2. Sei $\mathbb{X}$ eine Teilmenge von K^n.

a) Das Ideal $\mathcal{I}(\mathbb{X}) \cap K[y_1, \ldots, y_n]$ ist gerade das algebraische Verschwindungsideal von $\mathbb{X}$ in $K[y_1, \ldots, y_n]$.
b) Mit a) folgt zugleich, dass $\mathbb{X}$ genau dann endlich ist, wenn das Ideal $\mathcal{I}(\mathbb{X}) \cap K[y_i]$ für $i = 1, \ldots, n$ von $\{0\}$ verschieden ist. Siehe dazu auch [14], Proposition 3.7.1.

Ist $F \subset D_0$ ein Erzeugendensystem von $\mathcal{I}(\mathbb{X})_0 = \mathcal{I}(\mathbb{X}) \cap D_0$, so gilt insbesondere $\langle F \rangle_\partial \subseteq \mathcal{I}(\mathbb{X})$. Hierbei kann im Allgemeinen keine Gleichheit angenommen werden. Denn zum Beispiel ist $\mathcal{I}(\mathbb{X})_0 = \{0\} \subset \mathbb{Q}[y]$ das algebraische Verschwindungsideal der Menge $\mathbb{X} = \mathbb{Q}$, aber $y^{(1)} \in \mathcal{I}(\mathbb{X})$ offensichtlich kein Element von $\langle \mathcal{I}(\mathbb{X})_0 \rangle_\partial = \{0\}$.

Die üblichen Gesetzmäßigkeiten für Nullstellenmengen und Verschwindungsideale in Bezug auf Idealoperationen behalten hingegen auch im differentiellen Fall ihre Gültigkeit.

Lemma 1.3.3. *Seien $I_1, I_2 \subseteq D$ differentielle Ideale und F eine Teilmenge von D.*

a) Aus $I_1 \subseteq I_2$ folgt $\mathcal{Z}(I_2) \subseteq \mathcal{Z}(I_1)$.
b) Es gilt $\mathcal{Z}(I_1 + I_2) = \mathcal{Z}(I_1) \cap \mathcal{Z}(I_2)$ und $\mathcal{Z}(I_1 \cap I_2) = \mathcal{Z}(I_1 I_2) = \mathcal{Z}(I_1) \cup \mathcal{Z}(I_2)$.
c) Es ist $\mathcal{Z}(I_1) = \mathcal{Z}(\sqrt{I_1})$.
d) Es gilt $\mathcal{Z}(F) = \mathcal{Z}(\langle F \rangle_\partial)$.
e) Ist F ein differentielles Radikalerzeugendensystem von I_1, so gilt $\mathcal{Z}(F) = \mathcal{Z}(I_1)$.

Beweis. Die Beweise für a)–d) entsprechen exakt denen aus der algebraischen Geometrie und e) folgt aus c) bzw. d). □

Nach der letzten Aussage des Lemmas existiert also zu jedem differentiellen Ideal eine endliche Teilmenge von Polynomen mit derselben Nullstellenmenge.

Lemma 1.3.4. *Seien $\mathbb{X}_1$ und $\mathbb{X}_2$ Teilmengen von K^n.*

a) Aus $\mathbb{X}_1 \subseteq \mathbb{X}_2$ folgt $\mathcal{I}(\mathbb{X}_2) \subseteq \mathcal{I}(\mathbb{X}_1)$.
b) Es ist $\mathcal{I}(\mathbb{X}_1)$ ein differentielles Radikalideal.

Beweis. Jedes Polynom $f \in \mathcal{I}(\mathbb{X}_2)$ erfüllt $f(a) = 0$ für alle $a \in \mathbb{X}_2$, also insbesondere für die Elemente aus $\mathbb{X}_1$, d.h. $f \in \mathcal{I}(\mathbb{X}_1)$. Und ist $f^k \in \mathcal{I}(\mathbb{X}_1)$ für ein $k \geq 1$, so gilt wegen $f^k(a) = (f(a))^k = 0$ auch $f(a) = 0$ für jedes $a \in \mathbb{X}_1$. □

Schließlich ergibt sich das differentielle Analogon zum Hilbertschen Nullstellensatz.

Theorem 1.3.5 (Differentieller Nullstellensatz)**.**
Ist $I \subseteq D$ ein differentielles Ideal, so gilt $\mathcal{I}(\mathcal{Z}(I)) = \sqrt{I}$. Insbesondere ist für jedes echte differentielle Ideal I die zugehörige Nullstellenmenge nicht leer.

Beweis. Siehe [21], Kapitel II.7. □

1.4 Rankings

Eines der wichtigsten Probleme der algebraischen und der differentiellen Idealtheorie ist das Idealzugehörigkeitsproblem. Dieses beschäftigt sich mit der Frage, wie sich entscheiden lässt, ob ein Polynom $f \in D$ in einem (differentiellen) Ideal $I \subseteq D$ enthalten ist. Algebraisch liefert die Gröbnerbasistheorie eine adäquate Lösungsmethode. Ein zentraler Punkt dabei ist eine Anordnung aller Terme anhand von Termordnungen. Im differentiellen Fall bedarf es dafür zunächst einer Ordnung der Derivate in $\mathbb{D}^n$.

Als Erster führte Riquier ([21]) solche *Rankings* ein, als totale Ordnungen auf $\mathbb{D}^n$, die mit der jeweiligen Derivation verträglich sind. D.h. die Derivation eines Derivats führt immer zu einem echt größeren Derivat und für $u, v \in \mathbb{D}^n$ mit $u < v$ gelte auch $\partial u < \partial v$. Eine vollständige Klassifizierung aller Rankings über eine geeignete Darstellung durch Matrizen ist in [27] zu finden. Später verallgemeinerte Rust die Definition eines Rankings, indem er die Bedingung $u < \partial u$ für jedes $u \in \mathbb{D}^n$ nicht verlangte. Eine Klassifizierung dieser Ordnungen stellt er in [23] dar.

Rankings sind insbesondere Wohlordnungen auf $\mathbb{D}^n$. Diese Eigenschaft wird oftmals der entscheidende Punkt für die Gültigkeit einiger Aussagen im nächsten Abschnitt sein.

Für jedes Polynom lässt sich zudem das bzgl. einem Ranking größte Derivat auszeichnen. Dieses sogenannte *Leitderivat* übernimmt die Rolle des Leitterms eines Polynoms bzgl. einer Termordnung und wird im Weiteren von besonderer Bedeutung sein.

Im Folgenden bezeichnet $\mathbb{D}^n$ wieder die Menge aller Derivate des differentiellen Polynomrings $D = K\{y_1, \ldots, y_n\}$.

Definition 1.4.1. Eine totale Ordnung τ auf der Menge der Derivate $\mathbb{D}^n$ heißt *Ranking* auf $\mathbb{D}^n$, falls gilt

1) $u <_\tau \partial u$ für alle $u \in \mathbb{D}^n$,
2) $u_1 <_\tau u_2$ impliziert $\partial u_1 <_\tau \partial u_2$ für alle $u_1, u_2 \in \mathbb{D}^n$.

Ein Ranking τ auf $\mathbb{D}^n$ heißt *ordentlich*, falls zusätzlich gilt

3) $\mathrm{ord}(u_1) < \mathrm{ord}(u_2)$ impliziert $u_1 <_\tau u_2$ für alle $u_1, u_2 \in \mathbb{D}^n$.

Die durch die Bedingungen 1) und 2) definierten Rankings heißen in der Literatur auch *Riquier-Rankings*.

Beispiel 1.4.2. Die Ordnungen

$$y_1 < \partial y_1 < \partial^2 y_1 < \cdots < y_2 < \partial y_2 < \cdots < y_n < \partial y_n < \cdots$$

und

$$y_1 < y_2 < \cdots < y_n < \partial y_1 < \partial y_2 < \cdots < \partial y_n < \partial^2 y_1 < \cdots$$

definieren offensichtlich Rankings auf $\mathbb{D}^n$.

Satz 1.4.3. *Ist τ ein Ranking auf $\mathbb{D}^n$, so wird jede absteigende Kette $u_1 \geq_\tau u_2 \geq_\tau \cdots$ von Derivaten aus $\mathbb{D}^n$ stationär.*

Beweis. Angenommen, es existiert eine absteigende Kette $u_1 \geq_\tau u_2 \geq_\tau \cdots$ von Derivaten aus $\mathbb{D}^n$, die nicht stationär wird. Für jedes $i \in \{1, \ldots, n\}$ sei $(u_{ij})_{j\in\mathbb{N}}$ diejenige Teilfolge von $(u_k)_{k\in\mathbb{N}}$, die alle Derivate u_k mit $u_k = y_i^{(l)}$ für ein $l \in \mathbb{N}_0$ umfasst. Da die Kette $u_1 \geq_\tau u_2 \geq_\tau \cdots$ nicht stationär wird, müssen die Elemente mindestens einer dieser Teilfolgen ebenfalls eine absteigende Kette bilden, die nicht stationär wird. O.B.d.A. sei dies für $i = 1$ der Fall. Wir schreiben die entsprechende Kette als $y_1^{(k_1)} \geq_\tau y_1^{(k_2)} \geq_\tau \cdots$ mit $k_1, k_2, \ldots \in \mathbb{N}_0$. Nach Definition 1.4.1, 1) gilt dabei $k_1 \geq k_2 \geq \cdots$. Da die Menge der natürlichen Zahlen wohlgeordnet ist, wird diese Kette stationär, ein Widerspruch. □

Jedes Ranking τ auf $\mathbb{D}^n$ lässt sich nun wie folgt zu einer totalen Ordnung der Menge $\{u^d \mid u \in \mathbb{D}^n, d \in \mathbb{N}\}$ fortsetzen. Für Derivate $u_1, u_2 \in \mathbb{D}^n$ und $d_1, d_2 \in \mathbb{N}$ gelte dazu $u_1^{d_1} <_\tau u_2^{d_2}$ genau dann, wenn entweder $u_1 <_\tau u_2$ oder $u_1 = u_2$ und $d_1 < d_2$. Diese Konstruktion liefert sogar eine Wohlordnung auf der Menge $\{u^d \mid u \in \mathbb{D}^n, d \in \mathbb{N}\}$.

Korollar 1.4.4. *Ist τ ein Ranking auf $\mathbb{D}^n$, so wird jede absteigende Kette $t_1 \geq_\tau t_2 \geq_\tau \cdots$ von differentiellen Termen aus $\{u^d \mid u \in \mathbb{D}^n, d \in \mathbb{N}\}$ stationär.*

Beweis. Für jede absteigende Kette $u_1^{d_1} \geq_\tau u_2^{d_2} \geq_\tau \cdots$ mit Derivaten $u_1, u_2, \ldots \in \mathbb{D}^n$ und $d_1, d_2, \ldots \in \mathbb{N}_0$ erhalten wir die absteigende Kette $u_1 \geq_\tau u_2 \geq_\tau \cdots$, welche nach Satz 1.4.3 stationär wird. Da $\mathbb{N}$ wohlgeordnet ist, folgt daraus die Behauptung. $\square$

Definition 1.4.5. Sei τ ein Ranking auf $\mathbb{D}^n$, $f \in D \backslash \{0\}$ und $u \in \mathbb{D}^n$. Wir schreiben f als differentielles Polynom in $u \in \mathbb{D}^n$, d.h. $f = \sum_{i=0}^d f_i u^i$ mit $f_i \in D$, $f_d \neq 0$ und $u \notin \mathbb{D}(f_i)$ für $i = 0, \ldots, d$.

1) Die Zahl $\deg_u(f) = d$ heißt der *Grad* von f in u.
2) Das Derivat $\mathrm{LD}_\tau(f) = \max_\tau\{u \mid u \in \mathbb{D}(f)\}$ heißt das *Leitderivat* oder der *Leader* von f, $\mathrm{ldeg}_\tau(f) = \deg_{\mathrm{LD}_\tau(f)}(f)$ der *Leitgrad* von f und $\mathrm{LP}_\tau(f) = \mathrm{LD}_\tau(f)^{\mathrm{ldeg}_\tau(f)}$ die *Leitpotenz* von f. Ist $\mathrm{LD}_\tau(f) = y_i^{(k)}$ für ein $i \in \{1, \ldots, n\}$ und $k \geq 0$, so heißt $\mathrm{LV}_\tau(f) = y_i$ die *Leitvariable* von f.
3) Für $u = \mathrm{LD}_\tau(f)$ heißt $\mathrm{in}_\tau(f) = f_d$ das *Initial* von f und $\mathrm{sep}_\tau(f) = \sum_{i=1}^d i f_i u^{i-1}$ der *Separand* von f.

Genauso, wie wir den Begriff des Leitderivats mit dem des Leitterms identifizieren, kann das Initial als Analogon zum Leitkoeffizienten angesehen werden. Dabei ist das Initial von ∂f gerade der Separand von f und das Leitderivat von ∂f die Derivation des Leitderivats von f. Genauer gelten die folgenden Rechenregeln.

Lemma 1.4.6. *Seien $f, g \in D \backslash \{0\}$ differentielle Polynome.*

a) Ist $f + g \neq 0$, so gilt $\mathrm{LD}_\tau(f+g) \leq_\tau \max_\tau\{\mathrm{LD}_\tau(f), \mathrm{LD}_\tau(g)\}$. Dabei gilt Gleichheit, falls $\mathrm{LD}_\tau(f) \neq \mathrm{LD}_\tau(g)$ oder $\mathrm{LD}_\tau(f) = \mathrm{LD}_\tau(g)$ und $\mathrm{in}_\tau(f) + \mathrm{in}_\tau(g) \neq 0$.
b) Es gilt $\mathrm{LD}_\tau(fg) = \max_\tau\{\mathrm{LD}_\tau(f), \mathrm{LD}_\tau(g)\}$.
c) Es gilt $\mathrm{LD}_\tau(\partial f) = \partial(\mathrm{LD}_\tau(f))$.
d) Für jedes $k \in \mathbb{N}$ gilt $\mathrm{sep}_\tau(f^{(k)}) = \mathrm{sep}_\tau(f) = \mathrm{in}_\tau(\partial f) = \mathrm{in}_\tau(f^{(k)})$.

Beweis. Die Aussage in a) ergibt sich aus $\mathrm{LD}_\tau(f+g) \in \mathbb{D}(f+g) \subseteq \mathbb{D}(f) \cup \mathbb{D}(g)$ und die in b) aus $\mathrm{LD}_\tau(fg) = \max_\tau\{\, u \mid u \in \mathbb{D}(f) \cup \mathbb{D}(g)\} = \max_\tau\{\mathrm{LD}_\tau(f), \mathrm{LD}_\tau(g)\}$.

Für den Beweis von c) fassen wir f als differentielles Polynom in $\mathrm{LD}_\tau(f)$ auf, d.h. $f = \sum_{i=0}^d f_i \,\mathrm{LD}_\tau(f)^i$ mit $d = \mathrm{ldeg}_\tau(f)$, $f_0, \ldots, f_d \in D$ und $f_d \neq 0$. Wir erhalten für die Derivation von f

$$\partial f = \sum_{i=0}^d \partial f_i \,\mathrm{LD}_\tau(f)^i + \sum_{i=1}^d i f_i \,\mathrm{LD}_\tau(f)^{i-1} \partial(\mathrm{LD}_\tau(f)).$$

Dabei ist $\mathbb{D}(\partial f) \subseteq \{\partial u \mid u \in \mathbb{D}(f)\} \cup \mathbb{D}(f)$, und für jedes $u \in \mathbb{D}(f)$ folgt mit den Eigenschaften 1) und 2) aus Definition 1.4.1 daher $\partial(\mathrm{LD}_\tau(f)) \geq_\tau \partial u$ direkt aus $\mathrm{LD}_\tau(f) \geq_\tau u$, also $\mathrm{LD}_\tau(\partial f) = \partial(\mathrm{LD}_\tau(f))$.

Um d) zu zeigen, schreiben wir $\partial f = \sum_{i=0}^{d} \partial f_i \, \mathrm{LD}_\tau(f)^i + \mathrm{sep}_\tau(f)\partial(\mathrm{LD}_\tau(f))$. Nach c) ist nun $\partial(\mathrm{LD}_\tau(f))$ das Leitderivat von ∂f bzgl. τ, also $\mathrm{sep}_\tau(f)$ das Initial von ∂f. Analog ist wegen $\partial^k(\mathrm{LD}_\tau(f)) = \mathrm{LD}_\tau(\partial^k f)$ dann auch $\mathrm{sep}_\tau(f)$ das Initial von $\partial^k f$ für alle $k \in \mathbb{N}$. Daraus ergibt sich schließlich $\mathrm{sep}_\tau(f^{(k)}) = \mathrm{in}_\tau(f^{(k+1)}) = \mathrm{sep}_\tau(f)$. □

Für jedes Ranking lässt sich auf der Menge D aller Polynome eine Ordnung definieren. In [21] ist diese Fortsetzung für das erste Ranking aus Beispiel 1.4.2 und in [13] für beliebige Rankings beschrieben. Verwendet wird dabei die durch ein Ranking τ induzierte Ordnung $<_\tau$ auf der Menge der Terme $\{u^d \mid u \in \mathbb{D}^n, d \in \mathbb{N}\}$. Für Polynome $f_1, f_2 \in D\backslash K$ gilt nun gerade $f_1 \prec_\tau f_2$, falls $\mathrm{LP}_\tau(f_1) <_\tau \mathrm{LP}_\tau(f_2)$ erfüllt ist. Zusätzlich wird vereinbart, dass jedes Element aus K bzgl. $\prec_\tau$ stets kleiner als jedes Polynom aus $D\backslash K$ ist.

1.5 Pseudoreduktion

Nach der Festlegung eines Ordnungsbegriffs schließt sich im Allgemeinen die Definition eines Reduktionssystems an, d.h. eine Menge von Regeln, die beschreiben, wie gewisse Bestandteile eines Polynoms durch kleinere bzgl. der gewählten Ordnung ersetzt werden können. Bei dem üblichen Termersetzungssystem der algebraischen Gröbnerbasistheorie kann zum Beispiel ein Term eines Polynoms $f \in K[x_1, \ldots, x_n]$, der ein Vielfaches des Leitterms eines anderen Polynoms $g \in K[x_1, \ldots, x_n]$ bzgl. einer Termordnung σ ist, durch $\mathrm{LT}_\sigma(g) - \frac{1}{\mathrm{LC}_\sigma(g)} g$ ersetzt werden. Im Fall eines Rankings entspricht der Leitterm eines Polynoms nun dem Leitderivat und der Leitkoeffizient gerade dem Initial. Da wir zusätzlich noch eine Derivation zur Verfügung haben, sollte sich also jedes Derivat in $\mathbb{D}(f)$ der Form $\partial^k(\mathrm{LD}_\tau(g))$ reduzieren lassen. Dies ist aber im Allgemeinen nur dann möglich, wenn das Polynom f zuvor mit dem Initial von g multipliziert wird. Wir erhalten auf diese Weise ein sogenanntes *Pseudo-Ersetzungssystem*. Zuerst wurde diese Vorgehensweise in [21] und [13] beschrieben.

Definition 1.5.1. Seien $f, g \in D\backslash\{0\}$, $G \subseteq D\backslash\{0\}$ und τ ein Ranking auf $\mathbb{D}^n$.

1) Ist $u \in \mathbb{D}(f)$ mit $u = \partial^k \mathrm{LD}_\tau(g)$, $d = \deg_u(f) \geq \mathrm{ldeg}_\tau(g^{(k)})$ für ein $k \in \mathbb{N}_0$ und $f = \sum_{i=0}^{d} f_i u^i$ mit $f_0, \ldots, f_d \in D$, $f_d \neq 0$, so sagen wir g *pseudo-reduziert* f *in einem Schritt zu*
$$\tilde{f} = \mathrm{in}_\tau(g^{(k)})f - f_d u^{d - \mathrm{ldeg}_\tau(g^{(k)})} g^{(k)}$$
und notieren dies mit $f \xrightarrow{g}_p \tilde{f}$.
2) Es bezeichne $\xrightarrow{G}_p$ den reflexiven und transitiven Abschluss von $\bigcup_{g \in G} \xrightarrow{g}_p$ und $\xleftrightarrow{G}$ die zugehörige Äquivalenzrelation. Die Relation $\xrightarrow{G}_p$ heißt auch *Pseudo-Ersetzungssystem*.

3) Ein Polynom f heißt *pseudo-reduzibel* bzgl. G, falls es ein Element $g \in G$ gibt, welches f pseudo-reduziert. Andernfalls heißt f *pseudo-reduziert* bzgl. G. Die Menge G heißt *pseudo-reduziert*, falls jedes $g \in G$ bzgl. $G \backslash \{g\}$ pseudo-reduziert ist. Ist $\partial^k(\mathrm{LD}_\tau(g)) \notin \mathbb{D}(f)$ für alle $g \in G$ und $k \geq 1$, so heißt f *partiell reduziert* bzgl. G.
4) Das Pseudo-Ersetzungssystem $\xrightarrow{G}_p$ heißt *noethersch*, falls es keine unendliche Pseudo-Reduktionskette $f_1 \xrightarrow{g_1}_p f_2 \xrightarrow{g_2}_p \cdots$ mit Polynomen $f_1, f_2, \ldots \in D\backslash\{0\}$ und $g_1, g_2, \ldots \in G$ gibt. Es heißt *konfluent*, falls für alle Polynome $f, f_1, f_2 \in D$ mit $f \xrightarrow{G}_p f_1$ und $f \xrightarrow{G}_p f_2$ ein $f_3 \in D$ existiert mit $f_1 \xrightarrow{G}_p f_3$ und $f_2 \xrightarrow{G}_p f_3$. Das Pseudo-Ersetzungssystem heißt *lokal konfluent*, falls für alle $f, f_1, f_2 \in D$ und $g_1, g_2 \in G$ mit $f \xrightarrow{g_1}_p f_1$ und $f \xrightarrow{g_2}_p f_2$ ein $f_3 \in D$ existiert mit $f_1 \xrightarrow{G}_p f_3$ und $f_2 \xrightarrow{G}_p f_3$. Ist $\xrightarrow{G}_p$ noethersch und konfluent, so heißt es auch *konvergent*.

In einem Pseudo-Reduktionsschritt wird der entsprechende Summand $\mathrm{in}_\tau(g^{(k)}) f_d u^d$ stets durch ein bzgl. $\prec_\tau$ echt kleineres Polynom ersetzt. Dies garantiert letztlich, wie wir noch genauer sehen werden, dass nur endlich viele solcher Ersetzungen möglich sind.

Sind die Leitderivate zweier Polynome Derivate derselben differentiellen Unbestimmten, so ist eines der beiden pseudo-reduzibel bzgl. dem anderen. Dies ist auch der Grund dafür, dass eine pseudo-reduzierte Menge von Polynomen höchstens n Elemente enthalten kann.

Satz 1.5.2. *Sei $G = \{g_1, \ldots, g_s\} \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge.*

a) Es ist $|G| \leq n$, und für alle $i, j \in \{1, \ldots, s\}$ mit $i \neq j$ gilt $\mathrm{LV}_\tau(g_i) \neq \mathrm{LV}_\tau(g_j)$.
b) Für jedes Polynom $g \in G$ ist das Initial und der Separand von g pseudo-reduziert bzgl. G.

Beweis. Um a) zu zeigen, seien $i, j \in \{1, \ldots, s\}$ mit $i \neq j$. Angenommen, es gilt nun $\mathrm{LV}_\tau(g_i) = \mathrm{LV}_\tau(g_j)$. O.B.d.A. sei dabei $\mathrm{ord}(\mathrm{LD}_\tau(g_i)) \geq \mathrm{ord}(\mathrm{LD}_\tau(g_j))$. Wäre in diesem Fall $\mathrm{ord}(\mathrm{LD}_\tau(g_i)) > \mathrm{ord}(\mathrm{LD}_\tau(g_j))$, dann wäre g_j pseudo-reduzierbar durch g_l im Widerspruch zur Pseudo-Reduziertheit von G. Es gelte also $\mathrm{ord}(\mathrm{LD}_\tau(g_i)) = \mathrm{ord}(\mathrm{LD}_\tau(g_j))$ und O.B.d.A. $\mathrm{ldeg}_\tau(g_j) \geq \mathrm{ldeg}_\tau(g_l)$. Dann ist g_j wieder pseudo-reduzierbar durch g_l, und wir erhalten erneut einen Widerspruch. Demnach ist $\mathrm{LV}_\tau(g_i) \neq \mathrm{LV}_\tau(g_j)$ und $|G|$ nach oben durch die Anzahl der differentiellen Unbestimmten beschränkt.

Ist G pseudo-reduziert, so ist für jedes $g \in G$ wegen $\mathbb{D}(\mathrm{in}_\tau(g)) \subseteq \mathbb{D}(\mathrm{sep}_\tau(g)) \subseteq \mathbb{D}(g)$ und wegen $\deg_u(\mathrm{in}_\tau(g)) \leq \deg_u(\mathrm{sep}_\tau(g)) \leq \deg_u(g)$ für alle $u \in \mathbb{D}(g)$ sowohl das Initial als auch der Separand von g pseudo-reduziert bzgl. $G\backslash\{g\}$. Da $\mathrm{LD}_\tau(g) \geq \mathrm{LD}_\tau(\mathrm{in}_\tau(g))$ und $\mathrm{LD}_\tau(g) \geq \mathrm{LD}_\tau(\mathrm{sep}_\tau(g))$ gilt mit $\deg_{\mathrm{LD}_\tau(g)}(\mathrm{in}_\tau(g)) \leq \deg_{\mathrm{LD}_\tau(g)}(\mathrm{sep}_\tau(g)) < \mathrm{ldeg}_\tau(g)$, sind $\mathrm{in}_\tau(g)$ und $\mathrm{sep}_\tau(g)$ auch bzgl. $\{g\}$ pseudo-reduziert, also insgesamt bgzl. G. $\square$

In einem Pseudo-Reduktionsschritt $f \xrightarrow{g}_p \tilde{f}$ wird das Polynom f mit dem Initial oder dem Separanden von g multipliziert, je nachdem, ob die Ordnung des zu reduzierenden Derivats u von f der Ordnung des Leitderivats von g entspricht oder größer ist. Für ein bzgl. G zu Null pseudo-reduzierbares Polynom f bedeutet dies, dass das Produkt von f

mit allen beteiligten Initials bzw. Separanden ein Element von $\langle G\rangle_\partial$ ist. Daher wird im Folgenden das Polynom $h_G = \prod_{g\in G} \mathrm{in}_\tau(g)\mathrm{sep}_\tau(g)$ von entscheidender Bedeutung sein.

Satz 1.5.3. *Sei τ ein Ranking auf $\mathbb{D}^n$ und $G \subseteq D\backslash\{0\}$.*

a) Das Pseudo-Ersetzungssystem $\xrightarrow{G}_p$ ist noethersch.
b) Für jedes $f \in D\backslash\{0\}$ mit $f \xrightarrow{G}_p 0$ gilt $f \in \langle G\rangle_\partial : h_G^\infty$.

Beweis. Für den Beweis von a) nehmen wir an, dass eine unendliche Pseudo-Reduktionskette $f_1 \xrightarrow{g_1}_p f_2 \xrightarrow{g_2}_p \cdots$ mit differentiellen Polynomen $f_1, f_2, \ldots \in D\backslash\{0\}$, $g_1, g_2, \ldots \in G$ existiert. In jedem Pseudo-Reduktionsschritt wird dabei das Auftreten eines Derivats u zu einer Potenz d eliminiert und durch differentielle Terme ersetzt, die das Derivat u höchstens zur Potenz $d-1$ enthalten. Für jedes $i \in \mathbb{N}$ sei nun u_i das im i-ten Reduktionsschritt pseudo-reduzierte Derivat und d_i dessen Potenz. Weiter sei u_{i_1} für ein $i_1 \in \mathbb{N}$ das Maximum all dieser Derivate bzgl. τ. In der Pseudo-Reduktion wird das Derivat u_{i_1} insgesamt höchstens d_{i_1}-mal pseudo-reduziert, d.h. es existiert ein Index $j \in \mathbb{N}$ mit $u_k <_\tau u_{i_1}$ für alle $k \geq j$. Bei der Betrachtung der verkürzten Pseudo-Reduktionskette $f_{j+1} \xrightarrow{g_{j+1}}_p f_{j+2} \xrightarrow{g_{j+2}}_p \cdots$ erhalten wir auf die gleiche Weise das Element $u_{i_2} = \max_\tau\{u_i \mid i \in \mathbb{N}, i \geq j+1\} <_\tau u_{i_1}$. Eine Iteration dieses Verfahrens ergibt eine unendliche, echt absteigende Kette $u_{i_1} >_\tau u_{i_2} >_\tau \cdots$ von Derivaten aus $\mathbb{D}^n$ im Widerspruch zu Satz 1.4.3.

Um b) zu zeigen, sei $f_1 \in D$ ein von Null verschiedenes Polynom mit $f_1 \xrightarrow{G}_p 0$. D.h. es gibt Polynome $g_1, \ldots, g_m \in G$ und $f_2, \ldots, f_m \in D\backslash\{0\}$ mit $f_1 \xrightarrow{g_1}_p f_2 \xrightarrow{g_2}_p \cdots \xrightarrow{g_m}_p 0$. Für jedes $i \in \{1, \ldots, m\}$ wird dabei im i-ten Pseudo-Reduktionsschritt f_i mit $\mathrm{in}_\tau(g_i)$ bzw. mit $\mathrm{sep}_\tau(g_i)$ multipliziert und ein Polynom $h_i g_i^{(k_i)}$ subtrahiert. Insgesamt ergibt sich also

$$\prod_{i=1}^{m} \mathrm{in}_\tau(g_i)^{n_i}\mathrm{sep}_\tau(g_i)^{m_i} f_1 = \sum_{i=1}^{m} \tilde{h}_i g_i^{(k_i)} \in \langle G\rangle_\partial$$

mit gewissen $n_i, m_i \in \mathbb{N}_0$ und $\tilde{h}_i \in D$ für $i = 1, \ldots, m$. Dann ist aber $h_G^k f$ ein Element von $\langle G\rangle_\partial$ für $k = \max\{n_i + m_i \mid i = 1, \ldots, m\}$ und damit $f \in \langle G\rangle_\partial : h_G^\infty$. □

Nach obigem Satz ist also jedes bzgl. G zu Null pseudo-reduzierbare Polynom ein Element des differentiellen Ideals $\langle G\rangle_\partial : h_G^\infty$. Leider ist die Umkehrung dieser Aussage im Allgemeinen nicht richtig. Betrachten wir zum Beispiel die Menge $G = \{y^2\}$, so ist das Einspolynom offensichtlich ein Element von $\langle G\rangle_\partial : h_G^\infty = \langle y^2\rangle_\partial : (2y)^\infty$, aber sicherlich pseudo-reduziert bzgl. G.

Zu jedem Element $f \in D\backslash\{0\}$ lässt sich nun ein bzgl. G pseudo-reduziertes Polynom $\tilde{f} \in D$ berechnen, für das $f \xrightarrow{G}_p \tilde{f}$ gilt. Der zugehörige Algorithmus ist, wie zu erwarten, an den Divisionsalgorithmus aus der kommutativen Algebra angelehnt. Auch hier hängt die Berechnung des Polynoms $\tilde{f}$ wieder von der Reihenfolge der Elemente in G ab, d.h. $\tilde{f}$ ist im Allgemeinen nicht eindeutig bestimmt.

Satz 1.5.4. *Seien $s \geq 1$ und $f, g_1, \ldots, g_s \in D\backslash\{0\}$. Wir betrachten die folgenden Instruktionen:*

1) *Seien $h = 1$, $g = f$ und $n_i = q_{i0} = 0$ für $i = 1, \ldots, s$.*
2) *Bestimme den kleinsten Index $i \in \{1, \ldots, s\}$, so dass gilt $u := \partial^k \operatorname{LD}_\tau(g_i) \in \mathbb{D}(g)$ und $\deg_u(g) \geq \operatorname{ldeg}_\tau(g_i^{(k)})$ für ein $k \in \mathbb{N}_0$. Existiert solch ein Index i, schreibe $g = \sum_{j=0}^{\deg_u(g)} f_j u^j$ mit $f_0, \ldots, f_{\deg_u(g)} \in D$ und*
   - *setze $q_{ij} = 0$ für $j = n_i + 1, \ldots, k$ und $n_i = k$, falls $k > n_i$,*
   - *ersetze q_{jl} durch $\operatorname{in}_\tau(g_i^{(k)}) q_{jl}$ für $j = 1, \ldots, s$ und $l = 0, \ldots, n_j$, sowie q_{ik} durch $q_{ik} + f_{\deg_u(g)} u^{\deg_u(g) - \operatorname{ldeg}_\tau(g_i^{(k)})}$,*
   - *ersetze h durch $h \cdot \operatorname{in}_\tau(g_i^{(k)})$,*
   - *ersetze g durch $\operatorname{in}_\tau(g_i^{(k)}) g - f_{\deg_u(g)} u^{\deg_u(g) - \operatorname{ldeg}_\tau(g_i^{(k)})} g_i^{(k)}$,*
   - *fahre mit 2) fort, falls $g \neq 0$.*
3) *Gib $(h, g, [q_{10}, \ldots, q_{1n_1}], \ldots, [q_{s0}, \ldots, q_{sn_s}])$ aus und stoppe.*

Dies ist ein Algorithmus, dessen Ausgabe die folgenden Bedingungen erfüllt:

a) *Es gilt $hf = g + \sum\limits_{i=1}^{s} \sum\limits_{j=0}^{n_i} q_{ij} g_i^{(j)}$.*
b) *Das differentielle Polynom g ist pseudo-reduziert bzgl. $\{g_1, \ldots, g_s\}$.*
c) *Es ist $\operatorname{LP}_\tau(hf) = \operatorname{LP}_\tau(f)$, und für jedes $i \in \{1, \ldots, s\}$, $j \in \{0, \ldots, n_i\}$ mit $q_{ij} \neq 0$ gilt $\operatorname{LP}_\tau(f) \geq_\tau \operatorname{LP}_\tau(q_{ij} g_i^{(j)})$.*

Beweis. Das Terminieren des Algorithmus ist nach Satz 1.5.3 gesichert. Zudem ist die Gleichung in a) offensichtlich zu jedem Zeitpunkt erfüllt.

Des Weiteren ist das Polynom g in der Ausgabe des Algorithmus pseudo-reduziert bzgl. $\{g_1, \ldots, g_s\}$, da entweder $g = 0$ gilt oder kein Derivat in $\mathbb{D}(g)$ existiert, welches Derivation eines der Leitderivate von $g_1, \ldots, g_s$ ist.

Es bleibt noch c) zu beweisen. Ist zu einem Zeitpunkt in Schritt 2) die Bedingung für einen Index i erfüllt, so gilt in diesem Fall $\operatorname{LP}_\tau(\operatorname{in}_\tau(g_i^{(k)})) <_\tau \operatorname{LP}_\tau(g)$ und $\operatorname{LP}_\tau(\operatorname{in}_\tau(g_i^{(k)}) g) = \operatorname{LP}_\tau(f_{\deg_u(g)} u^{\deg_u(g) - \operatorname{ldeg}_\tau(g_i^{(k)})} g_i^{(k)})$. Nach der Aktualisierung aller Parameter besitzt demnach g eine bzgl. τ echt kleinere Leitpotenz. Damit ergibt sich zugleich $\operatorname{LP}_\tau(\operatorname{in}_\tau(g_i^{(k)})) <_\tau \operatorname{LP}_\tau(f)$, d.h. die Polynome hf und f besitzen bzgl. τ dieselbe Leitpotenz. Ferner gilt auch $\operatorname{LP}_\tau(f) \geq_\tau \operatorname{LP}_\tau(f_{\deg_u(g)} u^{\deg_u(g) - \operatorname{ldeg}_\tau(g_i^{(k)})} g_i^{(k)})$ und daher $\operatorname{LP}_\tau(f) \geq_\tau \operatorname{LP}_\tau(q_{ik} g_i^{(k)})$. □

Das Element g in der Ausgabe des Algorithmus heißt der *differentielle Pseudo-Rest* von f bzgl. $\mathcal{G} = (g_1, \ldots, g_s)$, notiert als $\operatorname{PR}_{\tau,\mathcal{G}}(f)$.

Als Nächstes geben wir einen Algorithmus an, der für eine Menge $F \subseteq D$ von Polynomen eine pseudo-reduzierte Menge $G \subseteq \langle F \rangle_\partial$ berechnet, so dass jedes Element von F bzgl. G zu Null pseudo-reduziert.

Satz 1.5.5. *Sei $F = \{f_1, \dots, f_s\} \subseteq D$ und τ ein Ranking auf $\mathbb{D}^n$. Wir betrachten die durch die folgenden Instruktionen definierte Prozedur* `PseudoRed`(F)*:*

1) *Setze $G = F \backslash \{0\}$.*
2) *Sortiere die Elemente von G aufsteigend nach ihrer Leitpotenz bzgl. τ und erhalte $G = \{g_1, \dots, g_r\}$ für ein $r \in \mathbb{N}_0$. Setze $R = \emptyset$.*
3) *Für aufsteigendes $i = 1, \dots, r$ entferne g_i aus G, falls g_i bzgl. $\{g_1, \dots, g_{i-1}\}$ pseudo-reduzibel ist.*
4) *Berechne für jedes $f \in F\backslash\{0\}$ den differentiellen Pseudo-Rest $\tilde{f} = \mathrm{PR}_{\tau,\mathcal{G}}(f)$. Ist $\tilde{f} \neq 0$, so füge $\tilde{f}$ zu R hinzu.*
5) *Gilt $R = \emptyset$, gib G aus und stoppe. Sonst ersetze G durch $G \cup R$ und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten endet und eine pseudo-reduzierte Menge G ausgibt, für die $\langle G\rangle_\partial \subseteq \langle F\rangle_\partial \subseteq \langle G\rangle_\partial : h_G^\infty$ gilt und bzgl. der jedes Polynom $f \in F$ zu Null pseudo-reduziert.

Beweis. Wir zeigen zunächst die Korrektheit des Algorithmus. Da G zu Beginn mit $F\backslash\{0\}$ initialisiert wird und zu G in Schritt 5) nur Elemente aus $\langle F\rangle_\partial$ hinzugefügt werden, gilt auch am Ende $\langle G\rangle_\partial \subseteq \langle F\rangle_\partial$. Die zweite Inklusion ist wegen des Abbruchkriteriums im letzten Schritt erfüllt. Denn ist $R = \emptyset$, so pseudo-reduziert jedes $f \in F\backslash\{0\}$ bzgl. G zu Null. Mit Satz 1.5.3 b) folgt dann bereits $F \subseteq \langle G\rangle_\partial : h_G^\infty$, also $\langle F\rangle_\partial \subseteq \langle G\rangle_\partial : h_G^\infty$. Zudem ist G nach Schritt 3) stets pseudo-reduziert.

Um zu zeigen, dass der Algorithmus auch terminiert, setzen wir G_i als die aktuelle Menge G am Ende des i-ten Durchlaufs von Schritt 5). Angenommen, bei jedem Durchlauf gilt $R \neq \emptyset$. Für alle $i \geq 1$ sei $t_i = \min_\tau\{\mathrm{LP}_\tau(g) \mid g \in G_i\}$ und $g_i \in G_i$ mit $\mathrm{LP}_\tau(g_i) = t_i$. Dann gilt insbesondere $t_{i+1} \leq_\tau t_i$ für alle $i \geq 1$ und die absteigende Folge $(t_i)_{i\in\mathbb{N}}$ wird nach Korollar 1.4.4 stationär, d.h. es existiert ein Index $i_1 \in \mathbb{N}$ mit $t_k = t_{i_1}$ für alle $k > i_1$. Ist $|G_k| = 1$ für ein $k > i_1$, so sind wir fertig. Sonst betrachten wir für $i \geq i_1$ nun die Terme $\tilde{t}_i = \min_\tau\{\mathrm{LP}_\tau(g) \mid g \in G_i\backslash\{g_i\}\}$. Auch diese bilden eine absteigende Folge differentieller Terme, die stationär wird. Wegen $|G_i| \leq |F| + n$ für alle $i \geq 1$ endet dieses Verfahren nach endlich vielen Schritten. □

Im restlichen Teil dieses Abschnitts wollen wir noch einige wichtige Resultate zum Thema Pseudo-Reduktion anführen. Dazu betrachten wir zumeist eine pseudo-reduzierte Menge $G \subseteq D\backslash\{0\}$ bzw. das zugehörige differentielle Ideal $\langle G\rangle_\partial : h_G^\infty$. Differentielle Ideale, die sich derart darstellen lassen, heißen auch *regulär* und werden in den nächsten Abschnitten noch von Bedeutung sein.

Ist nun $G \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge, so lassen sich einige Eigenschaften des differentiellen Ideals $\langle G\rangle_\partial : h_G^\infty$ von D auf das Ideal $\langle G\rangle : h_G^\infty$ von D bzw. auf das Ideal $(\langle G\rangle : h_G^\infty) \cap K[\mathbb{D}(G)]$ übertragen, wobei wir mit $\mathbb{D}(G)$ die Menge aller Derivate bezeichnen, die in den differentiellen Polynomen aus G vorkommen. Die Grundlage dafür liefert der folgende Satz. Für nähere Details verweisen wir auf [22].

Satz 1.5.6 (Rosenfeld)**.** *Ist $G \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge, so ist jedes differentielle, bzgl. G partiell reduzierte Polynom $f \in \langle G\rangle_\partial : h_G^\infty$ in dem Ideal $\langle G\rangle : h_G^\infty$ von D enthalten.*

Beweis. Sei $f \in (\langle G\rangle_\partial : h_G^\infty)\backslash\{0\}$ ein bzgl. G partiell reduziertes differentielles Polynom und $G = \{g_1, \dots, g_s\}$ für ein $s \in \mathbb{N}$. Wir schreiben

$$h_G^k f = \sum_{i=1}^{s} f_i g_i + \sum_{j=1}^{r} h_j g_{i_j}^{(k_j)}$$

mit $r \in \mathbb{N}_0$, $f_1, \dots, f_s, h_j \in D$, $h_j \neq 0$, $i_j \in \{1, \dots, s\}$ und $k_j \in \mathbb{N}$ für $j = 1, \dots, r$. Gilt hierbei $r = 0$, so ist die Behauptung gezeigt. Ist $r > 0$, so sei $u \in \mathbb{D}^n$ das bzgl. τ größte Derivat in der Menge $\{\mathrm{LD}_\tau(g_{i_j}^{(k_j)}) \mid j = 1, \dots, r\}$ und d die maximale Potenz, zu der u in der obigen Darstellung von f vorkommt. O.B.d.A. gelte $u = \mathrm{LD}_\tau(g_{i_r}^{(k_r)})$. Da mit f auch $h_G^k f$ bzgl. G partiell reduziert ist, gilt $u \notin \mathbb{D}(h_G^k f)$. Durch Multiplikation der Gleichung mit $\mathrm{sep}_\tau(g_{i_r})^d$ und Substitution von $\mathrm{sep}_\tau(g_{i_r})u$ durch $\mathrm{sep}_\tau(g_{i_r})u - g_{i_r}^{(k_r)}$ erhalten wir die Gleichung

$$\mathrm{sep}_\tau(g_{i_r})^d h_G^k f = \sum_{i=1}^{s} \tilde{f}_i g_i + \sum_{j=1}^{r-1} \tilde{h}_j g_{i_j}^{(k_j)}$$

für gewisse $\tilde{f}_1, \dots, \tilde{f}_s, \tilde{h}_1, \dots, \tilde{h}_{r-1} \in D$. Auf die gleiche Weise lassen sich nun auch die restlichen $r - 1$ Summanden eliminieren und es ergibt sich $h_G^l f \in \langle G\rangle$ für ein $l \geq k$, also $f \in \langle G\rangle : h_G^\infty$. □

Lemma 1.5.7. *Sei $G \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge.*

a) Jedes Polynom $f \in (\langle G\rangle_\partial : h_G^\infty) \cap K[\mathbb{D}(G)]$ ist bzgl. G partiell reduziert.
b) Es gilt $(\langle G\rangle_\partial : h_G^\infty) \cap K[\mathbb{D}(G)] = (\langle G\rangle : h_G^\infty) \cap K[\mathbb{D}(G)]$.

Beweis. Ist $f \in (\langle G\rangle_\partial : h_G^\infty) \cap K[\mathbb{D}(G)]\backslash\{0\}$ ein bzgl. G nicht partiell reduziertes Polynom, so existiert ein Derivat $u \in \mathbb{D}(f) \subseteq \mathbb{D}(G)$ mit $u = \partial^k(\mathrm{LD}_\tau(g))$ für ein $g \in G$ und ein $k > 0$. Da es zugleich ein differentielles Polynom $\tilde{g} \in G$ mit $u \in \mathbb{D}(\tilde{g})$ geben muss, erhalten wir einen Widerspruch zur Pseudo-Reduziertheit von G und damit a).

Die Inklusion $\supseteq$ in b) ist offensichtlich erfüllt. Die andere folgt mit Satz 1.5.6 und der Aussage in a). □

Für pseudo-reduzierte Mengen $G \subseteq D\backslash\{0\}$ überträgt sich die Primidealeigenschaft des zugehörigen regulären differentiellen Ideals $\langle G\rangle_\partial : h_G^\infty$ auf das Ideal $\langle G\rangle : h_G^\infty$ von $K[\mathbb{D}(G)]$. Von größerer Bedeutung ist aber, dass hierfür auch die Umkehrung gilt.

Satz 1.5.8. *Ist $G \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge, so ist $\langle G\rangle_\partial : h_G^\infty$ genau dann ein Primideal von D, wenn $(\langle G\rangle : h_G^\infty) \cap K[\mathbb{D}(G)]$ ein Primideal von $K[\mathbb{D}(G)]$ ist.*

Beweis. Siehe [21], Kapitel V.1. □

Sowohl reguläre differentielle Ideale als auch die zugehörigen algebraischen Ideale sind insbesondere Radikalideale.

Satz 1.5.9 (Lazard)**.** *Ist $G \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge, so sind $\langle G\rangle_\partial : h_G^\infty$ und $\langle G\rangle : h_G^\infty$ Radikalideale von D.*

Beweis. siehe [2], Theorem 4.2. □

Schließlich lässt sich für ein reguläres differentielles Ideal I die Menge I_s aller Polynome der Ordnung kleiner oder gleich s wiederum als ein reguläres algebraisches Ideal auffassen.

Satz 1.5.10. *Sei τ ein ordentliches Ranking auf $\mathbb{D}^n$, $G \subseteq D\backslash\{0\}$ eine pseudo-reduzierte Menge und $s \geq \max\{\mathrm{ord}(g) \mid g \in G\}$. Dann gilt*

$$(\langle G\rangle_\partial : h_G^\infty) \cap D_s = \langle \partial^k g \mid g \in G, 0 \leq k \leq s - \mathrm{ord}(g)\rangle : h_G^\infty.$$

Beweis. Es genügt, die Inklusion $\subseteq$ zu zeigen. Sei dazu $f \in (\langle G\rangle_\partial : h_G^\infty) \cap D_s$ und $I = \langle \partial^k g \mid g \in G, 0 \leq k \leq s - \mathrm{ord}(g)\rangle : h_G^\infty$. Ist f bzgl. G partiell reduziert, so folgt bereits $f \in (\langle G\rangle : h_G^\infty) \cap D_s \subseteq I$ nach Satz 1.5.6. Ansonsten existiert ein bzgl. G pseudo-reduziertes Polynom $\tilde{f}$, so dass für gewisse $k, k_1, \ldots, k_s \in \mathbb{N}$, $k \geq 0$, $f_1, \ldots, f_s \in D_s$ und $g_1, \ldots, g_s \in G$ gilt $h_G^k f = \sum_{i=1}^s f_i g_i^{(k_i)} + \tilde{f}$. Wegen $\mathrm{ord}(f) \leq s$ ist dabei $\mathrm{ord}(g_i^{(k_i)}) \leq s$ für $i = 1, \ldots, s$. Also ist mit $\tilde{f} \in (\langle G\rangle_\partial : h_G^\infty) \cap D_s$ auch f ein Element von I. □

Ein explizites Erzeugendensystem des Ideals $(\langle G\rangle_\partial : h_G^\infty) \cap D_s$ erhalten wir dabei zum Beispiel durch die Berechnung einer Gröbnerbasis des Ideals

$$\langle\{\partial^k g \mid g \in G, 0 \leq k \leq s - \mathrm{ord}(g)\} \cup \{h_G y - 1\}\rangle$$

von $D_s[y]$ bzgl. einer Eliminationsordnung für $\{y\}$, die mit dem Ranking τ verträglich ist.

1.6 Differentielle Pseudo-Gröbnerbasen

Mit der Festlegung eines Reduktionssystems ist zugleich ein obligatorischer Zugang zum Begriff der Gröbnerbasis verbunden. Denn für ein gegebenes differentielles Ideal $I \subseteq D$ lassen sich Teilmengen $G \subseteq I$ betrachten, bzgl. derer jedes Polynom in I zu Null reduziert. Da es sich in unserer Situation lediglich um ein Pseudo-Reduktionssystem handelt, werden wir solche Mengen auch als *Pseudo-Gröbnerbasen* bezeichnen. Diese Definition ist angelehnt an den Begriff der *charakteristischen Menge*. Kolchin bezeichnet so eine pseudo-reduzierte Menge G von Polynomen, so dass jedes $f \in I$ bzgl. G zu Null pseudo-reduziert, also eine Art *reduzierte* Pseudo-Gröbnerbasis. Die Theorie der charakteristischen Mengen ist sehr weit entwickelt, aber dennoch ein aktuelles Forschungsgebiet. Als Standardwerke gelten hierbei [13] und [21]. Dort finden sich auch erste Algorithmen zur Berechnung charakteristischer Mengen. Bestimmen lassen sich diese aber lediglich für differentielle Prim- und Radikalideale über die in Abschnitt 1.2 beschriebene Primidealzerlegung. Für das Radikal eines differentiellen Ideals I existieren darüber hinaus weitere Zerlegungsansätze. Der Rosenfeld-Gröbner-Algorithmus in [1] bzw. [2] berechnet eine Zerlegung in reguläre differentielle Ideale, d.h. pseudo-reduzierte Mengen $G_1, \ldots, G_r \subseteq D$ mit $\sqrt{I} = \bigcap_{i=1}^{r} (\langle G_i \rangle_\partial : h_{G_i}^\infty)$. Ist G_i zusätzlich eine charakteristische Menge von $\langle G_i \rangle_\partial : h_{G_i}^\infty$ für $i = 1, \ldots, r$, so wird die Zerlegung auch charakteristisch genannt. Solche Darstellungen werden z.B. in [11] bestimmt. In [3] und [25] werden saturierte Zerlegungen betrachtet, d.h. solche, für die h_{G_i} modulo $\langle G_i \rangle_\partial$ invertierbar ist.

Mit allen Methoden lässt sich schließlich das Radikalzugehörigkeitsproblem lösen. Eine wichtige Eigenschaft fehlt den charakteristischen Mengen aber. Sie bilden im Allgemeinen kein differentielles Erzeugendensystem des zugehörigen differentiellen Ideals. Letzteres ist eine zusätzliche Forderung, die Mansfield an ihren Begriff der differentiellen Gröbnerbasis stellt. Leider gibt der in [16] angegebene Algorithmus nicht notwendigerweise eine solche Menge aus.

Im Folgenden bezeichne wieder $D = K\{y_1, \ldots, y_n\}$ den differentiellen Polynomring, I ein differentielles Ideal von D und τ ein Ranking auf der Menge $\mathbb{D}^n$ aller Derivate.

Definition 1.6.1. Sei $I \subseteq D$ ein differentielles Ideal und τ ein Ranking auf $\mathbb{D}^n$. Eine (pseudo-reduzierte) Teilmenge $G \subseteq I \backslash \{0\}$ heißt *(reduzierte) differentielle τ-Pseudo-Gröbnerbasis* von I, falls jedes Polynom $f \in I \backslash \{0\}$ bzgl. G pseudo-reduzibel ist.

Nach obiger Definition ist eine differentielle Pseudo-Gröbnerbasis eines Ideals I nicht notwendig ein differentielles Erzeugendensystem von I. So ist z.B. für das Ranking τ mit $y_1 <_\tau y_2 <_\tau \partial y_1 <_\tau \partial y_2 <_\tau \cdots$ die Menge $\{y_1 y_2\}$ eine differentielle τ-Pseudo-Gröbnerbasis von $\langle y_2 \rangle_\partial \subseteq K\{y_1, y_2\}$, aber kein differentielles Erzeugendensystem. Allgemein gilt hingegen das Folgende.

Satz 1.6.2. *Sei $I \subseteq D$ ein differentielles Ideal, τ ein Ranking auf $\mathbb{D}^n$ und $G \subseteq I \backslash \{0\}$ eine differentielle τ-Pseudo-Gröbnerbasis von I.*

a) Für alle $f \in I \backslash \{0\}$ gilt $f \xrightarrow{G}_p 0$.
b) Es ist $\langle G \rangle_\partial \subseteq I \subseteq \langle G \rangle_\partial : h_G^\infty$.

Beweis. Sei zunächst $f \in I \backslash \{0\}$. Da G eine differentielle τ-Pseudo-Gröbnerbasis von I ist, ist f bzgl. G pseudo-reduzibel, d.h es existieren Polynome $\tilde{f}, h_1, h_2 \in D$ und ein $g \in G$ mit $f \xrightarrow{g}_p h_1 f - h_2 g = \tilde{f}$. Nun ist $\tilde{f}$ wieder ein Element des Ideals I. Ist $\tilde{f}$ von Null verschieden, so ist es wie f pseudo-reduzibel bzgl. G. Da $\xrightarrow{G}_p$ noethersch ist, erhalten wir nach endlich vielen dieser Schritte ein bzgl. G pseudo-reduziertes Element, also Null. Es folgt demnach a) und zusammen mit Satz 1.5.3 b) auch b). □

Die Existenz einer differentiellen Pseudo-Gröbnerbasis ist offensichtlich gegeben. Darüber hinaus gibt es sogar stets eine endliche. Eine reduzierte differentielle Pseudo-Gröbnerbasis kann nach Satz 1.5.2 zudem höchstens n Elemente umfassen.

Satz 1.6.3. *Sei $I \subseteq D$ ein differentielles Ideal und τ ein Ranking auf $\mathbb{D}^n$.*

a) Das Ideal I besitzt eine endliche differentielle τ-Pseudo-Gröbnerbasis.
b) Für zwei reduzierte differentielle τ-Pseudo-Gröbnerbasen $G, \widetilde{G}$ von I gilt $|G| = |\widetilde{G}|$, und zu jedem $g \in G$ existiert ein $\tilde{g} \in \widetilde{G}$ mit $\mathrm{LP}_\tau(g) = \mathrm{LP}_\tau(\tilde{g})$.

Beweis. Für den Beweis von a) sei A_0 die Menge aller pseudo-reduzierten Teilmengen von I. Ist $A_0 = \{\emptyset\}$, dann ist $G = \emptyset$ eine differentielle τ-Pseudo-Gröbnerbasis von I. Sei also $A_0 \neq \{\emptyset\}$. Da τ eine Wohlordnung auf $\{u^d \mid u \in \mathbb{D}^n, d \in \mathbb{N}\}$ ist, existiert in der Menge $\bigcup_{G \in A_0} \{\mathrm{LP}_\tau(g) \mid g \in G\}$ ein bzgl. τ kleinstes Element t_0. Sei nun B_0 die Menge aller pseudo-reduzierten Mengen $G \in A_0$, die ein differentielles Polynom f_G enthalten, welches das Minimum t_0 annimmt. Wir fassen die jeweiligen Mengen $G \backslash \{f_G\}$ zu einer neuen Menge A_1 von pseudo-reduzierten Teilmengen zusammen. Ist $A_1 \neq \{\emptyset\}$, so finden wir nach obigem Verfahren einen Term t_1 und bilden die Menge $B_1 \subseteq B_0$ von pseudo-reduzierten Teilmengen $G \in B_0$, für die ein $f_G \in G$ existiert mit $\mathrm{LP}_\tau(f_G) = t_1$. Eine Iteration dieses Verfahrens ergibt einen Index i, so dass $A_{i+1} = \{\emptyset\}$ gilt. Dies ist mit Satz 1.5.2 nach spätestens n Schritten der Fall. Wir zeigen nun, dass jede Menge in B_i eine differentielle τ-Pseudo-Gröbnerbasis von I ist.

Sei also $G = \{g_1, \ldots, g_i\} \in B_i$ mit $\mathrm{LD}_\tau(g_1) <_\tau \cdots <_\tau \mathrm{LD}_\tau(g_i)$ und $f \in I \backslash \{0\}$. Angenommen, f ist pseudo-reduziert bzgl. G. Wegen $\{f\} \in A_0$ und der Wahl von t_1 gilt $\mathrm{LP}_\tau(f) \geq_\tau \mathrm{LP}_\tau(g_1)$. Da das Polynom f nicht durch g_1 pseudo-reduzierbar ist, muss dabei $\mathrm{LD}_\tau(f) >_\tau \mathrm{LD}_\tau(g_1)$ gelten, also ist $\{g_1, f\}$ pseudo-reduziert. Es existiert nun ein maximaler Index $j \in \{1, \ldots, i\}$, so dass $\{g_1, \ldots, g_j, f\}$ pseudo-reduziert ist. Wäre $j < i$, so wäre $\mathrm{LP}_\tau(f) <_\tau \mathrm{LP}_\tau(g_{j+1}) = t_{j+1}$ im Widerspruch zur Wahl von t_{j+1}. Also ist $j = i$. Hieraus folgt aber $\{f\} \in A_{i+1}$, ein Widerspruch.

Seien nun $G = \{g_1, \ldots, g_r\}$ und $\widetilde{G} = \{\tilde{g}_1, \ldots, \tilde{g}_s\}$ reduzierte differentielle τ-Pseudo-Gröbnerbasen von I mit $\mathrm{LD}_\tau(g_1) <_\tau \cdots <_\tau \mathrm{LD}_\tau(g_r)$ bzw. $\mathrm{LD}_\tau(\tilde{g}_1) <_\tau \cdots <_\tau \mathrm{LD}_\tau(\tilde{g}_s)$. Dann ist zum einen $\tilde{g}_1$ pseudo-reduzibel bzgl. G, d.h. $\mathrm{LP}_\tau(g_1) \leq_\tau \mathrm{LP}_\tau(\tilde{g}_1)$, zum anderen g_1 pseudo-reduzibel bzgl. $\widetilde{G}$, d.h. $\mathrm{LP}_\tau(\tilde{g}_1) \leq_\tau \mathrm{LP}_\tau(g_1)$. Weiter gilt für $2 \leq j \leq \min\{r, s\}$, dass $\tilde{g}_j$ pseudo-reduzibel bzgl. G, aber pseudo-reduziert bzgl. $\{g_1, \ldots, g_{j-1}\}$ ist und analog für g_j. Also folgt $\mathrm{LP}_\tau(g_j) = \mathrm{LP}_\tau(\tilde{g}_j)$ für $1 \leq j \leq \min\{r, s\}$. Wäre nun $s > r$, so wäre $\tilde{g}_s$ pseudo-reduzibel bzgl. G und damit auch bzgl. $\{\tilde{g}_1, \ldots, \tilde{g}_s\}$ im Widerspruch zur Pseudo-Reduziertheit von $\widetilde{G}$. In gleicher Weise folgt $r \leq s$ und insgesamt $|G| = |\widetilde{G}|$. □

Für Pseudo-Gröbnerbasen differentieller Primideale sind besondere Eigenschaften erfüllt. So ist zum Beispiel jedes solche Ideal regulär.

Satz 1.6.4. *Sei $I \subseteq D$ ein differentielles Primideal und $G \subseteq D \backslash \{0\}$ eine pseudo-reduzierte Menge mit $G \subseteq I \subseteq \langle G \rangle_\partial : h_G^\infty$. Dann sind die folgenden Aussagen äquivalent:*

a) Die Menge G ist eine differentielle τ-Pseudo-Gröbnerbasis von I.
b) Es gilt $f \xrightarrow{G}_p 0$ genau dann, wenn $f \in \langle G \rangle_\partial : h_G^\infty$ gilt.

Sind die obigen Bedingungen erfüllt, so gilt insbesondere $I = \langle G \rangle_\partial : h_G^\infty$.

Beweis. Für den Beweis von a) $\Rightarrow$ b) bleibt wegen Satz 1.5.3 b) nur die Implikation „$\Leftarrow$" zu zeigen. Sei also $f \in D$ mit $f h_G^i \in \langle G \rangle_\partial \subseteq I$ für ein $i \in \mathbb{N}_0$. Nach Satz 1.5.2 b) sind für jedes $g \in G$ die Polynome $\mathrm{in}_\tau(g)$ und $\mathrm{sep}_\tau(g)$ pseudo-reduziert bzgl. G und, da sie von Null verschieden sind, nicht in I enthalten. Dann gilt aber auch $h_G \notin I$, denn I ist nach Voraussetzung prim. Mit demselben Argument folgt daraus $f \in I$ und mit Satz 1.6.2 a) schließlich $f \xrightarrow{G}_p 0$. Dies zeigt auch die zusätzliche Aussage.

Die Umkehrung folgt direkt aus $I \subseteq \langle G \rangle_\partial : h_G^\infty$ und b). □

Das Radikal eines differentiellen Ideals lässt sich nach Theorem 1.2.7 gerade in endlich viele differentielle Primideale zerlegen. Also ist das Radikal insbesondere der Durchschnitt endlich vieler regulärer differentieller Ideale.

Satz 1.6.5. *Sei $I \subseteq D$ ein differentielles Ideal. Dann existieren reduzierte differentielle τ-Pseudo-Gröbnerbasen $G_1, \dots, G_r \subseteq D$ von differentiellen Primidealen, so dass gilt*

$$\sqrt{I} = \bigcap_{i=1}^{r} (\langle G_i \rangle_\partial : h_{G_i}^\infty).$$

Beweis. Nach Theorem 1.2.7 existieren endlich viele differentielle Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ von D, so dass gilt $\sqrt{I} = \mathfrak{p}_1 \cap \dots \cap \mathfrak{p}_r$. Ist G_i eine reduzierte differentielle τ-Pseudo-Gröbnerbasis von $\mathfrak{p}_i$ für $i = 1, \dots, r$, so folgt $\sqrt{I} = \bigcap_{i=1}^r (\langle G_i \rangle_\partial : h_{G_i}^\infty)$ mit Satz 1.6.4. □

Es soll nun eine solche Zerlegung des Radikals eines differentiellen Ideals berechnet werden. Ritt bestimmt in seinem Algorithmus dazu schrittweise reguläre differentielle Ideale, die das Radikal umfassen. Ist ein solches nicht prim, so zerlegt er es geeignet. Andernfalls wird es vergrößert, aber natürlich nur solange es nicht dem Einheitsideal entspricht.

Satz 1.6.6 (Berechnung der Primidealzerlegung von Radikalidealen)**.**
Sei $F = \{f_1, \dots, f_s\} \subseteq D$ und τ ein Ranking auf $\mathbb{D}^n$. Wir betrachten die durch die folgenden Instruktionen definierte Prozedur $\mathtt{Kolchin-Ritt}(F)$*:*

1) *Berechne $G =$* $\mathtt{PseudoRed}(F)$*. Existiert ein $g \in G$ mit $g \in K$, so gib $\{1\}$ aus und stoppe.*
2) *Prüfe, ob G eine reduzierte differentielle τ-Pseudo-Gröbnerbasis eines differentiellen Primideals ist. Wenn ja, gib*

$$\{G\} \cup \bigcup_{\substack{g \in G \\ \mathrm{in}_\tau(g) \notin K}} \mathtt{Kolchin-Ritt}(G \cup \{\mathrm{in}_\tau(g)\}) \cup \mathtt{Kolchin-Ritt}(G \cup \{\mathrm{sep}_\tau(g)\})$$

   aus und stoppe.
3) *Bestimme differentielle Polynome $f_1, f_2 \in D \backslash \langle F \rangle_\partial$, die bzgl. G pseudo-reduziert sind und $f_1 f_2 \in \langle F \rangle_\partial$ erfüllen.*
4) *Gib* $\mathtt{Kolchin-Ritt}(F \cup \{f_1\}) \cup \mathtt{Kolchin-Ritt}(F \cup \{f_2\})$ *aus und stoppe.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten eine Menge A ausgibt, so dass gilt

$$\sqrt{\langle F \rangle_\partial} = \bigcap_{G \in A} (\langle G \rangle_\partial : h_G^\infty),$$

wobei $\langle G \rangle_\partial : h_G^\infty$ für jedes $G \in A$ ein differentielles Primideal von D ist.

Beweis. Siehe [21], Kapitel V.5. □

Für die Überprüfung der Bedingung in Schritt 2) gibt Ritt in [21], Kapitel V.1 einen entsprechenden Algorithmus an. Leider ist die durch den Algorithmus berechnete Zerlegung von $\sqrt{\langle F \rangle_\partial}$ nicht minimal, d.h. für zwei Mengen $G_1, G_2 \in A$ kann $\langle G_1 \rangle_\partial : h_{G_1}^\infty = \langle G_2 \rangle_\partial : h_{G_2}^\infty$ gelten. Dies kann aber durch einen Vergleich der reduzierten Gröbnerbasen von $\langle G_1 \rangle : h_{G_1}^\infty$ bzw. $\langle G_1 \rangle : h_{G_1}^\infty$ getestet werden.

Ferner bilden die Mengen G_i nicht notwendigerweise eine differentielle τ-Pseudo-Gröbnerbasis des jeweiligen differentiellen Primideals $\langle G_i \rangle_\partial : h_{G_i}^\infty$. Eine solche kann jedoch wie folgt bestimmt werden.

Satz 1.6.7. *Sei τ ein Ranking auf $\mathbb{D}^n$ und $G = \{g_1, \ldots, g_s\} \subseteq D$, so dass das differentielle Ideal $\langle G \rangle_\partial : h_G^\infty$ prim ist. Weiter sei $H \subseteq \mathbb{D}(G)$ eine* `Lex`*-Gröbnerbasis des Ideals $\langle G \rangle : h_G^\infty \subseteq \mathbb{D}(G)$, wobei die Unbestimmten bzgl. τ geordnet sind. Dann ist* `PseudoRed`(H) *eine reduzierte differentielle τ-Pseudo-Gröbnerbasis von $\langle G \rangle_\partial : h_G^\infty$.*

Beweis. Siehe [1], Theorem 6. □

Der obige Algorithmus liefert zwar keine differentielle Pseudo-Gröbnerbasis des Ideals $\sqrt{\langle F \rangle_\partial}$, aber mit der berechneten Zerlegung lässt sich bereits die Zugehörigkeit eines Polynoms zu $\sqrt{\langle F \rangle_\partial}$ testen. Hierbei sei erwähnt, dass für bestimmte Rankings eine differentielle Pseudo-Gröbnerbasis explizit berechnet werden kann. Dies werden wir in Abschnitt 1.8 aufgreifen.

Korollar 1.6.8 (Radikalzugehörigkeitstest)**.**
Sei $F = \{f_1, \ldots, f_s\} \subseteq D$, τ ein Ranking auf $\mathbb{D}^n$ und $f \in D \backslash \{0\}$. Dann ist f genau dann ein Element von $\sqrt{\langle F \rangle_\partial}$, wenn für alle $G \in \mathtt{Kolchin} - \mathtt{Ritt}(F)$ gilt $f \xrightarrow{G}_p 0$.

Beweis. Ist $f \in \sqrt{\langle F \rangle_\partial}$ ein von Null verschiedenes Polynom, so gilt $f \in \langle G \rangle_\partial : h_G^\infty$ nach Satz 1.6.6 für alle $G \in \mathtt{Kolchin} - \mathtt{Ritt}(F)$. Da hierbei $\langle G \rangle_\partial : h_G^\infty$ ein differentielles Primideal mit differentieller τ-Pseudo-Gröbnerbasis G ist, pseudo-reduziert f bzgl. G zu Null.

Für die Umkehrung sei $f \in D \backslash \{0\}$ ein Polynom, so dass $f \xrightarrow{G}_p 0$ für alle τ-Pseudo-Gröbnerbasen $G \in \mathtt{Kolchin} - \mathtt{Ritt}(F)$ gilt. Nach Satz 1.6.4 ist dann $f \in \langle G \rangle_\partial : h_G^\infty$ für alle $G \in \mathtt{Kolchin} - \mathtt{Ritt}(F)$ und damit $f \in \sqrt{\langle F \rangle_\partial}$. □

Der beschriebene Algorithmus `Kolchin-Ritt` ist eher von theoretischer Bedeutung. Für praktische Zwecke, wie zum Beispiel dem Radikalzugehörigkeitstest, genügt die Berechnung einer Zerlegung des Radikals von $\langle F \rangle_\partial$ in reguläre differentielle Ideale der Form $\langle G \rangle_\partial : H^\infty$. Dabei ist $G \subseteq \langle F \rangle_\partial$ eine pseudo-reduzierte Menge und $H \subseteq D$ bzgl. G partiell reduziert, wobei H alle Initials und Separanden der Polynome in G enthält. Eine solche Zerlegung lässt sich durch den sogenannten *Rosenfeld-Gröbner-Algorithmus* berechnen. Für genauere Betrachtungen dieses Algorithmus verweisen wir auf [1] und [2] bzw. für vergleichbare Ansätze auf [3] und [11].

Wir bezeichnen mit H_G die Menge der Initials und Separanden der Elemente von G.

Satz 1.6.9 (Rosenfeld-Gröbner-Algorithmus).
Sei $F = \{f_1, \ldots, f_s\} \subseteq D$ und τ ein Ranking auf $\mathbb{D}^n$. Wir betrachten die folgenden Instruktionen:

1) *Setze $A = \emptyset$ und $\Sigma = \{(F, \emptyset)\}$.*
2) *Gilt $\Sigma = \emptyset$, gib A aus und stoppe. Ansonsten wähle ein Paar $(G, H) \in \Sigma$ aus und entferne es aus Σ.*
3) *Bestimme eine pseudo-reduzierte Teilmenge $\widetilde{G} \subseteq G$, so dass jedes Polynom in G bzgl. $\widetilde{G}$ pseudo-reduzierbar ist. Berechne $R = \{\mathrm{PR}_{\tau,\widetilde{G}}(g) \mid g \in G\} \backslash \{0\}$.*
4) *Gilt $R = \emptyset$ und ist $1 \notin \langle \widetilde{G} \rangle : \{\{\mathrm{PR}_{\tau,\widetilde{G}}(h) \mid h \in H\} \cup H_{\widetilde{G}}\}^\infty$, so ersetze A durch $A \cup \{(\widetilde{G}, \{\mathrm{PR}_{\tau,\widetilde{G}}(h) \mid h \in H\} \cup H_{\widetilde{G}})\}$. Sonst ersetze Σ durch $\Sigma \cup \{(\widetilde{G} \cup R, H \cup H_{\widetilde{G}})\}$.*
5) *Ersetze Σ durch $\Sigma \cup \{(F \cup \{h\}, H) \mid h \in H_{\widetilde{G}} \backslash K\}$ und fahre mit Schritt 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten eine Menge A ausgibt, so dass gilt

$$\sqrt{\langle F \rangle_\partial} = \bigcap_{(G,H) \in A} (\langle G \rangle_\partial : H^\infty),$$

wobei $\langle G \rangle_\partial : H^\infty$ für jedes Paar $(G, H) \in A$ ein reguläres differentielles Ideal ist.

Beweis. Siehe [1], Abschnitt 4. □

Ein Radikalzugehörigkeitstest ergibt sich in dieser Situation wie folgt. Ist die Menge $A = \{(G_1, H_1), \ldots, (G_r, H_r)\}$ die Ausgabe des Rosenfeld-Gröbner-Algorithmus, so ist ein Polynom f nun genau dann in $\sqrt{\langle F \rangle_\partial}$ enthalten, wenn für $i = 1, \ldots, r$ dessen differentieller Pseudorest bzgl. G_i in $\langle G_i \rangle : H_i^\infty$ liegt. Letzteres ist also ein gewöhnlicher Idealzugehörigkeitstest, der mit Mitteln der Gröbnerbasistheorie durchgeführt werden kann.

1.7 Eliminationsideale

Für ein Ideal I des Polynomrings $K[x_1, \ldots, x_n]$ ist in vielen Anwendungen die Menge aller Polynome in I von Interesse, die nur in bestimmten Unbestimmten leben, ein sogenanntes Eliminationsideal von I. Berechnen lässt sich dieses, indem aus einer Gröbnerbasis von I bzgl. einer Eliminationsordnung alle Elemente entfernt werden, die noch andere Unbestimmte enthalten.

Im differentiellen Fall wollen wir diese Vorgehensweise mit Hilfe differentieller Pseudo-Gröbnerbasen bzgl. Eliminationsrankings imitieren. Da eine differentielle Pseudo-Gröbnerbasis eines differentiellen Ideals im Allgemeinen kein Erzeugendensystem ist, können wir zunächst nicht für jedes differentielle Ideal die Eliminationsideale angeben. Jedoch sind wieder spezielle Aussagen für differentielle Primideale und für die Radikale der Eliminationsideale möglich.

Im Folgenden sei $L \subseteq \{y_1, \ldots, y_n\}$ die Menge aller zu eliminierenden differentiellen Unbestimmten. Wir notieren den differentiellen Polynomring in $\{y_1, \ldots, y_n\} \backslash L$ über K mit $\widehat{D}$. Für die Menge der differentiellen Terme in $\widehat{D}$ schreiben wir $\widehat{\mathbb{T}}^n$ und $\widehat{\mathbb{D}}^n$ für die Menge der Derivate in $\widehat{D}$.

Definition 1.7.1. Sei $I \subseteq D$ ein differentielles Ideal und τ ein Ranking auf $\mathbb{D}^n$.

1) Das Ranking τ heißt *Eliminationsranking* für L, falls jedes Polynom $f \in D \backslash \{0\}$ mit $\mathrm{LD}_\tau(f) \in \widehat{\mathbb{D}}^n$ in $\widehat{D}$ enthalten ist.
2) Das differentielle Ideal $\widehat{I} = I \cap \widehat{D}$ heißt das *differentielle Eliminationsideal* von I bzgl. L.

Ein Ranking τ ist offensichtlich genau dann ein Eliminationsranking für L, wenn jede differentielle Unbestimmte $y \in L$ bzgl. τ echt größer als jedes Derivat $\tilde{y}^{(k)}$ mit $\tilde{y} \in \{y_1, \ldots, y_n\} \backslash L$ und $k \geq 0$ ist.

Beispiel 1.7.2. Für jedes $i \in \{1, \ldots, n\}$ ist das Ranking τ mit

$$y_1 <_\tau y_1^{(1)} <_\tau y_1^{(2)} <_\tau \cdots <_\tau y_2 <_\tau y_2^{(1)} <_\tau \cdots <_\tau y_n <_\tau y_n^{(1)} <_\tau \cdots$$

aus Beispiel 1.4.2 ein Eliminationsranking auf $\mathbb{D}^n$ für $L = \{y_i, \ldots, y_n\}$.

Die Bestimmung eines differentiellen Eliminationsideals steht in direktem Zusammenhang mit der Berechnung einer differentiellen Pseudo-Gröbnerbasis bzgl. eines geeigneten Eliminationsrankings, denn aus einer solchen lässt sich direkt eine differentielle Pseudo-Gröbnerbasis des Eliminationsideals gewinnen.

Ist τ ein Ranking auf $\mathbb{D}^n$, so bezeichnen wir im Weiteren mit $\widehat{\tau}$ das von τ durch Restriktion induzierte Ranking auf $\widehat{\mathbb{D}}^n$.

Satz 1.7.3. *Sei $I \subseteq D$ ein differentielles Ideal, τ ein Eliminationsranking auf $\mathbb{D}^n$ für $L \subseteq \{y_1, \ldots, y_n\}$ und $G \subseteq I$ eine (reduzierte) differentielle τ-Pseudo-Gröbnerbasis von I. Dann ist $\widehat{G} = G \cap \widehat{D}$ eine (reduzierte) differentielle $\widehat{\tau}$-Pseudo-Gröbnerbasis des differentiellen Eliminationsideals $\widehat{I}$ von I bzgl. L.*

Beweis. Es ist zu zeigen, dass jedes differentielle Polynom in $\widehat{I} \backslash \{0\}$ bzgl. $\widehat{G}$ pseudo-reduzibel ist. Sei dazu $f \in \widehat{I} \backslash \{0\}$. Wegen $f \in I \backslash \{0\}$ existiert dann ein $g \in G$ mit $\partial^k(\mathrm{LD}_\tau(g)) \in \mathbb{D}(f) \subseteq \widehat{\mathbb{D}}^n$ für ein $k \geq 0$. Da nun τ ein Eliminationsranking ist, folgt daraus $g \in \widehat{D}$. Also ist f bzgl. $\widehat{G}$ pseudo-reduzibel.

Schließlich ist mit G auch $\widehat{G} \subseteq G$ pseudo-reduziert. □

Für differentielle Primideale lässt sich auf diese Weise jedes Eliminationsideal als reguläres differentielles Ideal beschreiben.

Korollar 1.7.4. *Sei $I \subseteq D$ ein differentielles Primideal, τ ein Eliminationsranking auf $\mathbb{D}^n$ für $L \subseteq \{y_1, \ldots, y_n\}$ und $G \subseteq I$ eine τ-Pseudo-Gröbnerbasis von I. Dann ist $\widehat{G} = G \cap \widehat{D}$ eine differentielle $\widehat{\tau}$-Pseudo-Gröbnerbasis von $\widehat{I}$ und $\widehat{I} = \langle \widehat{G} \rangle_\partial : h_{\widehat{G}}^\infty$, wobei $\langle \widehat{G} \rangle_\partial$ das von $\widehat{G}$ differentiell erzeugte Ideal in $\widehat{D}$ bezeichnet.*

Beweis. Nach obigem Satz ist $\widehat{G}$ eine differentielle $\widehat{\tau}$-Pseudo-Gröbnerbasis von $\widehat{I}$. Da mit I auch $\widehat{I}$ ein differentielles Primideal ist, folgt mit Satz 1.6.4 die Behauptung. □

Mit Hilfe der Primidealzerlegung erhalten wir auch für das Radikal eines differentiellen Eliminationsideals eine Darstellung als Durchschnitt endlich vieler regulärer differentieller Ideale.

Korollar 1.7.5. *Sei $I \subseteq D$ ein differentielles Ideal und τ ein Eliminationsranking für $L \subseteq \{y_1, \ldots, y_n\}$ auf $\mathbb{D}^n$. Weiter seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq D$ differentielle Primideale mit differentiellen τ-Pseudo-Gröbnerbasen $G_1, \ldots, G_r$, so dass $\sqrt{I} = \bigcap_{i=1}^r (\langle G_i \rangle_\partial : h_{G_i}^\infty)$ erfüllt ist. Dann ist $\widehat{G}_i = G_i \cap \widehat{D}$ für $i = 1, \ldots, r$ eine differentielle $\widehat{\tau}$- Pseudo-Gröbnerbasis von $\widehat{\mathfrak{p}}_i$ und $\sqrt{\widehat{I}} = \bigcap_{i=1}^r (\langle \widehat{G}_i \rangle_\partial : h_{\widehat{G}_i}^\infty)$, wobei $\langle \widehat{G}_i \rangle_\partial$ das von $\widehat{G}_i$ differentiell erzeugte Ideal in $\widehat{D}$ bezeichnet.*

Beweis. Die Behauptung folgt aus $\sqrt{\widehat{I}} = \sqrt{I} \cap \widehat{D} = \mathfrak{p}_1 \cap \cdots \mathfrak{p}_r \cap \widehat{D} = \widehat{\mathfrak{p}}_1 \cap \cdots \cap \widehat{\mathfrak{p}}_r$ und Korollar 1.7.4. □

1.8 Der Dimensionsbegriff

In diesem Abschnitt wollen wir den Begriff der Dimension für Faktorringe D/I des differentiellen Polynomrings D einführen. In der kommutativen Algebra entspricht für ein Ideal $I \subseteq K[x_1, \ldots, x_n]$ die Dimension von $K[x_1, \ldots, x_n]/I$ gerade der maximalen Anzahl von Unbestimmten $X \subseteq \{x_1, \ldots, x_n\}$, für die $I \cap K[X] = \{0\}$ erfüllt ist. Diese Eigenschaft lässt sich ohne Weiteres für eine sinnvolle Definition der Dimension $\dim(D/I)$ im differentiellen Fall verwenden. In diesem Zusammenhang gehen wir auch kurz auf die *differentielle Hilbertfunktion* ein, die jeder Zahl $i \in \mathbb{N}_0$ die Dimension des Faktorrings D_i/I_i zuordnet. Zu den zentralen Ergebnissen hierbei zählt die Tatsache, dass für $i \gg 0$ deren Wert der Zahl $\dim(D/I)(i+1) + a$ für ein festes $a \in \mathbb{N}_0$ entspricht. Eine umfassende Darstellung dieser Theorie findet sich in [13].

Ein Algorithmus zur Berechnung der Dimension von D/I ist in [24] beschrieben. Dieser bestimmt zunächst eine Zerlegung von $\sqrt{I}$ in differentielle Primideale, für die die Dimension des zugehörigen Faktorrings bei der Wahl eines ordentlichen Rankings direkt berechnet werden kann. Der Algorithmus liefert schließlich das Maximum dieser Dimensionen, welches gerade der Zahl $\dim(D/I)$ entspricht.

Definition 1.8.1. Sei $Y \subseteq \{y_1, \ldots, y_n\}$ eine Menge von paarweise verschiedenen differentiellen Unbestimmten und $I \subseteq D$ ein differentielles Ideal.

1) Die Menge Y heißt *differentiell unabhängig modulo* I, falls gilt
$$I \cap K\{Y\} = \{0\},$$
und *maximal differentiell unabhängig modulo* I oder *parametrische Menge* von I, falls es keine differentiell unabhängige Menge $\widetilde{Y} \subseteq \{y_1, \ldots, y_n\}$ mit $|\widetilde{Y}| > |Y|$ gibt.
2) Ist Y maximal differentiell unabhängig modulo I, so heißt $|Y|$ die *Dimension* von D/I und wird mit $\dim(D/I)$ notiert. Ist $\dim(D/I) = 0$, so heißt I auch *nulldimensional*.

Die differentielle Unabhängigkeit einer Menge $Y \subseteq \{y_1, \ldots, y_n\}$ modulo einem differentiellen Ideal $I \subseteq D$ lässt sich anhand der Betrachtung eines entsprechenden Eliminationsideals testen. Denn Y ist offensichtlich genau dann differentiell unabhängig, wenn das differentielle Eliminationsideal $I \cap K\{Y\}$ das Nullideal ist. Letzteres können wir durch die Berechnung einer differentiellen Pseudo-Gröbnerbasis von I bzgl. eines geeigneten Eliminationsrankings entscheiden.

Satz 1.8.2. *Sei $Y \subseteq \{y_1, \ldots, y_n\}$ und $I \subseteq D$ ein differentielles Ideal. Dann sind die folgenden Aussagen äquivalent:*

a) Die Menge Y ist differentiell unabhängig modulo I.
b) Für jedes Eliminationsranking τ auf $\mathbb{D}^n$ für $\{y_1, \ldots, y_n\} \backslash Y$ und jede differentielle τ-Pseudo-Gröbnerbasis G von I gilt $G \cap K\{Y\} = \emptyset$.
c) Es existiert ein Eliminationsranking τ auf $\mathbb{D}^n$ für $\{y_1, \ldots, y_n\} \backslash Y$ und eine differentielle τ-Pseudo-Gröbnerbasis G von I mit $G \cap K\{Y\} = \emptyset$.

Beweis. Die Implikation a) $\Rightarrow$ b) folgt wegen $G \subseteq I$ direkt aus der Definition der differentiellen Unabhängigkeit. Für den Beweis von b) $\Rightarrow$ c) wählen wir das Ranking τ, für welches $y_i^{(k)} <_\tau y_j^{(l)}$ genau dann gilt, wenn $y_i \in Y$ und $y_j \notin Y$ bzw. $i, j \notin Y$ oder $i, j \in Y$ und $k < l$.

Sei nun τ ein Eliminationsranking auf $\mathbb{D}^n$ für $\{y_1, \ldots, y_n\} \backslash Y$ und G eine differentielle τ-Pseudo-Gröbnerbasis von I mit $\widehat{G} = G \cap K\{Y\} = \emptyset$. Nach Satz 1.7.3 ist dann $\widehat{G}$ eine differentielle $\widehat{\tau}$-Pseudo-Gröbnerbasis von $\widehat{I} = I \cap K\{Y\}$. Also muss $\widehat{I} = \{0\}$ gelten. □

Für maximal differentiell unabhängige Mengen $Y \subseteq \{y_1, \ldots, y_n\}$ existiert ein weiterer Zusammenhang mit differentiellen Pseudo-Gröbnerbasen bzgl. entsprechender Eliminationsrankings. Denn die Mächtigkeit von Y entspricht dann gerade der Anzahl der differentiellen Unbestimmten, für die kein Derivat als Leitderivat eines Polynoms in der reduzierten differentiellen Pseudo-Gröbnerbasis auftaucht.

Korollar 1.8.3. *Sei $I \subseteq D$ ein differentielles Ideal und $Y \subseteq \{y_1, \ldots, y_n\}$ maximal differentiell unabhängig modulo I. Ist τ ein Eliminationsranking auf $\mathbb{D}^n$ für $\{y_1, \ldots, y_n\} \backslash Y$ und G eine reduzierte differentielle τ-Pseudo-Gröbnerbasis von I, so gilt*
$$|G| = n - \dim(D/I).$$

Beweis. Nach obigem Satz gilt $G \cap K\{Y\} = \emptyset$. Da τ ein Eliminationsranking für $\{y_1, \ldots, y_n\} \backslash Y$ ist, folgt daraus $\mathrm{LD}_\tau(g) \notin K\{Y\}$ für alle $g \in G$. Damit ergibt sich $|G| \leq n - \dim(D/I)$. Des Weiteren ist nach Voraussetzung die Menge $\widetilde{Y} = Y \cup \{y\}$ für jede differentielle Unbestimmte $y \in \{y_1, \ldots, y_n\} \backslash Y$ differentiell abhängig modulo I, d.h. es existiert ein differentielles Polynom $f \in (I \cap K\{\widetilde{Y}\}) \backslash K$ mit $\mathrm{LD}_\tau(f) = y^{(k)}$ für ein $k \geq 0$. Da G eine differentielle τ-Pseudo-Gröbnerbasis von I ist, muss ein Polynom $g \in G$ existieren mit $\mathrm{LD}_\tau(g^{(l)}) = y^{(k)}$ für ein $l \geq 0$. Somit gilt auch $|G| \geq n - \dim(D/I)$. □

Bemerkung 1.8.4. Aus dem Beweis des Korollars geht hervor, dass für jedes Ranking τ auf $\mathbb{D}^n$ und für jede reduzierte differentielle τ-Pseudo-Gröbnerbasis von I stets gilt $|G| \geq n - \dim(D/I)$. Allgemeiner gilt das Folgende. Ist τ ein Ranking auf $\mathbb{D}^n$, G eine differentielle τ-Pseudo-Gröbnerbasis von I und $Y = \{y_1, \ldots, y_n\} \backslash \{\mathrm{LV}_\tau(g) \mid g \in G\}$, so ist Y differentiell unabhängig modulo I mit $|Y| \leq \dim(D/I)$.

Im restlichen Teil dieses Abschnitts wollen wir uns der Berechnung der Dimension eines differentiellen Faktorrings D/I widmen. Eine erste Überlegung dazu ist, dass für ein differentielles Ideal I die differentiellen Ringe D/I und $D/\sqrt{I}$ die gleiche Dimension besitzen. Ist zudem $\sqrt{I} = \bigcap_{i=1}^r \mathfrak{p}_i$ eine Zerlegung von $\sqrt{I}$ in differentielle Primideale, so entspricht die Dimension von D/I gerade dem Maximum der Dimensionen der Faktorringe $D/\mathfrak{p}_i$.

Satz 1.8.5. *Sei $I \subseteq D$ ein differentielles Ideal.*

a) Es gilt $\dim(D/I) = \dim(D/\sqrt{I})$.

b) Sind I_1, I_2 differentielle Ideale von D mit $I = I_1 \cap I_2$, so gilt

$$\dim(D/I) = \max\{\dim(D/I_1), \dim(D/I_2)\}.$$

Beweis. Die Aussage in a) folgt unmittelbar aus der Tatsache, dass jede modulo I differentiell unabhängige Menge $Y \subseteq \{y_1, \ldots, y_n\}$ wegen $\sqrt{I \cap K\{Y\}} = \sqrt{I} \cap K\{Y\}$ auch modulo $\sqrt{I}$ differentiell unabhängig ist und umgekehrt.

Sei $Y \subseteq \{y_1, \ldots, y_n\}$ differentiell unabhängig modulo I_1 oder modulo I_2. Dann ist $I \cap K\{Y\} = I_1 \cap I_2 \cap K\{Y\} = \{0\}$, also Y auch differentiell unabhängig modulo I. Ist umgekehrt Y differentiell unabhängig modulo I, so auch modulo I_1 oder I_2. Denn ansonsten gäbe es Polynome $f_1, f_2 \in K\{Y\} \backslash \{0\}$ mit $f_1 \in I_1$ bzw. $f_2 \in I_2$. Dies wäre aber wegen $0 \neq f_1 f_2 \in I_1 \cap I_2 \cap K\{Y\}$ ein Widerspruch zur differentiellen Unabhängigkeit von Y modulo I. □

Um die Bedeutung der Dimension genauer zu verstehen, betrachten wir die sogenannte differentielle Hilbertfunktion. Diese liefert zu einer ganzen Zahl i die algebraische Dimension des Faktorings D_i/I_i.

Definition 1.8.6. Ist $I \subseteq D$ ein differentielles Ideal, so heißt die Abbildung

$$\mathrm{HF}_{D/I} : \mathbb{Z} \longrightarrow \mathbb{Z},\ i \mapsto \dim(D_i/I_i)$$

die *differentielle Hilbertfunktion* von D/I.

Die algebraische Hilbertfunktion entspricht für genügend große Werte einer Polynomfunktion, dem sogenannten Hilbertpolynom. Diese Eigenschaft ist auch für die differentielle Hilbertfunktion erfüllt. Das Besondere hieran ist, dass das zugehörige Polynom höchstens Grad 1 besitzt.

Satz 1.8.7. *Sei $I \subseteq D$ ein differentielles Primideal. Dann existiert ein lineares Polynom* $\mathrm{HP}_{D/I} \in \mathbb{Q}[t]$ *mit* $\mathrm{HP}_{D/I}(i) = \mathrm{HF}_{D/I}(i)$ *für* $i \gg 0$, *das sogenannte* differentielle Hilbertpolynom *von D/I. Ist* $\mathrm{HP}_{D/I}(t) = a_1(t+1) + a_0$, *so gilt insbesondere* $a_1 = \dim(D/I)$.

Beweis. Siehe [13], Kapitel III, § 5. □

Dem Koeffizienten a_0 des differentiellen Hilbertpolynoms kommt auch eine Bedeutung zu. Dazu betrachten wir die sogenannte Ordnung eines differentiellen Ideals.

Definition 1.8.8. Sei τ ein ordentliches Ranking auf $\mathbb{D}^n$ und $I \subseteq D$ ein differentielles Ideal.

1) Ist $G = \{g_1, \ldots, g_s\} \subseteq D$ eine pseudo-reduzierte Menge und $I = \langle G \rangle_\partial : h_G^\infty$, dann heißt die Zahl $\mathrm{ord}(I) = \sum_{i=1}^{s} \mathrm{ord}(g_i)$ die *Ordnung* von I.
2) Ist $\sqrt{I} = \bigcap_{i=1}^{r} \mathfrak{p}_i$ eine Zerlegung von $\sqrt{I}$ in differentielle Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \subseteq D$ und sind $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_s}$ die Primideale mit maximaler Dimension, dann heißt die Zahl $\mathrm{ord}(I) = \max\{\mathrm{ord}(\mathfrak{p}_{i_1}), \ldots, \mathrm{ord}(\mathfrak{p}_{i_s})\}$ die *Ordnung* von I.

Für die Wohldefiniertheit des Ordnungsbegriffs muss offensichtlich gewährleistet sein, dass diese für ein reguläres differentielles Ideal nicht von dem gewählten ordentlichen Ranking abhängt. Dies aber zeigt der folgende Satz.

Satz 1.8.9. *Sei τ ein ordentliches Ranking auf $\mathbb{D}^n$, $G \subseteq D$ eine pseudo-reduzierte Menge und $I = \langle G \rangle_\partial : h_G^\infty$.*

a) Es ist $\dim(D/I) = n - |G|$.
b) Für das differentielle Hilbertpolynom von D/I gilt

$$\mathrm{HP}_{D/I}(t) = \dim(D/I)(t+1) + \mathrm{ord}(I).$$

Beweis. Siehe [24], Theorem 3.1. □

Mit diesem Resultat lässt sich nun auch auf das differentielle Hilbertpolynom beliebiger differentieller Ideale schließen.

Korollar 1.8.10. *Ist $I \subseteq D$ ein differentielles Ideal, so ist*

$$\mathrm{HP}_{D/I}(t) = \dim(D/I)(t+1) + \mathrm{ord}(I)$$

das differentielle Hilbertpolynom von D/I.

Beweis. Ist $\sqrt{I} = \bigcap_{i=1}^{r} \mathfrak{p}_i$ eine Zerlegung von $\sqrt{I}$ in differentielle Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ von D, so gilt $\dim(D_t/I_t) = \max\{\dim(D_t/(\mathfrak{p}_i)_t) \mid i = 1, \ldots, r\}$ für $t \geq 0$ nach Satz 1.8.5. Seien $\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_s}$ die Primideale mit maximaler Dimension. Mit obigem Satz und der Tatsache, dass jedes Primideal regulär ist, folgt dann für $t \gg 0$

$$\begin{aligned}
\dim(D_t/I_t) &= \max\{\mathrm{HP}_{D/\mathfrak{p}_i}(t) \mid i = 1, \ldots, r\} \\
&= \max\{\dim(D/\mathfrak{p}_i)(t+1) + \mathrm{ord}(\mathfrak{p}_i) \mid i = 1, \ldots, r\} \\
&= \max\{\dim(D/\mathfrak{p}_i) \mid i = 1, \ldots, r\}(t+1) + \max\{\mathrm{ord}(\mathfrak{p}_{i_j}) \mid j = 1, \ldots, s\} \\
&= \dim(D/I)(t+1) + \mathrm{ord}(I).
\end{aligned}$$

□

Die differentielle Hilbertfunktion bzw. die Dimension und Ordnung eines differentiellen Ideals I kann wie bereits erwähnt mit Hilfe der Primidealzerlegung von $\sqrt{I}$ bestimmt werden.

Korollar 1.8.11 (Dimensionsberechnung).
Seien $f_1, \ldots, f_s \in D\backslash\{0\}$ differentielle Polynome und $F = \{f_1, \ldots, f_s\}$. Wir betrachten die folgenden Instruktionen:

1) *Wähle ein ordentliches Ranking τ auf $\mathbb{D}^n$ und berechne $A = \mathtt{Kolchin} - \mathtt{Ritt}(F)$.*
2) *Bestimme $d = \max\{n - |G| \mid G \in A\}$ und entferne alle G aus A, für die $n - |G| < d$ gilt.*
3) *Für jedes $G \in A$ berechne $k_G = \sum_{g \in G} ord(g)$ und bestimme $k = \max\{k_G \mid G \in A\}$.*
4) *Gib (d, k) aus und stoppe.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten ein Paar (d, k) ausgibt, so dass gilt $d = \dim(D/\sqrt{\langle F \rangle_\partial})$ und $k = \mathrm{ord}(\sqrt{\langle F \rangle_\partial})$.

Beweis. Die Behauptung folgt aus Satz 1.6.6 und Satz 1.8.5. □

Der Algorithmus endet mit demselben Ergebnis, falls in Schritt 1) statt `Kolchin-Ritt` der Rosenfeld-Gröbner-Algorithmus aufgerufen wird. In diesem Fall besteht die Menge A nicht aus Primidealen, sondern aus beliebigen regulären Idealen von D.

Für eine Menge $G \in A$, die das Maximum in Schritt 2) annimmt, gilt zudem, dass die Menge derjenigen differentiellen Unbestimmten, deren Derivate nicht Leitderivat eines Polynoms $g \in G$ sind, eine modulo $\sqrt{\langle F \rangle_\partial}$ maximal differentiell unabhängige Menge bildet. Es lassen sich tatsächlich alle solche Mengen bestimmen. Hierbei spielt die Ordnung des Ideals eine wesentliche Rolle, denn es gilt das Folgende.

Satz 1.8.12. *Sei $F = \{f_1, \ldots, f_s\} \subseteq D$ und $s = \mathrm{ord}(\langle F \rangle_\partial)$. Dann ist eine Teilmenge $Y \subseteq \{y_1, \ldots, y_n\}$ genau dann differentiell unabhängig modulo $\sqrt{\langle F \rangle_\partial}$, wenn die Menge $\{y^{(k)} \mid y \in Y, 0 \leq k \leq s\}$ unabhängig modulo $\sqrt{\langle F \rangle_\partial} \cap D_s$ ist.*

Beweis. Siehe [24], Bemerkung 4.8. □

Dabei lässt sich die zweite Aussage durch geeignete Gröbnerbasisberechnungen verifizieren (siehe dazu [15], Kapitel 5.7). Das zugehörige Ideal $\sqrt{\langle F\rangle_\partial} \cap D_s$ kann dabei durch den Algorithmus `Kolchin-Ritt` bzw. den Rosenfeld-Gröbner-Algorithmus in Zusammenhang mit Satz 1.5.10 bestimmt werden.

Abschließend wollen wir noch kurz darauf eingehen, wie wir eine differentielle Pseudo-Gröbnerbasis von $\sqrt{\langle F\rangle_\partial}$ bzgl. eines Rankings τ berechnen können, für welches $y_i^{(k)} <_\tau y_j$ gilt, falls $y_i <_\tau y_j$ ist.

Satz 1.8.13. *Sei $F = \{f_1, \ldots, f_s\} \subseteq D$ und $\sqrt{\langle F\rangle_\partial} = I_1 \cap \ldots \cap I_r$ eine Zerlegung von $\sqrt{\langle F\rangle_\partial}$ in reguläre differentielle Ideale $I_1, \ldots, I_r$ von D. Weiter sei $d = \dim(D/\sqrt{\langle F\rangle_\partial})$, $s = \mathrm{ord}(\sqrt{\langle F\rangle_\partial})$ und $s' = \max\{\mathrm{ord}(I_j) \mid j = 1, \ldots, r\}$. Dann ist in $\sqrt{\langle F\rangle_\partial} \cap D_{d(s+1)+s+s'}$ eine differentielle τ-Pseudo-Gröbnerbasis von $\sqrt{\langle F\rangle_\partial}$ enthalten.*

Beweis. Siehe [24], Theorem 4.5. □

Es ist nicht nur die Existenz einer solchen Pseudo-Gröbnerbasis gesichert, sie lässt sich auch wie folgt berechnen. Für $I_j \cap D_{d(s+1)+s+s'}$ und somit auch für $\sqrt{\langle F\rangle_\partial} \cap D_{d(s+1)+s+s'}$ lässt sich mit Satz 1.5.10 eine Gröbnerbasis berechnen. Wird dabei eine mit τ verträgliche lexikographische Eliminationsordnung gewählt, so ergibt sich daraus schließlich eine differentielle Pseudo-Gröbnerbasis von $\sqrt{\langle F\rangle_\partial}$.

Kapitel 2

Differentielle Gröbnerbasen

In der algebraischen Idealtheorie spielt die Theorie der Gröbnerbasen eine zentrale Rolle. Eine Gröbnerbasis G eines Ideals I besitzt dabei vielfältige Eigenschaften, die es ermöglichen, komplexe Probleme zu lösen. Hierzu gehört sicherlich das Idealzugehörigkeitsproblem, aber auch die Durchführung grundlegender Idealoperationen wie der Durchschnitt oder der Quotient zweier Ideale und die Berechnung von Eliminationsidealen. Dies führt unweigerlich zu der Frage, ob und wie sich eine solche Theorie für differentielle Ideale entwickeln lässt. Eine erste Antwort ergibt sich nach einem Blick auf die Inhalte aller bisherigen Forschungsarbeiten. Dabei zeigt sich, dass sich die Mehrheit der wissenschaftlichen Arbeiten mit denen in Kapitel 1 thematisierten charakteristischen Mengen beschäftigt. Der Hauptgrund dafür liegt nun gerade darin, dass eine direkte Übertragung der Gröbnerbasistheorie mit all seinen Eigenschaften nicht gelingen kann. Hierbei genügt es darauf zu verweisen, dass der differentielle Polynomring $K\{y_1, \ldots, y_n\}$ nicht noethersch ist, auch nicht im differentiellen Sinn. Hingegen arbeitet die Theorie der differentiellen Pseudo-Gröbnerbasen stets mit endlichen Mengen, die insbesondere aus algorithmischer Sicht eine bessere Handhabe zulassen. Jedoch ist diese Theorie bisher auf differentielle Prim- und Radikalideale beschränkt.

Dennoch gibt es bereits verschiedene sinnvolle Ansätze für eine Gröbnerbasistheorie für differentielle Polynomideale, wie die Arbeiten von Carrà-Ferro ([5]), Mansfield ([16]), Ollivier ([18]) und Zobnin ([29]) zeigen. Speziell in den letzten beiden Arbeiten werden natürliche Definitionen einer Gröbnerbasis verwendet, die der algebraischen sehr ähnlich sind und somit einen Großteil der Eigenschaften von Gröbnerbasen erhalten.

Um eine korrekte Definition einer differentiellen Gröbnerbasis festzulegen, werden wir uns notwendigerweise zunächst mit Ordnungen der Terme in $K\{y_1, \ldots, y_n\}$ beschäftigen. Dies liefert die Grundlage für die Einführung von Termersetzungssystemen, einer Alternative für die in Abschnitt 1.5 angesprochenen Pseudo-Ersetzungssysteme. Anschließend betrachten wir Filtrierungen des differentiellen Polynomrings und erhalten den Begriff der differentiellen Gröbnerbasis aus dem der differentiellen Standardbasis bzgl. sogenannter Gröbner-Filtrierungen. In Abschnitt fünf erarbeiten wir dann die grundlegenden Eigenschaften differentieller Gröbnerbasen, bevor wir im letzten Abschnitt auf deren Berechnung eingehen. Wir werden dazu eine differentielle Version des Buchberger-Algorithmus angeben und Kriterien entwickeln, unter denen dieser terminiert.

Im Folgenden werden wir bei den Elementen von $D = K\{y_1, \ldots, y_n\}$ und $\mathbb{T}^n$ nur noch von Polynomen bzw. Termen sprechen.

2.1 Differentielle Termordnungen

Bei der Einführung einer Gröbnerbasistheorie besteht der erste Schritt stets darin, eine geeignete Definition für den Termordnungsbegriff in dem jeweiligen Kontext zu finden. Da der differentielle Polynomring $K\{y_1, \ldots, y_n\}$ auch als Polynomring in unendlich vielen Unbestimmten angesehen werden kann, liegt es nahe, zunächst die üblichen Eigenschaften einer Termordnung zu fordern. Also sollte eine differentielle Termordnung σ auf der Menge der Terme $\mathbb{T}^n$ eine totale, mit der Termmultiplikation verträgliche Ordnung sein, so dass insbesondere jeder Term bzgl. σ echt größer als 1 ist. Dies entspricht exakt der Definition in [5], berücksichtigt aber in keinster Weise die Derivation ∂. Auf diesen Aspekt wird hingegen in [28] eingegangen, wobei zum einen gefordert wird, dass σ ein Ranking auf der Menge der Derivate $\mathbb{D}^n$ definiert, und zum anderen aber weitere Bedingungen gefordert werden, die schließlich nur lexikographische Termordnungen zulassen. Ein Weglassen Letzterer führt hingegen zu einer sinnvollen Definition von differentiellen Termordnungen, wie sie auch in [19] angegeben wird. Denn solche Ordnungen erfüllen bereits die Wohlordnungseigenschaft auf $\mathbb{T}^n$, die stets die Grundlage weiterer Betrachtungen ist. Daher werden auch wir diese Definition verwenden. Eine natürliche Zusatzeigenschaft einer Termordnung wäre die Verträglichkeit mit der Derivation von Termen, d.h. wenn für Terme $t_1, t_2 \in \mathbb{T}^n$ mit $t_1 >_\sigma t_2$ auch der Leitterm von ∂t_1 bzgl. σ echt größer als der von ∂t_2 wäre. Diese sogenannten strikt stabilen differentiellen Termordnungen werden in [18] betrachtet. Für sie ergeben sich besondere Resultate, aber für eine allgemeine Theorie ist diese Verträglichkeit nicht notwendig.

Nachdem wir differentielle Termordnungen definiert haben, gelangen wir wie gewohnt zum Begriff des Leitterms eines Polynoms und dessen Eigenschaft bzgl. der Grundoperationen. Anschließend untersuchen wir differentielle Termordnungen, die weiteren Bedingungen genügen, und weisen nach, dass jede differentielle Termordnung zugleich eine Wohlordnung ist.

Sei dazu wieder $\mathbb{T}^n$ die Menge aller Terme und $\mathbb{D}^n$ die Menge aller Derivate im differentiellen Polynomring $D = K\{y_1, \ldots, y_n\}$.

Definition 2.1.1. Sei σ eine totale Ordnung auf $\mathbb{T}^n$. Die Ordnung σ heißt *differentielle Termordnung* auf $\mathbb{T}^n$, falls gilt:

1) Aus $t_1 <_\sigma t_2$ folgt $t_1 t_3 <_\sigma t_2 t_3$ für alle $t_1, t_2, t_3 \in \mathbb{T}^n$.
2) Für alle $t \in \mathbb{T}^n \backslash \{1\}$ gilt $1 <_\sigma t$.
3) Die Einschränkung $\sigma|_{\mathbb{D}^n}$ von σ auf $\mathbb{D}^n$ ist ein Ranking auf $\mathbb{D}^n$.

Das durch die Einschränkung von σ auf $\mathbb{D}^n$ definierte Ranking notieren wir wieder mit σ. Entsprechend schreiben wir auch $\mathrm{LD}_\sigma(f)$ für das Leitderivat und $\mathrm{LV}_\sigma(f)$ für die

Leitvariable von f bzgl. des Rankings σ. Ist τ ein Ranking auf $\mathbb{D}^n$ mit $\sigma|_{\mathbb{D}^n} = \tau$, so nennen wir σ von τ *induziert.*

Beispiel 2.1.2. Für ein Ranking τ auf $\mathbb{D}^n$ ist die Ordnung $\tau\texttt{Lex}$ auf $\mathbb{T}^n$ wie folgt definiert. Für Terme $t_1 = u_1 \cdots u_r$ und $t_2 = v_1 \cdots v_s$ mit Derivaten $u_1 \geq_\tau u_2 \geq_\tau \cdots \geq_\tau u_r$ bzw. $v_1 \geq_\tau v_2 \geq_\tau \cdots \geq_\tau v_s$ gelte $t_1 >_{\tau\texttt{Lex}} t_2$ genau dann, wenn ein $i \in \{1, \ldots, \min\{r, s\}\}$ existiert mit $u_k = v_k$ für $k = 1, \ldots, i-1$ und $u_i >_\tau v_i$ oder t_2 ein Teiler von t_1 ist. Offensichtlich ist $\tau\texttt{Lex}$ eine differentielle Termordnung auf $\mathbb{T}^n$, die sogenannte *differentiell lexikographische Termordnung* bzgl. τ.

Definition 2.1.3. Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$ und seien $t_1, t_2 \in \mathbb{T}^n$.

1) Die Ordnung σ heißt *gradkompatibel*, falls mit $t_1 \geq_\sigma t_2$ stets $\deg(t_1) \geq \deg(t_2)$ gilt.
2) Die Ordnung σ heißt *gewichtskompatibel*, falls mit $t_1 \geq_\sigma t_2$ auch $w(t_1) \geq w(t_2)$ gilt.
3) Die Ordnung σ heißt *ordnungskompatibel*, falls aus $t_1 \geq_\sigma t_2$ stets $\mathrm{ord}(t_1) \geq \mathrm{ord}(t_2)$ folgt.

Für jede differentielle Termordnung σ auf $\mathbb{T}^n$ ist die Ordnung $\sigma\texttt{Deg}$, die zwei Terme zunächst hinsichtlich ihres Grades und im Falle der Gradgleichheit bzgl. σ vergleicht, eine gradkompatible differentielle Termordnung auf $\mathbb{T}^n$. Analog ergibt sich aus σ eine gewichts- bzw. ordnungskompatible differentielle Termordnung, falls als erstes Entscheidungskriterium das Gewicht bzw. die Ordnung der Terme herangezogen wird.

Bemerkung 2.1.4. Für jede ordnungskompatible differentielle Termordnung σ und für jedes Polynom $f \in D \backslash K$ gilt $\mathrm{ord}(\partial f) > \mathrm{ord}(f)$. Dies folgt aus

$$\mathrm{ord}(f) = \mathrm{ord}(\mathrm{LT}_\sigma(f)) < \mathrm{ord}(\mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f))))$$

und der Tatsache, dass sich der Term $\mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f)))$ in ∂f nicht weghebt. Denn ist $u \in \mathbb{D}^n$ und $t \in \mathbb{T}^n$, so dass $\mathrm{LT}_\sigma(f) = tu$ und $\mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f))) = tu^{(1)}$ gilt, und wäre $\tilde{t} \in \mathrm{Supp}(f) \backslash \{\mathrm{LT}_\sigma(f)\}$ mit $tu^{(1)} \in \mathrm{Supp}(\partial \tilde{t})$, so wäre $u^{(1)} \in \mathbb{D}(\tilde{t})$ im Widerspruch zu $\mathrm{ord}(\tilde{t}) \leq \mathrm{ord}(\mathrm{LT}_\sigma(f))$.

Jedes Polynom $f \in D$ besitzt bzgl. einer differentiellen Termordnung σ eine eindeutige Darstellung der Form $f = \sum_{i=1}^m c_i t_i$ mit $c_i \in K \backslash \{0\}$, $t_i \in \mathbb{T}^n$ für $i = 1, \ldots, m$ und $t_1 >_\sigma t_2 >_\sigma \cdots >_\sigma t_m$. Also existiert im Träger von f ein eindeutig bestimmtes bzgl. σ größtes Element.

Definition 2.1.5. Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$ und $f \in D \backslash \{0\}$ ein Polynom mit der Darstellung $f = \sum_{i=1}^m c_i t_i$ wie oben.

1) Der Term $\mathrm{LT}_\sigma(f) = t_1$ heißt der *Leitterm* von f bzgl. σ, $\mathrm{LC}_\sigma(f) = c_1$ der *Leitkoeffizient* von f und $\mathrm{LM}_\sigma(f) = c_1 t_1$ das *Leitmonom* von f.
2) Für ein differentielles Ideal $I \subseteq D$ heißt $\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(f) \mid f \in I \backslash \{0\} \rangle$ das *Leittermideal* von I bzgl. σ. Zudem schreiben wir $\mathrm{LT}_\sigma\{I\} = \{\mathrm{LT}_\sigma(f) \mid f \in I \backslash \{0\}\}$.

Wie üblich ergibt sich als Leitterm des Produkts zweier Polynome gerade das Produkt der Leitterme und als Leitterm der Summe der Polynome das Maximum der beiden einzelnen Leitterme bzgl. σ, falls diese sich nicht wegheben. Hingegen muss der Leitterm der Derivation eines Polynoms im Allgemeinen Nichts mit dem ursprünglichen Leitterm gemeinsam haben, er muss bzgl. σ nicht einmal größer sein.

Lemma 2.1.6. *Seien $f, g \in D\backslash\{0\}$ Polynome und $t \in \mathbb{T}^n$.*

a) Ist $f + g \neq 0$, so gilt $\mathrm{LT}_\sigma(f+g) \leq_\sigma \max_\sigma\{\mathrm{LT}_\sigma(f), \mathrm{LT}_\sigma(g)\}$. Ist $\mathrm{LT}_\sigma(f) \neq \mathrm{LT}_\sigma(g)$ oder $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(g)$ und $\mathrm{LC}_\sigma(f) + \mathrm{LC}_\sigma(g) \neq 0$, so gilt die Gleichheit.
b) Es gilt $\mathrm{LT}_\sigma(fg) = \mathrm{LT}_\sigma(f) \cdot \mathrm{LT}_\sigma(g)$.
c) Für alle $\tilde{t} \in \mathrm{Supp}(\partial t)$ gilt $\tilde{t} >_\sigma t$.
d) Es gibt ein $k \in \mathbb{N}$ mit $w(\mathrm{LT}_\sigma(\partial^k f)) > w(\mathrm{LT}_\sigma(f))$.

Beweis. a) ergibt sich aus $\mathrm{LT}_\sigma(f+g) \in \mathrm{Supp}(f+g) \subseteq \mathrm{Supp}(f) \cup \mathrm{Supp}(g)$.

Um b) zu zeigen, verwenden wir die Eigenschaft 1) aus Definition 2.1.1. Da jeder Term in fg von der Form $t \cdot \tilde{t}$ ist mit $t \in \mathrm{Supp}(f)$ und $\tilde{t} \in \mathrm{Supp}(g)$, erhalten wir folglich $\mathrm{LT}_\sigma(f) \cdot \mathrm{LT}_\sigma(g) \geq_\sigma t \cdot \mathrm{LT}_\sigma(g) \geq_\sigma t \cdot \tilde{t}$, also $\mathrm{LT}_\sigma(fg) = \mathrm{LT}_\sigma(f) \cdot \mathrm{LT}_\sigma(g)$.

Für den Beweis von c) schreiben wir t als $t = u_1^{d_1} \cdots u_m^{d_m}$ mit $d_1, \ldots, d_m \in \mathbb{N}$ und Derivaten $u_1, \ldots, u_m \in \mathbb{D}^n$. Der Träger von ∂t ist demnach durch die Menge $\{u_1^{d_1} \cdots u_i^{d_i - 1} \partial u_i \cdots u_m^{d_m} \mid i = 1, \ldots, m\}$ gegeben. Wegen $\partial u_i >_\sigma u_i$ ergibt sich daraus $u_1^{d_1} \cdots u_i^{d_i-1} \partial u_i \cdots u_m^{d_m} >_\sigma t$ für $i = 1, \ldots, m$.

Es bleibt noch d) zu zeigen. Für jedes $i \in \mathbb{N}$ sei dazu $t_i \in \mathrm{Supp}(\partial^i f)$ ein Term von $\partial^i f$ mit minimalem Gewicht. Wegen $w(t_{i+1}) > w(t_i)$ existiert dann ein $k \in \mathbb{N}$ mit $w(\mathrm{LT}_\sigma(\partial^k f)) \geq w(t_k) > w(\mathrm{LT}_\sigma(f))$. □

Bemerkung 2.1.7.

a) Für ein Polynom $f \in D$ ist der Leitterm von ∂f nicht zwangsläufig ein Term in $\mathrm{Supp}(\partial(\mathrm{LT}_\sigma(f))$. Wir betrachten dazu das Ranking τ auf $\mathbb{D}^n$ mit

$$1 <_\tau y_1 <_\tau y_1^{(1)} <_\tau y_1^{(2)} <_\tau \cdots <_\tau y_2 <_\tau y_2^{(1)} <_\tau y_2^{(2)} <_\tau \cdots$$

und die von τ induzierte differentielle Termordnung $\sigma = \tau\mathtt{DegRevLex}$, die wie folgt definiert ist. Für Terme $t_1 = u_1^{k_1} \cdots u_m^{k_m}$ und $t_2 = v_1^{l_1} \cdots v_p^{l_p}$ mit Derivaten $u_1 < \cdots < u_m$ und $v_1 < \cdots < v_l$ gelte $t_1 >_\sigma t_2$ genau dann, wenn $\deg(t_1) > \deg(t_2)$ erfüllt ist oder wenn $\deg(t_1) = \deg(t_2)$ gilt und ein $i \in \{1, \ldots, m\}$ existiert, so dass $u_1^{k_1} \cdots u_{i-1}^{k_{i-1}} = v_1^{l_1} \cdots v_{i-1}^{l_{i-1}}$ und $u_i >_\tau v_i$ bzw. $u_i = v_i$ und $k_i < l_i$ gilt.
Für das Polynom $f = (y_1^{(1)})^2 + y_1 y_2$ ist dann $(y_1^{(1)})^2$ der Leitterm von f bzgl. σ. Als Leitterm von $\partial f = 2y_1^{(1)} y_1^{(2)} + y_1^{(1)} y_2 + y_1 y_2^{(1)}$ erhalten wir aber $y_1^{(1)} y_2$.

b) Darüber hinaus gilt im Allgemeinen nicht $\mathrm{LT}_\sigma(\partial f) >_\sigma \mathrm{LT}_\sigma(f)$. Denn für die obige differentielle Termordnung $\sigma = \tau\mathtt{DegRevLex}$ und das Polynom $f = (y_1^{(1)})^2 - 2y_1 y_1^{(2)}$ mit Derivation $\partial f = -2y_1 y_1^{(3)}$ ergibt sich $\mathrm{LT}_\sigma(\partial f) = y_1 y_1^{(3)} <_\sigma (y_1^{(1)})^2 = \mathrm{LT}_\sigma(f)$.

Die Bemerkung hat gezeigt, dass beim Übergang von einem Polynom zu seiner Derivation der Leitterm bzgl. σ nicht zwangsläufig größer wird. Dennoch käme dies einer natürlichen Eigenschaft gleich. Deshalb betrachten wir im Weiteren insbesondere solche differentiellen Termordnungen, die diese zusätzliche Bedingung erfüllen. Zum ersten Mal fanden diese Erwähnung in [29] für den univariaten Fall und in [18], wobei dort die Bedingung bereits zur Definition der differentiellen Termordnung zählt.

Definition 2.1.8. Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$.

1) Die Ordnung σ heißt *(strikt) stabil*, falls für alle Terme $t_1, t_2 \in \mathbb{T}^n$ aus $t_1 <_\sigma t_2$ stets $\mathrm{LT}_\sigma(\partial t_1) \leq_\sigma \mathrm{LT}_\sigma(\partial t_2)$ bzw. $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$ folgt.
2) Die Ordnung σ heißt *∂-lexikographisch*, falls für jeden Term $t \in \mathbb{T}^n \backslash \{1\}$ gilt $\mathrm{LT}_\sigma(\partial t) = \mathrm{LT}_{\sigma\mathtt{Lex}}(\partial t)$.

Beispiel 2.1.9. Sei τ ein Ranking auf $\mathbb{D}^n$.

a) Die differentiellen Termordnungen $\tau\mathtt{Lex}$ und $\tau\mathtt{DegLex}$ sind strikt stabil.
b) Die differentielle Termordnung $\tau\mathtt{DegRevLex}$ aus Bemerkung 2.1.7 ist nicht stabil.

Lemma 2.1.10. *Sei σ eine stabile differentielle Termordnung auf $\mathbb{T}^n$.*

a) Ist σ ordnungskompatibel, so ist σ auch strikt stabil.
b) Ist σ ∂-lexikographisch, so ist σ strikt stabil.

Beweis. Für den Beweis von a) betrachten wir Terme $t_1, t_2 \in \mathbb{T}^n$ mit $t_1 <_\sigma t_2$. Ist $\mathrm{ord}(t_1) < \mathrm{ord}(t_2)$, dann gilt auch $\mathrm{ord}(\partial t_1) < \mathrm{ord}(\partial t_2)$, also $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$. Im Fall $\mathrm{ord}(t_1) = \mathrm{ord}(t_2) = k$ schreiben wir zunächst $t_1 = \tilde{t}_1 u_1 \cdots u_n$ bzw. $t_2 = \tilde{t}_2 v_1 \cdots v_m$ mit Termen $\tilde{t}_1, \tilde{t}_2 \in \mathbb{T}^n$ der Ordnung echt kleiner k und Derivaten $u_1, \ldots, u_n, v_1, \ldots, v_m \in \mathbb{D}^n$ der Ordnung k. O.B.d.A. sei dabei $\mathrm{LT}_\sigma(\partial t_1) = \tilde{t}_1 u_1 \cdots u_n^{(1)}$ bzw. $\mathrm{LT}_\sigma(\partial t_2) = \tilde{t}_2 v_1 \cdots v_m^{(1)}$. Dann ist $\mathrm{LT}_\sigma(\partial t_1) \geq_\sigma \mathrm{LT}_\sigma(\partial t_2)$ wegen der Stabilität von σ, wobei Gleichheit genau dann gilt, wenn $\tilde{t}_1 = \tilde{t}_2$, $u_1 \cdots u_{n-1} = v_1 \cdots v_{m-1}$ und $u_n^{(1)} = v_n^{(1)}$, also wenn $t_1 = t_2$ gilt.

Sei nun σ eine stabile, ∂-lexikographische differentielle Termordnung auf $\mathbb{T}^n$ und seien $u, v \in \mathbb{D}^n$ Derivate mit $u <_\sigma v$. Dann gilt $\mathrm{LT}_\sigma(\partial(uv)) = \mathrm{LT}_{\sigma\mathtt{Lex}}(u\partial v + v\partial u) = u\partial v$. Für jeden Term $t \in \mathbb{T}^n$ ergibt sich daraus $\mathrm{LT}_\sigma(\partial t) = \tilde{t}\,\partial(\mathrm{LD}_\sigma(t))$ mit $\tilde{t} \in \mathbb{T}^n$. Sind nun $t_1, t_2 \in \mathbb{T}^n$ mit $t_1 <_\sigma t_2$, so erhalten wir

$$\tilde{t}_1 \partial(\mathrm{LD}_\tau(t_1)) = \mathrm{LT}_\sigma(\partial t_1) \leq_\sigma \mathrm{LT}_\sigma(\partial t_2) = \tilde{t}_2 \partial(\mathrm{LD}_\tau(t_2))$$

für gewisse $\tilde{t}_1, \tilde{t}_2 \in \mathbb{T}^n$. Gilt dabei $\mathrm{LD}_\tau(t_1) = \mathrm{LD}_\tau(t_2)$, so muss $\tilde{t}_1 <_\sigma \tilde{t}_2$ und damit $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$ gelten. Ist $\mathrm{LD}_\tau(t_1) <_\sigma \mathrm{LD}_\tau(t_2)$, also $t_1 <_{\sigma\mathtt{Lex}} t_2$, so folgt $\mathrm{LT}_\sigma(\partial t_1) <_{\sigma\mathtt{Lex}} \mathrm{LT}_\sigma(\partial t_2)$, d.h. insbesondere $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$. Gilt schließlich $\mathrm{LD}_\tau(t_1) >_\sigma \mathrm{LD}_\tau(t_2)$, so folgt $\mathrm{LT}_\sigma(\partial t_1) \neq \mathrm{LT}_\sigma(\partial t_2)$, also wieder $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$.
□

Dass nicht jede strikt stabile differentielle Termordnung zugleich ∂-lexikographisch ist, zeigt das folgende Beispiel.

Beispiel 2.1.11. Sei $D = \mathbb{Q}\{y_1, y_2\}$ und σ die gewichtskompatible differentielle Termordnung, die Terme in $\mathbb{T}^2$ mit gleichem Gewicht zunächst lexikographisch nach ihrem y_2-Anteil und solche mit identischen y_2-Anteil lexikographisch nach ihrem y_1-Anteil ordnet. Durch σ ist eine strikt stabile differentielle Termordnung definiert, denn für $t_1, t_2 \in \mathbb{T}^2$ mit $t_1 <_\sigma t_2$ gilt entweder $w(t_1) < w(t_2)$ oder $w(t_1) = w(t_2)$. Im ersten Fall ergibt sich $w(\partial t_1) < w(\partial t_2)$ nach Lemma 1.2.3 b) und damit $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$. Im zweiten Fall ist nun entweder der y_2-Anteil von t_1 lexikographisch kleiner als der von t_2, womit auch der y_2-Anteil von $\mathrm{LT}_\sigma(\partial t_1)$ lexikographisch kleiner wäre als der von $\mathrm{LT}_\sigma(\partial t_2)$, oder diese sind gleich und es ist $t_1 <_{\sigma\mathtt{Lex}} t_2$. Dann gilt aber auch $\mathrm{LT}_\sigma(\partial t_1) <_\sigma \mathrm{LT}_\sigma(\partial t_2)$, da $\sigma\mathtt{Lex}$ strikt stabil ist. Wir betrachten nun den Term $t = y_1^{(1)} y_2$ mit $\partial t = y_1^{(2)} y_2 + y_1^{(1)} y_2^{(1)}$. Dabei ist $y_1^{(1)} y_2^{(1)}$ der Leitterm von ∂t bzgl. σ, aber $y^{(1)} >_\sigma y_2$, d.h. σ ist nicht ∂-lexikographisch.

Beschränken wir uns auf die Klasse der strikt stabilen differentiellen Termordnungen, so gilt die gewünschte Zusatzeigenschaft. Darüber hinaus lässt sich der Leitterm der k-ten Derivation eines Polynoms für ein beliebiges $k \geq 0$ direkt angeben. Denn die Leitterme aller Derivationen eines Polynoms unterscheiden sich nur in einem Derivat.

Satz 2.1.12. *Sei $f \in D \backslash K$ ein Polynom und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$.*

a) Es gilt $\mathrm{LT}_\sigma(\partial f) = \mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f)))$.
b) Es existiert ein differentieller Term $t \in \mathbb{T}^n$ und ein Derivat $u \in \mathbb{D}^n$, so dass gilt $\mathrm{LT}_\sigma(f^{(k)}) = tu^{(k)}$ für alle $k \geq 0$.
c) Ist $\mathrm{LT}_\sigma(f^{(k)}) = tu^{(k)}$ wie in b) und $v \in \mathbb{D}^n$ ein Derivat mit $u^{(1)} v >_\sigma uv^{(1)}$, so gilt $\mathrm{LT}_\sigma(\partial^k(vf)) = v\,\mathrm{LT}_\sigma(f^{(k)})$.

Beweis. Für den Beweis von a) sei $t \in \mathrm{Supp}(f) \backslash \{\mathrm{LT}_\sigma(f)\}$. Dann impliziert die strikte Stabilität von σ gerade $\mathrm{LT}_\sigma(\partial t) <_\sigma \mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f)))$. Mit Lemma 1.2.3 a) gilt zusätzlich $\partial(\mathrm{LT}_\sigma(f)) \notin K$ und damit $\mathrm{LT}_\sigma(\partial f) = \mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f)))$.

Ist $\mathrm{LT}_\sigma(f) = u_1 \cdots u_m$ der Leitterm von f bzgl. σ mit Derivaten $u_1, \ldots, u_m \in \mathbb{D}^n$, so gilt also $\mathrm{LT}_\sigma(\partial f) = \mathrm{LT}_\sigma(\partial(\mathrm{LT}_\sigma(f))) = \mathrm{LT}_\sigma(\partial(u_1 \cdots u_m)) = u_1 \cdots u_{i-1} u_i^{(1)} u_{i+1} \cdots u_m$ für ein $i \in \{1, \ldots, m\}$. Demnach ist $u_j u_i^{(1)}$ bzgl. σ echt größer als $u_i u_j^{(1)}$ für alle $j \in \{1, \ldots, m\}$ mit $u_j \neq u_i$. Mit der strikten Stabilität von σ folgt nun

$$\mathrm{LT}_\sigma(u_j^{(1)} u_i^{(1)} + u_j u_i^{(2)}) = \mathrm{LT}_\sigma(\partial(u_j u_i^{(1)})) >_\sigma \mathrm{LT}_\sigma(\partial(u_i u_j^{(1)})) = \mathrm{LT}_\sigma(u_i^{(1)} u_j^{(1)} + u_i u_j^{(2)}).$$

Also ist $u_j u_i^{(2)}$ der Leitterm von $\mathrm{LT}_\sigma(\partial(u_j u_i^{(1)}))$ und damit $u_1 \cdots u_{i-1} u_i^{(2)} u_{i+1} \cdots u_m$ der Leitterm von $\partial^2 f$ bzgl. σ. Analog erhalten wir mit $u_1 \cdots u_{i-1} u_i^{(k)} u_{i+1} \cdots u_m$ den Leitterm von $f^{(k)}$ für jedes $k \geq 0$. Wir können schließlich $t = u_1 \cdots u_{i-1} u_{i+1} \cdots u_m$ setzen.

Die Aussage in c) ergibt sich aus $\mathrm{LT}_\sigma(\partial(vf)) = \max_\sigma\{v^{(1)} tu, vtu^{(1)}\} = vtu^{(1)}$ und der strikten Stabilität von σ. $\square$

Das Derivat des Leitterms eines Polynoms, das den Leitterm der k-ten Derivation bestimmt, muss nicht zwangsläufig das bzgl. σ lexikographisch größte Derivat im differentiellen Träger des Leitterms sein. Dies ist im Allgemeinen nur für solche σ zutreffend, die auch ∂-lexikographisch sind.

Im restlichen Teil dieses Abschnitts wollen wir noch zeigen, dass jede differentielle Termordnung σ auch eine Wohlordnung auf der Menge $\mathbb{T}^n$ definiert. Dies stellt sicher, dass wir in jeder beliebigen nicht-leeren Teilmenge von Termen ein bzgl. σ minimales Element finden.

Satz 2.1.13. *Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$ und $t_1 \geq_\sigma t_2 \geq_\sigma \cdots$ eine absteigende Kette von Termen. Existiert ein $M \in \mathbb{N}$ mit $\deg(t_i) \leq M$ für alle $i \in \mathbb{N}$, so wird die Kette stationär.*

Beweis. Sei $t_1 \geq_\sigma t_2 \geq_\sigma \cdots$ eine absteigende Kette von Termen $t_1, t_2, \ldots \in \mathbb{T}^n$ und $t_{d1} \geq_\sigma t_{d2} \geq_\sigma \cdots$ die Teilkette aller Terme vom Grad $d \leq M$. Wir zeigen mit Induktion nach d, dass diese stationär wird und damit auch $t_1 \geq_\sigma t_2 \geq_\sigma \cdots$. Für $d = 0$ ist $t_{di} = 1$ für alle $i \in \mathbb{N}$, d.h. die Kette ist stationär. Sei die Behauptung nun für alle Teilketten vom Grad echt kleiner d bewiesen. Da σ nach Satz 1.4.3 eine Wohlordnung auf $\mathbb{D}^n$ ist, existiert in der Menge $\{\mathrm{LD}_\tau(t_{di}) \mid i \in \mathbb{N}\}$ ein bzgl. σ kleinstes Derivat $\mathrm{LD}_\tau(t_{di_1})$ für ein $i_1 \in \mathbb{N}$. Auf die gleiche Weise erhalten wir für die Menge $\{\mathrm{LD}_\tau(t_{di}) \mid i > i_1\}$ ein bzgl. σ kleinstes Derivat $\mathrm{LD}_\tau(t_{di_2})$. Setzen wir dies fort, so ergibt sich eine absteigende Kette $t_{di_1} \geq_\sigma t_{di_2} \geq_\sigma \cdots$ von Termen mit $\mathrm{LD}_\tau(t_{di_1}) \leq_\sigma \mathrm{LD}_\tau(t_{di_2}) \leq_\sigma \cdots$. Dann ist $\frac{t_{di_1}}{\mathrm{LD}_\tau(t_{di_1})} \geq_\sigma \frac{t_{di_2}}{\mathrm{LD}_\tau(t_{di_2})} \geq_\sigma \cdots$ eine absteigende Kette von Termen vom Grad $d-1$, die nach Induktionsvoraussetzung stationär wird. Dies hat zur Folge, dass $t_{di_1} \geq_\sigma t_{di_2} \geq_\sigma \cdots$ und damit auch $t_{d1} \geq_\sigma t_{d2} \geq_\sigma \cdots$ stationär wird, also die Behauptung bewiesen ist. □

Satz 2.1.14. *Jede differentielle Termordnung auf $\mathbb{T}^n$ ist eine Wohlordnung auf $\mathbb{T}^n$.*

Beweis. Angenommen, für eine differentielle Termordnung σ existiert eine unendliche, echt absteigende Kette $t_1 >_\sigma t_2 >_\sigma \cdots$ von Termen. Nach Satz 2.1.13 ist dann der Grad der Terme nicht beschränkt, d.h. wir dürfen O.B.d.A. annehmen, dass der Grad von t_i für jedes $i \in \mathbb{N}$ echt kleiner als $\deg(t_{i+1})$ ist. Für jedes $i \in \mathbb{N}$ schreiben wir nun t_i als $t_i = \bar{t}_i\tilde{t}_i$ mit $\bar{t}_i, \tilde{t}_i \in \mathbb{T}^n$, so dass $u <_\sigma \mathrm{LD}_\tau(t_1)$ für alle $u \in \mathbb{D}(\bar{t}_i)$ und $u \geq_\sigma \mathrm{LD}_\tau(t_1)$ für alle $u \in \mathbb{D}(\tilde{t}_i)$. Hierbei ist der Grad der Terme $\tilde{t}_i$ beschränkt. Wäre dies nicht der Fall, so gäbe es einen Index $j \in \mathbb{N}$ mit $\deg(\tilde{t}_j) > \deg(t_1)$ im Widerspruch zu $t_1 >_\sigma t_j$. Nach Satz 2.1.13 gibt es daher in der Folge $(\tilde{t}_i)_{i\in\mathbb{N}}$ ein bzgl. σ minimales Element $\tilde{t}_{i_1}$. Analog finden wir ein solches Element $\tilde{t}_{i_2}$ in der Folge $(\tilde{t}_i)_{i>i_1}$. Wir erhalten derart eine unendlich aufsteigende Kette $\tilde{t}_{i_1} \leq_\sigma \tilde{t}_{i_2} \leq_\sigma \cdots$ von Termen. Zu dieser finden wir entsprechend die absteigende Kette $\bar{t}_{i_1} >_\sigma \bar{t}_{i_2} >_\sigma \cdots$ mit $\mathrm{LD}_\tau(t_1) >_\sigma \mathrm{LD}_\tau(\bar{t}_{i_1})$. Wieder muss der Grad der Terme unbeschränkt sein. Da wir die obigen Überlegungen beliebig oft wiederholen können, erhalten wir auf diese Weise eine bzgl. σ unendliche, echt absteigende Kette von Derivaten. Dies liefert schließlich einen Widerspruch zur Wohlordnungseigenschaft von σ auf $\mathbb{D}^n$. □

2.2 Differentielle Reduktion

Mit dem Begriff des Leitterms lässt sich neben der differentiellen Pseudo-Reduktion eine zweite Ersetzungsregel für differentielle Polynome definieren. Dabei erweitern wir die übliche Definition der Termersetzung wie folgt. Ein Polynom $f \in D$ soll genau dann bzgl. eines Polynoms $g \in D\backslash\{0\}$ reduzierbar sein, falls es im Träger von f einen Term gibt, der Vielfaches des Leitterms einer geeigneten k-ten Derivation von g ist. Der entsprechende Summand von f wird im Reduktionsschritt dann durch $g^{(k)} - \mathrm{LM}_\sigma(g^{(k)})$ ersetzt. Wir werden zeigen, dass für eine Teilmenge $G \subseteq D\backslash\{0\}$ das zugehörige Termersetzungssystem noethersch ist, d.h. das jedes Polynom bzgl. G nur endlich oft reduziert werden kann. Dies basiert im Wesentlichen auf der Wohlordnungseigenschaft der zugrunde liegenden differentiellen Termordnung.

Ferner formulieren wir die differentielle Version des Divisionsalgorithmus. Dieser liefert zu einem Polynom $f \in D$ und einem Tupel $(g_1, \ldots, g_s) \in (D\backslash\{0\})^s$ ein bzgl. $\{g_1, \ldots, g_s\}$ reduziertes Polynom g, so dass f bzgl. $\{g_1, \ldots, g_s\}$ zu g reduziert.

In diesem Abschnitt sei wieder $D = K\{y_1, \ldots, y_n\}$ und σ eine differentielle Termordnung auf $\mathbb{T}^n$.

Definition 2.2.1. Seien $f, g \in D$ mit $g \neq 0$ und $G \subseteq D\backslash\{0\}$.

1) Existiert ein differentieller Term $t \in \mathrm{Supp}(f)$ mit $t = \tilde{t}\,\mathrm{LT}_\sigma(g^{(k)})$ für ein $\tilde{t} \in \mathbb{T}^n$ und $k \in \mathbb{N}_0$, so sagen wir: *g reduziert f in einem Schritt zu* $\tilde{f} = f - \frac{c}{\mathrm{LC}_\sigma(g^{(k)})}\tilde{t}g^{(k)}$, wobei c der Koeffizient von f in t ist, und schreiben dafür $f \xrightarrow{g} \tilde{f}$.
2) Es bezeichne $\xrightarrow{G}$ den reflexiven, transitiven Abschluss von $\bigcup_{g\in G} \xrightarrow{g}$ und $\xleftrightarrow{G}$ die zugehörige Äquivalenzrelation. Die Relation $\xrightarrow{G}$ heißt auch *Termersetzungssystem*.
3) Das Polynom f heißt *reduzibel* bzgl. G, falls es ein Element $g \in G$ gibt, welches f reduziert. Andernfalls heißt f *reduziert* bzgl. G. Die Menge G heißt reduziert, falls jedes $g \in G$ bzgl. $G\backslash\{g\}$ reduziert ist.
4) Das Termersetzungssystem $\xrightarrow{G}$ heißt *noethersch*, falls es keine unendliche Reduktionskette $f_1 \xrightarrow{g_1} f_2 \xrightarrow{g_2} \cdots$ mit Polynomen $f_i \in D\backslash\{0\}$ und $g_i \in G$ für $i \in \mathbb{N}$ gibt. Es heißt *konfluent*, falls für alle $f, f_1, f_2 \in D$ mit $f \xrightarrow{G} f_1$ und $f \xrightarrow{G} f_2$ ein $f_3 \in D$ existiert mit $f_1 \xrightarrow{G} f_3$ und $f_2 \xrightarrow{G} f_3$. Das Termersetzungssystem heißt *lokal konfluent*, falls für alle $f, f_1, f_2 \in D$ und $g_1, g_2 \in G$ mit $f \xrightarrow{g_1} f_1$ und $f \xrightarrow{g_2} f_2$ ein $f_3 \in D$ existiert mit $f_1 \xrightarrow{G} f_3$ und $f_2 \xrightarrow{G} f_3$. Ist $\xrightarrow{G}$ noethersch und konfluent, so heißt es auch *konvergent*.

Beispiel 2.2.2. Sei $D = \mathbb{Q}\{y_1, y_2\}$ und σ eine gewichtskompatible differentielle Termordnung mit $y_1 <_\sigma y_2$. Wir betrachten die Menge $G = \{g_1, g_2\} \subseteq D$ mit $g_1 = y_1 y_2^{(1)} + y_1^2$ und $g_2 = (y_2^{(1)})^2 + y_2$. Dann ergeben sich die Leitterme $\mathrm{LT}_\sigma(g_1) = y_1 y_2^{(1)}$, $\mathrm{LT}_\sigma(g_2) = (y_2^{(1)})^2$ und $\mathrm{LT}_\sigma(g_1^{(1)}) = y_1 y_2^{(2)}$, $\mathrm{LT}_\sigma(g_2^{(1)}) = y_2^{(1)} y_2^{(2)}$. Für das Polynom $f = y_1 y_2^{(1)} y_2^{(2)}$ erhalten wir bzgl. G die Reduktionskette

$$\begin{aligned} f &\xrightarrow{g_1} f - y_2^{(1)} g_1^{(1)} = -y_1^{(1)}(y_2^{(1)})^2 - 2y_1 y_1^{(1)} y_2^{(1)} \xrightarrow{g_1} -y_1^{(1)}(y_2^{(1)})^2 + 2y_1^2 y_1^{(1)} \\ &\xrightarrow{g_2} 2y_1^2 y_1^{(1)} + y_1^{(1)} y_2 = \tilde{f}. \end{aligned}$$

Das Polynom $\tilde{f}$ ist reduziert bzgl. G. Ein weiteres solches Element ist $\frac{1}{2}\, y_1^2$ mit

$$f \xrightarrow{g_2} f - \tfrac{1}{2}\, y_1 g_2^{(1)} = -\tfrac{1}{2}\, y_1 y_2^{(1)} \xrightarrow{g_1} \tfrac{1}{2}\, y_1^2.$$

Das obige Beispiel zeigt, dass Reduktionen bzgl. einer Menge von Polynomen nicht immer zu einem eindeutigen Ergebnis führen. Unter welchen Bedingungen dies dennoch erfüllt ist, werden wir später noch genauer erörtern.

Lemma 2.2.3. *Sei $G \subseteq D\backslash\{0\}$ und seien $f, f_1, f_2, f_3, f_4 \in D\backslash\{0\}$.*

a) Aus $f_1 \xrightarrow{G} f_2$ und $f_2 \xrightarrow{G} f_1$ folgt $f_1 = f_2$.
b) Aus $f_1 \xrightarrow{G} f_2$ folgt $tf_1 \xrightarrow{G} tf_2$ für alle $t \in \mathbb{T}^n$.
c) Gilt $f_1 \xleftrightarrow{G} f_2$ und $f_3 \xleftrightarrow{G} f_4$, so auch $f_1 + f_3 \xleftrightarrow{G} f_2 + f_4$.
d) Es gilt $f \xleftrightarrow{G} 0$ genau dann, wenn $f \in \langle G \rangle_\partial$.

Beweis. In jedem Reduktionsschritt wird ein Term durch bzgl. σ kleinere Terme ersetzt. Gilt $f_1 \xrightarrow{G} f_2 \xrightarrow{G} f_1$ für Polynome $f_1, f_2 \in D\backslash\{0\}$, so wird bei der Reduktion $f_1 \xrightarrow{G} f_2$ in keinem der zugehörigen Schritte der Leitterm von f_1 reduziert, da sonst $\mathrm{LT}_\sigma(f_1) >_\sigma \mathrm{LT}_\sigma(f_2) \geq_\sigma \mathrm{LT}_\sigma(f_1)$ gelten würde. Mit dem gleichen Argument können auch die restlichen Terme von f nicht reduziert werden, d.h. es gilt bereits $f_1 = f_2$ und damit a).

Da b) offensichtlich für jeden einzelnen Reduktionsschritt gilt, ist die Aussage auch für die gesamte Reduktionskette erfüllt.

Für c) genügt es zu zeigen, dass $h_1 + f_3 \xleftrightarrow{G} h_2 + f_3$ für alle $h_1, h_2 \in D$ und $g \in G$ aus $h_1 \xrightarrow{g} h_2$ folgt, denn dies induziert $f_1 + f_3 \xleftrightarrow{G} f_2 + f_3$. Sei also $t = \tilde{t}\, \mathrm{LT}_\sigma(g^{(k)}) \in \mathrm{Supp}(h_1)$ für ein $\tilde{t} \in \mathbb{T}^n$ und ein $k \geq 0$. Dann ist $h_2 = h_1 - c\tilde{t}g^{(k)}$ mit $c \in K\backslash\{0\}$. Es bezeichne $\tilde{c}$ den Koeffizienten von t in f_3. Ist $\tilde{c} = -c\,\mathrm{LC}_\sigma(g^{(k)})$, so gilt $t \notin \mathrm{Supp}(h_1 + f_3)$ und $h_2 + f_3 = h_1 + f_3 - c\tilde{t}g^{(k)} \xrightarrow{g} h_1 + f_3$. Andernfalls ergibt sich

$$h_1 + f_3 \xrightarrow{g} h_1 + f_3 - \left(c + \tfrac{\tilde{c}}{\mathrm{LC}_\sigma(g^{(k)})}\right) \tilde{t}g^{(k)} = h_2 + f_3 - \tfrac{\tilde{c}}{\mathrm{LC}_\sigma(g^{(k)})}\, \tilde{t}g^{(k)} \xleftarrow{g} h_2 + f_3.$$

Für den Beweis von d) sei zunächst $f \xleftrightarrow{G} 0$. Dann können wir f schreiben als $\sum_{i=1}^r c_i t_i g_i^{(k_i)}$ für gewisse $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}^n$, $k_i \in \mathbb{N}_0$ und $g_i \in G$ für $i = 1, \ldots, r$. Also gilt $f \in \langle G \rangle_\partial$. Umgekehrt besitzt f wieder eine solche Darstellung. Wegen $g_i^{(k_i)} \xleftrightarrow{G} 0$ und b) erhalten wir $c_i t_i g_i^{(k_i)} \xleftrightarrow{G} 0$ für $i = 1, \ldots, r$ und mit c) schließlich die Behauptung. $\square$

Die Wohlordnungseigenschaft einer differentiellen Termordnung garantiert nun die Endlichkeit einer jeden Reduktionskette. Damit lässt sich jedes Polynom in endlich vielen Schritten bzgl. G zu einem reduzierten Element reduzieren.

Satz 2.2.4. *Ist $G \subseteq D\backslash\{0\}$ eine Menge von Polynomen, so ist das zugehörige Termersetzungssystem $\xrightarrow{G}$ noethersch.*

Beweis. Angenommen, es existiert eine unendliche Reduktionskette $f_1 \xrightarrow{g_1} f_2 \xrightarrow{g_2} \cdots$ mit Polynomen $f_1, f_2, \ldots \in D\backslash\{0\}$ und $g_1, g_2, \ldots \in G$. In jedem Reduktionsschritt wird dabei ein Term durch eine Summe von bzgl. σ echt kleineren ersetzt. Bezeichnet t_i für jedes $i \in \mathbb{N}$ den im i-ten Schritt reduzierten Term, so besitzt die Menge $\{t_i \mid i \in \mathbb{N}\}$ ein bzgl. σ maximales Element $\tilde{t}_1$ mit zugehörigem Index i_1. Sei nun $\tilde{t}_2 = \max_\sigma\{t_i \mid i > i_1\}$. Setzen wir dies fort, so erhalten wir eine unendliche, echt absteigende Kette $\tilde{t}_1 >_\sigma \tilde{t}_2 >_\sigma \cdots$ von Termen im Widerspruch zu der Tatsache, dass σ eine Wohlordnung auf $\mathbb{T}^n$ ist. □

Für ein Polynom $f \in D$ lässt sich nun ein bzgl. G reduziertes Polynom mit $f \xrightarrow{G} g$ algorithmisch berechnen. Da das zugehörige Termersetzungssystem noethersch ist, ist dabei garantiert, dass die Berechnung in endlich vielen Schritten erfolgen kann.

Satz 2.2.5 (Der differentielle Divisionsalgorithmus)**.**
Seien $s \geq 1$ und $f, g_1, \ldots, g_s \in D\backslash\{0\}$. Wir betrachten die folgenden Instruktionen:

1) *Seien $\tilde{f} = f$, $g = 0$ und $n_i = 0$ für $i = 1, \ldots, s$.*
2) *Bestimme den kleinsten Index $i \in \{1, \ldots, s\}$, so dass $\mathrm{LT}_\sigma(\tilde{f}) = t\,\mathrm{LT}_\sigma(g_i^{(k)})$ für ein minimales $k \in \mathbb{N}_0$ und ein $t \in \mathbb{T}^n$ gilt. Existiert solch ein i,*
   - *setze $q_{ij} = 0$ für $j = n_i + 1, \ldots, k$ und $n_i = k$, falls $k > n_i$,*
   - *ersetze q_{ik} durch $q_{ik} + \frac{\mathrm{LC}_\sigma(\tilde{f})}{\mathrm{LC}_\sigma(g_i^{(k)})}t$,*
   - *ersetze $\tilde{f}$ durch $\tilde{f} - \frac{\mathrm{LC}_\sigma(\tilde{f})}{\mathrm{LC}_\sigma(g_i^{(k)})}tg_i^{(k)}$,*
   - *fahre mit 2) fort, falls $\tilde{f} \neq 0$.*
3) *Ist $\tilde{f} \neq 0$, so ersetze g durch $g + \mathrm{LM}_\sigma(\tilde{f})$ und $\tilde{f}$ durch $\tilde{f} - \mathrm{LM}_\sigma(\tilde{f})$. Ist $\tilde{f} \neq 0$, so fahre mit 2) fort.*
4) *Gib $(g, [q_{10}, \ldots, q_{1n_1}], \ldots, [q_{s0}, \ldots, q_{sn_1}])$ aus und stoppe.*

Dies ist ein Algorithmus, dessen Ausgabe die folgenden Bedingungen erfüllt:

a) *Es gilt $f = g + \sum\limits_{i=1}^{s}\sum\limits_{j=0}^{n_i} q_{ij}g_i^{(j)}$.*
b) *Das Polynom g ist reduziert bzgl. $\{g_1, \ldots, g_s\}$.*
c) *Für jedes $i \in \{1, \ldots, s\}$, $j \in \{1, \ldots, n_i\}$ mit $q_{ij} \neq 0$ und jeden Term $t \in \mathrm{Supp}(q_{ij})$ ist $t\,\mathrm{LT}_\sigma(g_i^{(j)}) \notin \{t\,\mathrm{LT}_\sigma(g_i^{(k)}) \mid t \in \mathbb{T}^n, 0 \leq k < j\}$ und reduziert bzgl. $\{g_1, \ldots, g_{i-1}\}$.*
d) *Für jedes $i \in \{1, \ldots, s\}$ und $j \in \{0, \ldots, n_i\}$ mit $q_{ij} \neq 0$ gilt $\mathrm{LT}_\sigma(q_{ij}g_i^{(j)}) \leq_\sigma \mathrm{LT}_\sigma(f)$.*
e) *Der Vektor $(g, [q_{10}, \ldots, q_{1n_1}], \ldots, [q_{s0}, \ldots, q_{sn_1}])$ ist durch die Aussagen a)–d) eindeutig bestimmt.*

Beweis. Um a) zu zeigen, befassen wir uns zunächst mit der Korrektheit des Algorithmus. Diese ergibt sich aus der Tatsache, dass nach jedem Schritt die Gleichung $f = \tilde{f} + g + \sum_{i=1}^{s} \sum_{j=1}^{n_i} q_{ij} g_i^{(j)}$ erfüllt ist. Mit $\tilde{f} = 0$ in Schritt 4) erhalten wir dann die gewünschte Darstellung von f. Es bleibt noch zu beweisen, dass der Algorithmus terminiert. Die Schritte 2) und 3) werden nur endlich oft durchgeführt, da entweder der Leitterm von $\tilde{f}$ bzgl. σ durch kleinere Terme ersetzt oder komplett gestrichen wird. Nach jedem solchen Schritt verkleinert sich also der Leitterm von $\tilde{f}$ bzgl. σ, was wegen der Wohlordnungseigenschaft von σ nur endlich oft möglich ist. Schließlich lässt sich in endlich vielen Schritten entscheiden, ob ein entsprechender Index i im zweiten Schritt existiert. Denn für jedes $i \in \{1, \dots, s\}$ gilt $w(\mathrm{LT}_\sigma(g_i^{(k)})) > w(\mathrm{LT}_\sigma(\tilde{f}))$ für ein $k \in \mathbb{N}$ nach Lemma 1.2.3. Damit kann $\mathrm{LT}_\sigma(\tilde{f})$ aber kein Vielfaches von $\mathrm{LT}_\sigma(g_i^{(k)})$ sein.

Zudem ist die Aussage b) erfüllt, da in Schritt 3) ein skalares Vielfaches eines Terms nur dann zu g addiert wird, wenn dieser nicht Vielfaches eines Terms $\mathrm{LT}_\sigma(g_i^{(k)})$ ist.

Analog ergibt sich c) aus der Tatsache, dass in Schritt 2) der Index und die Ordnung der Derivation von g_i minimal gewählt werden.

Für jeden Term t, dessen skalares Vielfaches zu q_{ij} hinzuaddiert wird, gilt im zugehörigen Schritt 2) die Relation $\mathrm{LT}_\sigma(\tilde{f}) = t\,\mathrm{LT}_\sigma(g_i^{(k)})$. Wie bereits erwähnt, ist im Laufe des Algorithmus stets $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(\tilde{f})$ und damit d) erfüllt.

Seien schließlich $f = g + \sum_{i=1}^{s} \sum_{j=0}^{n_i} q_{ij} g_i^{(j)} = \tilde{g} + \sum_{i=1}^{s} \sum_{j=0}^{m_i} \tilde{q}_{ij} g_i^{(j)}$ zwei Darstellungen von f, die den Bedingungen a)–d) genügen. Dann ist

$$(g - \tilde{g}) + \sum_{i=1}^{s} \sum_{j=0}^{\max\{n_i, m_i\}} (q_{ij} - \tilde{q}_{ij}) g_i^{(j)} = 0,$$

wobei $q_{ij} = 0 = \tilde{q}_{ik}$ gesetzt wird für $j > n_i$ bzw. $k > m_i$. Da nach b) und c) die Leitterme aller von Null verschiedenen Summanden bzgl. σ verschieden sind, kann es solche nicht geben, d.h $g = \tilde{g}$ und $q_{ij} = \tilde{q}_{ij}$ für $i = 1, \dots, s$ und $j = 0, \dots, \max\{n_i, m_i\}$. □

Das Element g in der Ausgabe des obigen Algorithmus heißt der *differentielle Rest* von f bzgl. $\mathcal{G} = (g_1, \dots, g_s)$ und wird mit $\mathrm{DR}_{\sigma,\mathcal{G}}(f)$ bezeichnet.

Beispiel 2.2.6. Für das Polynom $f = y_1 y_2^{(1)} y_2^{(2)}$ aus Beispiel 2.2.2 ergeben sich zwei mögliche differentielle Reste. Bzgl. $\mathcal{G} = (g_1, g_2)$ erhalten wir den differentiellen Rest $\mathrm{DR}_{\sigma,\mathcal{G}}(f) = y_1^{(1)} y_2 + 2y_1^2 y_1^{(1)}$ und $\mathrm{DR}_{\sigma,\mathcal{G}}(f) = \frac{1}{2} y_1^2$ bzgl. $\mathcal{G} = (g_2, g_1)$.

2.3 Filtrierungen

Mit dem Begriff der differentiellen Termordnung wollen wir uns nun auf die Suche nach der korrekten Definition einer differentiellen Gröbnerbasis begeben. Dabei liegt es zunächst nahe, sich an der Definition einer Gröbnerbasis im Polynomring $K[x_1, \dots, x_n]$ zu orientieren. Eine Menge $G \subseteq K[x_1, \dots, x_n]$ ist bekanntlich eine Gröbnerbasis eines

Ideals I, falls die Leitterme der Polynome aus G das Leittermideal von I erzeugen. Nun gibt es mehrere Ansätze, dies auf den differentiellen Fall zu übertragen. Ein Möglichkeit wäre, für differentielle Gröbnerbasen exakt die gleiche Definition zu verwenden. Dann bestände aber keine Hoffnung auf endliche differentielle Gröbnerbasen, denn im Allgemeinen ist $\mathrm{LT}_\sigma(\partial f)$ kein Vielfaches von $\mathrm{LT}_\sigma(f)$ für ein Polynom $f \in D\backslash\{0\}$.

Ein anderer Ansatz wäre zu verlangen, dass die Leitterme der Polynome aus G das Leittermideal von I differentiell erzeugen. Dagegen spricht die Tatsache, dass das Leittermideal $\mathrm{LT}_\sigma(I)$ im Allgemeinen kein differentielles Ideal ist. In [18] wird dieses Problem umgangen, indem das Leittermideal als sogenanntes differentielles Monoideal angesehen wird, d.h. als ein multiplikatives Monoid von Termen, so dass für jeden Term t auch der Leitterm von ∂t darin enthalten ist. Eine wesentliche Voraussetzung dafür ist jedoch, dass die jeweilige differentielle Termordnung strikt stabil ist.

Eine Forderung, die sich schließlich als sinnvoll herausstellt, ist, dass das Leittermideal von I von der Menge $\{\mathrm{LT}_\sigma(g^{(k)}) \mid g \in G, k \in \mathbb{N}_0\}$ erzeugt wird. In diesem Fall lässt sich auch zeigen, dass G die üblichen äquivalenten Bedingungen erfüllt. So werden wir im nächsten Abschnitt sehen, dass für solche Mengen G jedes Polynom in I bzgl. G zu Null reduziert. Dies entspricht im Übrigen gerade der Definition einer differentiellen Gröbnerbasis in [5], wobei Carrà-Ferro nur lexikographische Termordnungen betrachtet.

Um die Wahl dieser Definition zu begründen, beschäftigen wir uns zunächst mit Filtrierungen des differentiellen Polynomrings D und den zugehörigen assoziiert graduierten Ringen. In diesem Zusammenhang betrachten wir das allgemeine Konzept der Standardbasis, die für Gröbner-Filtrierungen gerade den Begriff der differentiellen Gröbnerbasis liefert. Dabei gehen wir inhaltlich wie in [15] vor.

Sei wieder $D = K\{y_1, \ldots, y_n\}$ und σ eine differentielle Termordnung auf $\mathbb{T}^n$.

Definition 2.3.1. Sei Γ ein Monoid und σ eine Monoidordnung auf Γ. Weiter sei $F_\gamma D$ ein K-Untervektorraum von D für jedes $\gamma \in \Gamma$. Die Familie $\Phi = \{F_\gamma D \mid \gamma \in \Gamma\}$ heißt (Γ, σ)-*Filtrierung* von D, falls gilt

1) $F_\gamma D \subseteq F_{\gamma'} D$ für alle $\gamma, \gamma' \in \Gamma$ mit $\gamma \leq_\sigma \gamma'$,
2) $\bigcup_{\gamma\in\Gamma} F_\gamma D = D$,
3) $(F_\gamma D) \cdot (F_{\gamma'} D) \subseteq F_{\gamma\gamma'} D$ für alle $\gamma, \gamma' \in \Gamma$,
4) $1 \in F_1 D$ und $1 \notin F_\gamma D$ für $\gamma <_\sigma 1$.

Eine (Γ, σ)-Filtrierung Φ von D heißt *ordentlich*, falls zu jedem $f \in D\backslash\{0\}$ ein $\gamma \in \Gamma$ existiert mit $f \in (F_\gamma D)\backslash(F_{<_\sigma\gamma} D)$, wobei $F_{<_\sigma\gamma} D = \bigcup_{\gamma'<_\sigma\gamma} F_{\gamma'} D$ ist. Dann heißt γ die *Ordnung* von f bzgl. Φ und wird mit $\mathrm{ord}_\Phi(f)$ bezeichnet.

Von besonderem Interesse für uns ist die sogenannte σ-*Gröbner-Filtrierung* von D für eine differentielle Termordnung σ auf $\mathbb{T}^n$. Dazu setzen wir $\Gamma = \mathbb{T}^n$, $\Phi = \{F_t D \mid t \in \mathbb{T}^n\}$ mit $F_t D = \{f \in D\backslash\{0\} \mid \mathrm{LT}_\sigma(f) \leq_\sigma t\}$ und erhalten eine ordentliche Filtrierung von D. Für ein Polynom $f \in D\backslash\{0\}$ ist dann $\mathrm{LT}_\sigma(f)$ die Ordnung von f.

Lemma 2.3.2. *Sei $\Phi = \{F_\gamma D \mid \gamma \in \Gamma\}$ eine (Γ, σ)-Filtrierung von D, $I \subseteq D$ ein differentielles Ideal und $F_\gamma I = (F_\gamma D) \cap I$ für jedes $\gamma \in \Gamma$. Dann ist $\Psi = \{F_\gamma I \mid \gamma \in \Gamma\}$ eine (Γ, σ)-Filtrierung von I.*

Beweis. Siehe [15], Proposition 6.5.9. □

Für $\gamma, \gamma' \in \Gamma$ lässt sich eine kanonische Multiplikationsabbildung

$$F_\gamma D / F_{<_\sigma \gamma} D \times F_{\gamma'} D / F_{<_\sigma \gamma'} D \longrightarrow F_{\gamma\gamma'} D / F_{<_\sigma \gamma\gamma'} D$$

definieren. Diese ist wegen $(F_\gamma D) \cdot (F_{\gamma'} D) \subseteq F_{\gamma\gamma'} D$ wohldefiniert. Durch eine Fortsetzung dieser Multiplikation auf

$$\mathrm{gr}_\Phi(D) = \bigoplus_{\gamma \in \Gamma} F_\gamma D / F_{<_\sigma \gamma} D$$

wird auf $\mathrm{gr}_\Phi(D)$ eine K-Algebrastruktur induziert. Die K-Algebra $\mathrm{gr}_\Phi(D)$ wird auch der *assoziiert graduierte Ring* von D bzgl. Φ genannt.

Satz 2.3.3. *Die K-Algebren D und $\mathrm{gr}_\Phi(D)$ sind isomorph.*

Beweis. Siehe [15], Proposition 6.5.8. □

Definition 2.3.4. Sei Φ eine ordentliche Filtrierung von D.

1) Für ein $f \in D \backslash \{0\}$ heißt die Restklasse von f in $F_{\mathrm{ord}_\Phi(f)} D / F_{<_\sigma \mathrm{ord}_\Phi(f)} D$ die *Leitform* von f bzgl. Φ und wird mit $\mathrm{LF}_\Phi(f)$ notiert. Zusätzlich setzen wir $\mathrm{LF}_\Phi(0) = 0$.
2) Ist $I \subseteq D$ ein differentielles Ideal, so heißt $\mathrm{LF}_\Phi(I) = \langle \mathrm{LF}_\Phi(f) \mid f \in I \rangle$ das *Leitformenideal* von I bzgl. Φ.

Ist Φ die σ-Gröbner-Filtrierung von D, so lässt sich wegen $\mathrm{ord}_\Phi(f) = \mathrm{ord}_\Phi(\mathrm{LT}_\sigma(f))$ die Leitform eines Polynoms mit dessen Leitmonom bzw. Leitterm identifizieren, d.h. für jedes $f \in D \backslash \{0\}$ gilt $\mathrm{LF}_\Phi(f) = \mathrm{LF}_\Phi(\mathrm{LM}_\sigma(f))$.

Das Leitformenideal eines differentiellen Ideals $I \subseteq D$ ist im Allgemeinen kein differentielles Ideal. Genauer gesagt gibt es keine nicht-triviale Derivation $\tilde{\partial}$ auf $\mathrm{gr}_\Phi(I)$, so dass $\tilde{\partial}\,\mathrm{LF}_\Phi(f) \in \mathrm{LF}_\Phi(I)$ für jedes $f \in I$ erfüllt ist. Es gelten jedoch die folgenden Eigenschaften der Leitform.

Lemma 2.3.5. *Sei Φ die σ-Gröbner-Filtrierung von D und seien $f, g \in D$.*

a) Es gilt $\mathrm{LF}_\Phi(fg) = \mathrm{LF}_\Phi(f)\,\mathrm{LF}_\Phi(g)$.
b) Ist $\mathrm{LM}_\sigma(f) + \mathrm{LM}_\sigma(g) \neq 0$, *so gilt* $\mathrm{LF}_\Phi(f+g) = \mathrm{LF}_\Phi(f) + \mathrm{LF}_\Phi(g)$.
c) Ist σ strikt stabil, so gilt $\mathrm{LF}_\Phi(\partial f) = \mathrm{LF}_\Phi(\partial\,\mathrm{LM}_\sigma(f))$ *für alle $f \in D \backslash \{0\}$.*
d) Für jedes $h \in \mathrm{LF}_\Phi(I)$ existiert ein $\tilde{h} \in I$ mit $\mathrm{LF}_\Phi(\tilde{h}) = h$.
e) Es ist $\mathrm{gr}_\Phi(D) = K[\mathrm{LF}_\Phi(t) \mid t \in \mathbb{T}^n]$.

Beweis. Die Aussage a) gilt nach Definition der Multiplikation in $\mathrm{gr}_\Phi(D)$ und c) wegen $\mathrm{LF}_\Phi(\partial f) = \mathrm{LF}_\Phi(\mathrm{LM}_\sigma(\partial f)) = \mathrm{LF}_\Phi(\mathrm{LM}_\sigma(\partial\, \mathrm{LM}_\sigma(f))) = \mathrm{LF}_\Phi(\partial\, \mathrm{LM}_\sigma(f))$.

Für den Beweis von b) gelte $\mathrm{LM}_\sigma(f) + \mathrm{LM}_\sigma(g) \neq 0$. Besitzen f und g den gleichen Leitterm t bzgl. σ, so ergibt sich

$$\begin{aligned}\mathrm{LF}_\Phi(f+g) &= \mathrm{LF}_\Phi((\mathrm{LC}_\sigma(f) + \mathrm{LC}_\sigma(g))t)\\ &= \mathrm{LF}_\Phi(\mathrm{LC}_\sigma(f)t) + \mathrm{LF}_\Phi(\mathrm{LC}_\sigma(g)t)\\ &= \mathrm{LF}_\Phi(f) + \mathrm{LF}_\Phi(g).\end{aligned}$$

Andernfalls sei O.B.d.A. der Leitterm von f bzgl. σ echt größer als $\mathrm{LT}_\sigma(g)$. Dann folgt die Behauptung aus $\mathrm{LF}_\Phi(f) = \mathrm{LF}_\Phi(f) + \mathrm{LF}_\Phi(g)$.

Um d) zu zeigen, schreiben wir h als $h = \sum_{i=1}^s \mathrm{LF}_\Phi(f_i)\,\mathrm{LF}_\Phi(g_i) = \sum_{i=1}^s \mathrm{LF}_\Phi(f_i g_i)$ mit Polynomen $f_1,\dots,f_s \in D$, $g_1,\dots,g_s \in I$ und minimalem $s \in \mathbb{N}$. Dann sind die Leitformen der Polynome $f_i g_i$ paarweise verschieden und mit b) erhalten wir $h = \mathrm{LF}_\Phi(\tilde{h})$ für $\tilde{h} = \sum_{i=1}^s f_i g_i \in I$.

Schließlich folgt e) aus den Tatsachen, dass $\mathbb{T}^n$ den Polynomring D als K-Algebra erzeugt und dass $\mathrm{gr}_\Phi(D)$ und D nach Satz 2.3.3 als K-Algebren isomorph sind. □

Wir kommen nun zur Definition differentieller Gröbnerbasen, die sich aus dem Begriff der differentiellen Standardbasis ableiten lässt. Dabei ist die Definition der differentiellen Standardbasis eine Verallgemeinerung des üblichen Standardbasisbegriffs. Letzterer beschreibt eine Teilmenge $G \subseteq I$, so dass das Leitformenideal von I von den Leitformen der Elemente in G erzeugt wird. Da nun G genau dann ein differentielles Erzeugendensystem von I ist, wenn $\{\partial^k g \mid g \in G\}$ ein Erzeugendensystem von I ist, übertragen wir diese differentielle Sichtweise auch auf den assoziiert graduierten Ring.

Definition 2.3.6. Sei Φ eine Filtrierung von D und $I \subseteq D$ ein differentielles Ideal. Eine Teilmenge $G \subseteq I$ heißt *differentielle Φ-Standardbasis* von I, falls gilt

$$\mathrm{LF}_\Phi(I) = \langle \mathrm{LF}_\Phi(g^{(k)}) \mid g \in G, k \in \mathbb{N}_0\rangle.$$

Ist σ eine differentielle Termordnung auf $\mathbb{T}^n$ und Φ die σ-Gröbner-Filtrierung von D, so heißt G auch *differentielle σ-Gröbnerbasis* von I. Die Menge G heißt *reduzierte differentielle σ-Gröbnerbasis*, falls zusätzlich G reduziert ist.

Dass dies den Begriff der Standardbasis verallgemeinert, erklärt sich wie folgt. Der zugrunde liegende Polynomring $K[x_1,\dots,x_n]$ lässt sich als differentieller Polynomring mit der trivialen Derivation ansehen. In diesem Fall gilt aber $g^{(k)} = 0$ für alle $k > 0$ und alle $g \in G$, d.h. als Erzeuger des Leitformenideals verbleiben die Leitformen aller Elemente von G.

Da für die σ-Gröbner-Filtrierung die Leitform eines Polynoms mit dem Leitmonom zu identifizieren ist, ist eine Teilmenge G also genau dann eine differentielle σ-Gröbnerbasis von I, wenn gilt

$$\mathrm{LT}_\sigma(I) = \langle \mathrm{LT}_\sigma(g^{(k)}) \mid g \in G, k \in \mathbb{N}_0\rangle.$$

Jedes differentielle Ideal $I \subseteq D$ besitzt nun offensichtlich eine differentielle σ-Gröbnerbasis, denn für $G = I \backslash \{0\}$ ist obige Bedingung trivialerweise erfüllt. Mit den typischen Eigenschaften einer derart definierten differentiellen Gröbnerbasis werden wir uns genauer im nächsten Abschnitt auseinandersetzen.

Schließlich wollen wir noch den Zusammenhang zu der Theorie in [18] erwähnen. Dazu betrachten wir den folgenden Ansatz. Die Derivation ∂ des differentiellen Rings D induziert auf $\mathrm{gr}_\Phi(D)$ eine Abbildung δ mit $\delta(\mathrm{LF}_\Phi(f)) = \mathrm{LF}_\Phi(\partial f)$ für alle $f \in D$. Diese ist nach Lemma 2.3.5 c) wohldefiniert, falls σ strikt stabil ist.

Sind $f_1, \dots, f_s \in \mathrm{gr}_\Phi(D)$, so notieren wir mit $\langle f_1, \dots, f_s \rangle_\delta$ das kleinste Ideal von $\mathrm{gr}_\Phi(D)$, welches $f_1, \dots, f_s$ und mit jedem Element $f \in \langle f_1, \dots, f_s \rangle_\delta$ auch $\delta(f)$ enthält.

Lemma 2.3.7. *Sei σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$, $G \subseteq D$ und Φ die σ-Gröbner-Filtrierung von D.*

a) Die Abbildung δ ist eine Derivation auf $\mathrm{gr}_\Phi(D)$.
b) Für jedes differentielle Ideal $I \subseteq D$ ist das Leitformenideal bzgl. δ abgeschlossen, d.h. für jedes $f \in \mathrm{LF}_\Phi(I)$ gilt $\delta(f) \in \mathrm{LF}_\Phi(I)$.
c) Es gilt $\langle \mathrm{LF}_\Phi(g^{(k)}) \mid g \in G, k \in \mathbb{N}_0 \rangle = \langle \mathrm{LF}_\Phi(g) \mid g \in G \rangle_\delta$.

Beweis. Die Aussage in c) folgt direkt aus a) und $\mathrm{LF}_\Phi(g^{(k)}) = \delta^k(\mathrm{LF}_\Phi(g))$.

Für den Beweis von a) seien $f, g \in D$ und $c \in K$. Wegen der strikten Stabilität von σ gilt nun $c\,\mathrm{LM}_\sigma(f) + \mathrm{LM}_\sigma(g) \neq 0$ genau dann, wenn $c\,\mathrm{LM}_\sigma(\partial f) + \mathrm{LM}_\sigma(\partial g) \neq 0$. Im Fall $c\,\mathrm{LM}_\sigma(f) + \mathrm{LM}_\sigma(g) \neq 0$ erhalten wir mit Lemma 2.3.5 b)

$$\begin{aligned}\delta(c\,\mathrm{LF}_\Phi(f) + \mathrm{LF}_\Phi(g)) &= \delta(\mathrm{LF}_\Phi(cf + g)) = \mathrm{LF}_\Phi(\partial(cf + g)) \\ &= \mathrm{LF}_\Phi(c\partial f + \partial g) = c\,\mathrm{LF}_\Phi(\partial f) + \mathrm{LF}_\Phi(\partial g) \\ &= c\delta(\mathrm{LF}_\Phi(f)) + \delta(\mathrm{LF}_\Phi(g)).\end{aligned}$$

Im Fall $c\,\mathrm{LM}_\sigma(f) + \mathrm{LM}_\sigma(g) = 0$ ergibt sich direkt

$$\delta(c\,\mathrm{LF}_\Phi(f) + \mathrm{LF}_\Phi(g)) = \mathrm{LF}_\Phi(0) = c\,\mathrm{LF}_\Phi(\partial f) + \mathrm{LF}_\Phi(\partial g).$$

Insgesamt folgt damit die K-Linearität von δ. Ferner ist stets $\mathrm{LM}_\sigma(f^{(1)}g) \neq -\mathrm{LM}_\sigma(fg^{(1)})$. Mit Lemma 2.3.5 ergibt sich damit auch

$$\begin{aligned}\delta(\mathrm{LF}_\Phi(f) \cdot \mathrm{LF}_\Phi(g)) &= \delta(\mathrm{LF}_\Phi(fg)) = \mathrm{LF}_\Phi(\partial(fg)) \\ &= \mathrm{LF}_\Phi(f^{(1)}g + fg^{(1)}) = \mathrm{LF}_\Phi(f^{(1)}g) + \mathrm{LF}_\Phi(fg^{(1)}) \\ &= \delta(\mathrm{LF}_\Phi(f)) \cdot \mathrm{LF}_\Phi(g) + \mathrm{LF}_\Phi(f) \cdot \delta(\mathrm{LF}_\Phi(g)).\end{aligned}$$

Bleibt noch b) zu zeigen. Sei dazu $f \in \mathrm{LF}_\Phi(I)$. Dann existiert nach Lemma 2.3.5 d) ein Polynom $\tilde{f} \in I$ mit $\mathrm{LF}_\Phi(\tilde{f}) = f$. Somit ist $\delta(f) = \delta(\mathrm{LF}_\Phi(\tilde{f})) = \mathrm{LF}_\Phi(\partial \tilde{f}) \in \mathrm{LF}_\Phi(I)$. □

Der nächste Satz liefert nun die Erkenntnis, dass für strikt stabile differentielle Termordnungen die Definition 2.3.6 einer differentiellen Gröbnerbasis mit der in [18] übereinstimmt.

Satz 2.3.8. *Sei $I \subseteq D$ ein differentielles Ideal und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Dann sind die folgenden Bedingungen äquivalent:*

a) Die Menge G ist eine differentielle σ-Gröbnerbasis von I.
b) Es gilt $\mathrm{LF}_\Phi(I) = \langle \mathrm{LF}_\Phi(g) \mid g \in G \rangle_\delta$.

Beweis. Die Behauptung folgt direkt aus Lemma 2.3.7 c). □

Unsere Definition einer differentiellen Gröbnerbasis ist also eine sinnvolle Erweiterung auf den allgemeinen Fall. Zudem vermeiden wir die Verwendung der Abbildung δ. Diese ist zwar K-linear, induziert auf dem differentiellen Polynomring D aber keineswegs eine K-lineare Abbildung.

2.4 Charakterisierung differentieller Gröbnerbasen

In diesem Abschnitt wollen wir überprüfen, inwieweit sich die speziellen Eigenschaften der rein algebraischen Gröbnerbasen auf differentielle Gröbnerbasen übertragen lassen. Es wird sich zeigen, dass sich auch im differentiellen Fall jedes Element eines Ideals auf eine bestimmte Art und Weise in der differentiellen Gröbnerbasis darstellen lässt. Zudem erhalten wir auch in unserer Situation die Konvergenz des zugehörigen Termersetzungssystems und damit die Existenz einer Normalform.

Da, wie wir im letzten Abschnitt gesehen haben, nicht jedes differentielle Ideal eine endliche differentielle Gröbnerbasis besitzt, beschäftigen wir uns anschließend mit der Frage, unter welchen Bedingungen die Existenz einer endlichen differentiellen Gröbnerbasis gesichert ist. Dabei werden sowohl die Wahl der differentiellen Termordnung als auch das Ideal selbst bzw. dessen Dimension eine wesentliche Rolle spielen. Die hier entwickelten Charakterisierungen lassen sich als Verallgemeinerungen der Aussagen in [29] über differentielle Ideale des univariaten differentiellen Polynomrings $K\{y\}$ verstehen. Zobnin macht dabei im Wesentlichen von der Tatsache Gebrauch, dass jedes nicht-triviale differentielle Ideal stets null-dimensional ist. Seine Aussagen können daher nicht generell übertragen werden, da in unserer Situation der differentielle Faktorring D/I auch andere Dimensionen annehmen kann. Jedoch werden wir uns auch auf den null-dimensionalen Fall konzentrieren, da sich dann hinreichende Kriterien formulieren lassen.

Wie gewohnt sei $D = K\{y_1, \dots, y_n\}$ und σ eine differentielle Termordnung auf $\mathbb{T}^n$.

Satz 2.4.1. *Sei $I \subseteq D$ ein differentielles Ideal und $G \subseteq I \backslash \{0\}$. Dann sind die folgenden Aussagen äquivalent:*

a) Die Menge G ist eine differentielle σ-Gröbnerbasis von I.
b) Zu jedem Polynom $f \in I \backslash \{0\}$ existiert eine Darstellung $f = \sum_{i=1}^s f_i g_i^{(k_i)}$ mit $s \in \mathbb{N}$, $f_i \in D \backslash \{0\}$, $g_i \in G$ und $k_i \in \mathbb{N}_0$ für $i = 1, \dots, s$, so dass für jedes $i \in \{1, \dots, s\}$ gilt $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(f_i g_i^{(k_i)})$.

Beweis. Für den Beweis von a) $\Rightarrow$ b) sei G eine differentielle σ-Gröbnerbasis von I und $f_1 \in I\backslash\{0\}$. Dann existiert ein Polynom $g_1 \in G$, so dass $\mathrm{LT}_\sigma(f_1) = t_1 \,\mathrm{LT}_\sigma(g_1^{(k_1)})$ für ein $t_1 \in \mathbb{T}^n$ und ein $k_1 \in \mathbb{N}_0$ gilt. Für das Polynom $f_2 = f_1 - \frac{\mathrm{LC}_\sigma(f_1)}{\mathrm{LC}_\sigma(g_1^{(k_1)})} t_1 g_1^{(k_1)} \in I$ gilt entweder $f_2 = 0$ oder $f_2 \neq 0$ und $\mathrm{LT}_\sigma(f_1) \geq_\sigma \mathrm{LT}_\sigma(f_2)$. Im Fall $f_2 \neq 0$ finden wir wie eben ein $g_2 \in G$ mit $\mathrm{LT}_\sigma(f_2) = t_2 \,\mathrm{LT}_\sigma(g_2^{(k_2)})$ für ein $t_2 \in \mathbb{T}^n$ und ein $k_2 \in \mathbb{N}_0$. Nun ist entweder wieder $f_3 = f_2 - \frac{\mathrm{LC}_\sigma(f_2)}{\mathrm{LC}_\sigma(g_2^{(k_2)})} t_2 g_2^{(k_2)} = 0$ oder $\mathrm{LT}_\sigma(f_2) \geq_\sigma \mathrm{LT}_\sigma(f_3)$. Da das Termersetzungssystem $\xrightarrow{G}$ noethersch ist, ist die Anzahl der Wiederholungen dieses Schrittes endlich. Ist s die Anzahl dieser Schritte, so gilt also $f_1 = \sum_{i=1}^s \tilde{f}_i g_i^{(k_i)}$ für gewisse $\tilde{f}_1, \ldots, \tilde{f}_s \in D\backslash\{0\}$ und $g_1, \ldots, g_s \in G$, wobei $\mathrm{LT}_\sigma(f_1) \geq_\sigma \mathrm{LT}_\sigma(\tilde{f}_i g_i^{(k_i)})$ für $i = 1, \ldots, s$ erfüllt ist.

Es besitze nun jedes Polynom $f \in I\backslash\{0\}$ eine solche Darstellung. Dann existiert wegen $\mathrm{LT}_\sigma(f) \geq_\sigma \mathrm{LT}_\sigma(f_i g_i^{(k_i)})$ für $i = 1, \ldots, s$ ein Index $j \in \{1, \ldots, s\}$, so dass der Term $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(f_j g_j^{(k_j)}) = \mathrm{LT}_\sigma(f_j)\,\mathrm{LT}_\sigma(g_j^{(k_j)})$ im Ideal $\langle \mathrm{LT}_\sigma(g^{(k)}) \mid g \in G, k \in \mathbb{N}_0\rangle$ liegt. Damit ist G eine differentielle σ-Gröbnerbasis von I. □

Eine differentielle σ-Gröbnerbasis eines differentiellen Ideals I ist also insbesondere ein differentielles Erzeugendensystem von I. Damit folgt aber zugleich, da nicht jedes differentielle Ideal endlich erzeugt ist, dass es differentielle Ideale gibt, die für keine differentielle Termordnung σ eine endliche differentielle σ-Gröbnerbasis besitzen.

Andere zu erwartende Eigenschaften sind hingegen erfüllt.

Satz 2.4.2. *Sei $G \subseteq D\backslash\{0\}$ und I das von G differentiell erzeugte Ideal von D. Dann sind die folgenden Aussagen äquivalent:*

a) Die Menge G ist eine differentielle σ-Gröbnerbasis von I.
b) Jedes Polynom $f \in I\backslash\{0\}$ ist reduzibel bzgl. G.
c) Das Termersetzungssystem $\xrightarrow{G}$ ist konvergent.
d) Zu jedem $f \in D\backslash\{0\}$ existiert genau ein bzgl. G reduziertes Polynom $\mathrm{DN}_{\sigma,I}(f) \in D$ mit $f \xrightarrow{G} \mathrm{DN}_{\sigma,I}(f)$, die sogenannte differentielle Normalform *von f bzgl. (σ, I).*
e) Für ein $f \in D\backslash\{0\}$ gilt $f \xrightarrow{G} 0$ genau dann, wenn $f \in I$ gilt.

Beweis. Sei zunächst G eine differentielle σ-Gröbnerbasis von I und $f \in I\backslash\{0\}$. Dann existiert ein Term $t \in \mathbb{T}^n$ und ein Polynom $g \in G$, so dass $t\,\mathrm{LT}_\sigma(g^{(k)})$ für ein $k \geq 0$ der Leitterm von f bzgl. σ ist. Damit ist aber f reduzibel bzgl. G.

Sei jetzt jedes $f \in I\backslash\{0\}$ reduzibel bzgl. G. Für den Beweis der Konfluenz von $\xrightarrow{G}$ genügt es, dessen lokale Konvergenz zu zeigen. Seien dazu $f, f_1, f_2 \in D$ und $g_1, g_2 \in G$ mit $f \xrightarrow{g_1} f_1$ und $f \xrightarrow{g_2} f_2$. Da das Termersetzungssystem noethersch ist, existieren zwei bzgl. G reduzierte Polynome $\tilde{f}_1, \tilde{f}_2 \in D$ mit $f_1 \xrightarrow{G} \tilde{f}_1$ bzw. $f_2 \xrightarrow{G} \tilde{f}_2$. Dann ist auch $\tilde{f}_1 - \tilde{f}_2 \in I$ bzgl. G reduziert und mit b) folgt $\tilde{f}_1 - \tilde{f}_2 = 0$.

Wir wollen nun die Implikation c) $\Rightarrow$ d) beweisen. Da das Termersetzungssytem $\xrightarrow{G}$ noerthersch ist, existiert zu $f \in D\backslash\{0\}$ ein bzgl. G reduziertes Polynom $\mathrm{DN}_{\sigma,I}(f) \in D$

mit $f \xrightarrow{G} \mathrm{DN}_{\sigma,I}(f)$. Angenommen, es gibt ein zweites solches Element $\tilde{f} \in D$. Dann existiert wegen der Konfluenz von $\xrightarrow{G}$ ein Polynom $\bar{f} \in D$, so dass $\mathrm{DN}_{\sigma,I}(f) \xrightarrow{G} \bar{f}$ und $\tilde{f} \xrightarrow{G} \bar{f}$ erfüllt ist. Aus der Reduziertheit von $\mathrm{DN}_{\sigma,I}(f)$ und $\tilde{f}$ bzgl. G folgt daraus schließlich $\mathrm{DN}_{\sigma,I}(f) = \bar{f} = \tilde{f}$.

Für den Beweis von d) $\Rightarrow$ e) sei zunächst $f \in D \backslash \{0\}$ mit $f \xrightarrow{G} 0$. D.h. es existieren Elemente $g_1, \ldots, g_s \in G$ und $f_1, \ldots, f_{s-1} \in D \backslash \{0\}$ mit $f \xrightarrow{g_1} f_1 \xrightarrow{g_2} \cdots \xrightarrow{g_{s-1}} f_{s-1} \xrightarrow{g_s} 0$. Also lässt sich f schreiben als $f = \sum_{i=1}^{s} c_i t_i g_i^{(k_i)}$, wobei $c_i \in K \backslash \{0\}$, $k_i \in \mathbb{N}_0$ und $t_i \in \mathbb{T}^n$ für $i = 1, \ldots, s$. Hieraus folgt wegen $G \subseteq I$ direkt $f \in I$.

Umgekehrt sei jetzt $f \in I \backslash \{0\}$ gegeben. Nach Lemma 2.2.3 d) gilt dann $f \xleftrightarrow{G} 0$, d.h. es existieren $f_1, \ldots, f_s \in I$ mit $f_1 = f$, $f_s = 0$ und $f_i \xrightarrow{G} f_{i+1}$ bzw. $f_{i+1} \xrightarrow{G} f_i$ für $i = 1, \ldots, s-1$. Sei hierbei $j \in \{1, \ldots, s-2\}$ der maximale Index, für den $f_{j+1} \xrightarrow{G} f_j$ erfüllt ist. Für f_{j+1} gilt also $f_{j+1} \xrightarrow{G} 0$ und $f_{j+1} \xrightarrow{G} f_j$. Da Null ein bzgl. G reduziertes Element ist, erhalten wir mit d) schließlich $f_j \xrightarrow{G} 0$. Induktiv lässt sich nun $f \xrightarrow{G} 0$ schließen.

Es bleibt noch die Implikation e) $\Rightarrow$ a) zu zeigen. Seien dazu $f \in I \backslash \{0\}$, $g_1, \ldots, g_s \in G$ und $f_1, \ldots, f_{s-1} \in D \backslash \{0\}$ mit $f \xrightarrow{g_1} f_1 \xrightarrow{g_2} \cdots \xrightarrow{g_{s-1}} f_{s-1} \xrightarrow{g_s} 0$. Für f erhalten wir also die Darstellung $f = \sum_{i=1}^{s} c_i t_i g_i^{(k_i)}$, wobei $c_i \in K \backslash \{0\}$, $k_i \in \mathbb{N}_0$ und $t_i \in \mathbb{T}^n$ für $i = 1, \ldots, s$. Für jedes $i \in \mathbb{N}$ wird im i-ten Schritt der Reduktion immer ein Term von f_i durch kleinere bzgl. σ ersetzt. Da die Reduktionskette bei Null endet, muss dies auch für den Leitterm von f bzgl. σ in einem der Schritte gelten. D.h. es existiert ein Index $i \in \{1, \ldots, s\}$ mit $\mathrm{LT}_\sigma(f) = \mathrm{LT}_\sigma(t_i g_i^{(k_i)}) = t_i \, \mathrm{LT}_\sigma(g_i^{(k_i)}) \in \langle \mathrm{LT}_\sigma(g^{(k)}) \mid g \in G, k \in \mathbb{N}_0 \rangle$. □

Für ein differentielles Ideal $I \subseteq D$ und ein Polynom $f \in D$ hängt die differentielle Normalform von f bzgl. (σ, I) nicht von der differentiellen σ-Gröbnerbasis G von I ab, da die differentielle Normalform von f bzgl. einer anderen differentiellen Gröbnerbasis ebenfalls bzgl. G reduziert wäre, die Differenz der Normalformen als Element von I aber bzgl. G zu Null reduzieren würde.

Ist $G = \{g_1, \ldots, g_s\}$, so entspricht zudem die differentielle Normalform eines Polynoms gerade dessen differentiellem Rest bzgl. $(g_1, \ldots, g_s)$. Letzterer hängt daher nicht mehr von der gewählten Reihenfolge der Elemente $g_1, \ldots, g_s$ ab.

Korollar 2.4.3. *Ist $I \subseteq D$ ein differentielles Ideal und $G = \{g_1, \ldots, g_s\} \subseteq I \backslash \{0\}$ eine differentielle σ-Gröbnerbasis von I, so stimmen für jedes Polynom $f \in D \backslash \{0\}$ der differentielle Rest von f bzgl. $(g_1, \ldots, g_s)$ und die differentielle Normalform von f bzgl. (σ, I) überein.*

Beweis. Wird in Schritt 2) des differentiellen Divisionsalgorithmus ein Index i gefunden, so entspricht die darauffolgende Aktualisierung der beteiligten Daten gerade einem Reduktionsschritt bzgl. G. Also gilt $f \xrightarrow{G} \mathrm{DR}_{\sigma,\mathcal{G}}(f)$ für jedes $f \in D \backslash \{0\}$. Schließlich folgt $\mathrm{DN}_{\sigma,I}(f) = \mathrm{DR}_{\sigma,\mathcal{G}}(f)$ aus Satz 2.2.5 b) und Satz 2.4.2. □

Wir haben bereits gesehen, dass nicht jedes differentielle Ideal eine endliche differentielle Gröbnerbasis besitzt. Dies ist auch für differentielle Ideale, die endlich erzeugt sind, der Fall, wie das folgende Beispiel zeigt.

Beispiel 2.4.4. Wir betrachten das von y^2 differentiell erzeugte Ideal $I \subseteq \mathbb{Q}\{y\}$. Neben y^2 ist wegen $2(y^{(1)})^3 = y^{(1)}(2yy^{(2)} + 2(y^{(1)})^2) - 2yy^{(1)}y^{(2)} = y^{(1)}\partial^2 y^2 - y^{(2)}\partial y^2$ auch $(y^{(1)})^3$ ein Element des Leittermideals von I. Analog lässt sich zeigen, dass es für jede Ordnung $k \in \mathbb{N}_0$ eine Zahl $l \in \mathbb{N}$ gibt, so dass $(y^{(k)})^l \in \mathrm{LT}_{\mathtt{Lex}}(I)$ gilt. Also muss für jedes k auch ein Polynom mit einem solchen Leitterm in einer differentiellen `Lex`-Gröbnerbasis von I enthalten sein, die somit in keinem Fall endlich sein kann.

Für das Ideal im obigen Beispiel erhalten wir im Übrigen bzgl. jeder strikt stabilen differentiellen Termordnung stets eine unendliche differentielle Gröbnerbasis. Die allgemeine Situation ist aber noch komplizierter, denn es gibt differentielle Ideale, die für eine differentielle Termordnung eine endliche differentielle Gröbnerbasis besitzen und für eine andere nicht.

Beispiel 2.4.5. Sei $I \subseteq \mathbb{Q}\{y_1, y_2\}$ das von $\{y_1^{(1)}, y_1 y_2\}$ differentiell erzeugte Ideal, und seien τ_1, τ_2 Rankings auf $\mathbb{D}^2$ definiert durch $y_1 <_{\tau_1} y_2$ bzw. $y_2 <_{\tau_2} y_1$. Jedes von Null verschiedene Polynom in I ist Summe von Termen, die Vielfache von $y_1^{(k)}$ oder $y_1 y_2^{(l)}$ für ein geeignetes $k \geq 1$ bzw. $l \geq 0$ sind. Damit ist $\{y_1^{(1)}, y_1 y_2\}$ bereits eine differentielle τ_1`Lex`-Gröbnerbasis von I. Hingegen besitzt I wegen $y_1 y_2^{(l)} \in \mathrm{LT}_{\tau_2\mathtt{Lex}}(I)$ für jedes $l \geq 0$ keine endliche differentielle τ_1`Lex`-Gröbnerbasis.

Im Folgenden werden wir uns auf (strikt) stabile differentielle Termordnungen beschränken. Dies gewährleistet eine gewisse Stabilität bei der Derivation von Termen und Polynomen. Insbesondere bei strikter Stabilität können wir für jedes $f \in D \backslash K$ dann die Beziehung $\mathrm{LT}_\sigma(\partial f) = \mathrm{LT}_\sigma(\partial \, \mathrm{LT}_\sigma(f))$ verwenden. Unter dieser Voraussetzung ergibt sich eine notwendige Bedingung für die Existenz einer endlichen differentiellen Gröbnerbasis.

Satz 2.4.6. *Sei $I \subseteq D$ ein differentielles Ideal und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Besitzt I eine endliche differentielle σ-Gröbnerbasis, so existieren genau $N = n - \dim(D/I)$ paarweise verschiedene Indizes $i_1, \ldots, i_N \in \{1, \ldots, n\}$, so dass gilt $y_{i_j}^{(k_j)} \in \mathrm{LT}_\sigma(I)$ für gewisse $k_j \in \mathbb{N}_0$ und $j = 1, \ldots, N$.*

Beweis. Es bezeichne N die Anzahl der differentiellen Unbestimmten $y \in \{y_1, \ldots, y_n\}$, für die ein Derivat einer gewissen Ordnung im Leittermideal von I enthalten ist. Des Weiteren seien $G = \{g_1, \ldots, g_s\}$ eine endliche differentielle σ-Gröbnerbasis von I und $t_1, \ldots, t_s \in \mathbb{T}^n$ sowie $u_1, \ldots, u_s \in \mathbb{D}^n$, so dass für $i = 1, \ldots, s$ und jedes $k \geq 0$ gilt $\mathrm{LT}_\sigma(g_i^k) = t_i u_i^{(k)}$. Ist $Y_1 \subseteq \{y_1, \ldots, y_n\}$ eine $(\dim(D/I)+1)$-elementige Menge paarweise verschiedener differentieller Unbestimmter, so gibt es ein von Null verschiedenes Polynom $f_1 \in I \cap K\{Y_1\}$. Zugleich muss ein Element $g \in G$ existieren, so dass $\mathrm{LT}_\sigma(g^{(k)})$ für ein $k \geq 0$ ein Teiler von $\mathrm{LT}_\sigma(f_1)$ ist. Damit erhalten wir mit $G_1 = \{g \in G \mid \mathrm{LT}_\sigma(g) \in K\{Y_1\}\}$ eine nicht-leere Teilmenge von G. Sei nun $k = \max\{\mathrm{ord}(t_i) \mid g_i \in G_1, i \in \{1, \ldots, s\}\}$.

Nach Korollar 1.8.10 ist $\dim(D_t/I_t) = \dim(D/I)(t+1) + \operatorname{ord}(I)$ für $t \gg 0$. Insbesondere impliziert dies $\dim(D_t/I_t) < |Y_1|(t-k)$ für $t \gg 0$. Damit sind die Restklassen der Derivate in $\mathbb{D} = \{y^{(j)} \mid y \in Y_1, k < j \leq t\}$ in D_t/I_t algebraisch abhängig über K. Also existiert ein von Null verschiedenes Polynom $f \in I \cap K[\mathbb{D}]$. Weiter muss es ein Element $g_i \in G_1$ geben, so dass $\mathrm{LT}_\sigma(g_i^{(j)}) = t_i u_i^{(j)}$ ein Teiler von $\mathrm{LT}_\sigma(f)$ ist. Da nun jedes Derivat in $\mathbb{D}(\mathrm{LT}_\sigma(f))$ eine größere Ordnung als t_i besitzt, ergibt sich $t_i = 1$ und somit $\mathrm{LT}_\sigma(g_i) = u_i \in Y_1$. Die gleiche Überlegung können wir für eine $(\dim(D/I)+1)$-elementige Menge $Y_2 \subseteq \{y_1, \ldots, y_n\} \backslash \{\mathrm{LV}_\sigma(\mathrm{LT}_\sigma(g_i))\}$ vornehmen. Dies liefert wieder ein Element $g \in G$ mit $\mathrm{LT}_\sigma(g) \in \mathbb{D}^n$ und $\mathrm{LV}_\sigma(\mathrm{LT}_\sigma(g)) \in Y_2$. Da wir diesen Schritt insgesamt $(n - \dim(D/I))$-mal ausführen können, erhalten wir die Ungleichung $N \geq n - \dim(D/I)$.

Seien nun $g_1, \ldots, g_N \in I$ mit $\mathrm{LT}_\sigma(g_j) = y_{i_j}^{(k_j)}$ für $j = 1, \ldots, N$. Dann bildet das Tupel $(g_1^{(0)}, \ldots, g_1^{(t-\operatorname{ord}(g_1))}, \ldots, g_N^{(0)}, \ldots, g_N^{(t-\operatorname{ord}(g_N))})$ für $t \gg 0$ eine reguläre Sequenz für D_t, und wir erhalten

$$\begin{aligned}\dim(D_t/I_t) &\leq \dim(D_t/\langle g_1^{(l_1)}, \ldots, g_N^{(l_N)} \mid 0 \leq l_j \leq t - \operatorname{ord}(g_j)\rangle) \\ &= n(t+1) - \sum_{j=1}^{N}(t - \operatorname{ord}(g_j) + 1) \\ &= (n-N)t + n - N + \sum_{j=1}^{N} \operatorname{ord}(g_j).\end{aligned}$$

Für $N > n - \dim(D/I)$ ergäbe sich also

$$\begin{aligned}\dim(D_t/I_t) &\leq (\dim(D/I) - 1)t + \dim(D/I) - 1 + \sum_{j=1}^{N} \operatorname{ord}(g_j) \\ &< \dim(D/I)(t+1) + \operatorname{ord}(I)\end{aligned}$$

für $t \gg 0$, ein Widerspruch. $\square$

Ist $G \subseteq D\backslash\{0\}$ eine nicht-leere Menge von Polynomen, deren Terme vom Grad größer oder gleich zwei sind, so besagt der obige Satz, dass das von G differentiell erzeugte Ideal bzgl. jeder strikt stabilen differentiellen Termordnung eine unendliche reduzierte differentielle Gröbnerbasis besitzt, unabhängig davon, ob das Ideal selbst endlich oder unendlich erzeugt ist. Denn in diesem Fall enthält das Ideal kein von Null verschiedenes Polynom, so dass ein Derivat $y_i^{(k_i)}$ in dessen Träger enthalten ist.

Der nächste Satz liefert nun ein hinreichendes Kriterium für die Existenz einer endlichen differentiellen Gröbnerbasis. Dieses ist aber genauer betrachtet nur für den nulldimensionalen Fall von Bedeutung.

Satz 2.4.7. *Sei $I \subseteq D$ ein differentielles Ideal und σ eine ∂-lexikographische oder stabile differentielle Termordnung auf $\mathbb{T}^n$. Existiert zu jedem $i \in \{1, \ldots, n\}$ ein $k_i \geq 0$ mit $y_i^{(k_i)} \in \mathrm{LT}_\sigma(I)$, so besitzt I eine endliche differentielle σ-Gröbnerbasis.*

Beweis. Seien $f_1, \ldots, f_n \in I \backslash \{0\}$ mit $\mathrm{LT}_\sigma(f_i) = y_i^{(k_i)}$ für $i = 1, \ldots, n$ und gewisse $k_1, \ldots, k_n \in \mathbb{N}_0$. Wir betrachten die Menge $\mathbb{D} = \{y_i^{(l_i)} \mid 0 \leq l_i < k_i, i = 1, \ldots, n\}$ von Derivaten. Da der Polynomring $K[\mathbb{D}]$ noethersch ist, besitzt das Ideal $I \cap K[\mathbb{D}]$ eine endliche σ-Gröbnerbasis G. Dann ist $G \cup \{f_1, \ldots, f_n\}$ eine differentielle σ-Gröbnerbasis von I, falls $y_i^{(k_i+k)}$ für $k \geq 0$ der Leitterm von $f_i^{(k)}$ bzgl. σ ist. Ist σ stabil, so ist dies offensichtlich erfüllt. Sei σ also ∂-lexikograpisch. Angenommen, es existiert ein Term $t \in \mathbb{T}^n$ und ein Derivat $u \in \mathbb{D}^n$ mit $tu \in \mathrm{Supp}(f_i)$ und $tu^{(1)} = \mathrm{LT}_\sigma(\partial(tu)) >_\sigma y_i^{(k_i+1)}$. Wegen $y_i^{(k_i)} >_\sigma u$ ist dann $uy_i^{(k_i+1)} >_\sigma u^{(1)} y_i^{(k_i)}$ und es gilt daher

$$tu^{(1)} y_i^{(k_i)} <_\sigma tuy_i^{(k_i+1)} <_\sigma y_i^{(k_i)} y_i^{(k_i+1)},$$

d.h. $tu^{(1)} <_\sigma y_i^{(k_i+1)}$ im Widerspruch zur Wahl von tu. □

Korollar 2.4.8. *Sei $I \subseteq D$ ein null-dimensionales differentielles Ideal und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Dann sind die folgenden Aussagen äquivalent:*

a) Das Ideal I besitzt eine endliche differentielle σ-Gröbnerbasis.
b) Zu jedem $i \in \{1, \ldots, n\}$ existiert ein $k_i \geq 0$ mit $y_i^{(k_i)} \in \mathrm{LT}_\sigma(I)$.

Beweis. Die Behauptung folgt direkt aus Satz 2.4.6 und Satz 2.4.7. □

Ist die Existenz einer endlichen differentiellen Gröbnerbasis für eine strikt stabile differentielle Termordnung gesichert, so lässt sich diese Aussage zwar nicht auf jede andere strikt stabile differentielle Termordnung übertragen, aber zumindest auf diejenigen, die zusätzlich ordnungskompatibel sind.

Korollar 2.4.9. *Sei σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$ und I ein null-dimensionales differentielles Ideal von D, das eine endliche differentielle σ-Gröbnerbasis besitzt.*

a) Das Ideal I besitzt eine endliche differentielle σ`Lex`-Gröbnerbasis.
b) Für jede stabile oder ∂-lexikographische differentielle Termordnung τ, die zusätzlich ordnungskompatibel ist, existiert eine endliche differentielle τ-Gröbnerbasis von I.

Beweis. Die Aussage a) folgt aus Satz 2.4.7 und der Tatsache, dass jedes Derivat $y_i^{(k_i)}$, welches bzgl. σ als Leitterm eines Polynoms $g_i \in I$ auftritt, auch bzgl. σ`Lex` der Leitterm dieses Polynoms ist.

Für den Beweis von b) seien $g_1, \ldots, g_n \in I$ mit $g_i = y_i^{(k_i)} + \tilde{g}_i$ und $\mathrm{ord}_{y_j}(\tilde{g}_i) < k_j$ für $i, j = 1, \ldots, n$. O.B.d.A. gelte $k_1 \leq k_2 \leq \cdots \leq k_n$. Dann ist bereits $y_n^{(k_n)}$ der Leitterm von g_n bzgl. τ. Weiter lässt sich $g_{n-1}^{(k_n - k_{n-1})} = y_{n-1}^{(k_n)} + \tilde{g}_{n-1}^{(k_n - k_{n-1})}$ mittels g_n zu einem Polynom reduzieren, welches $y_{n-1}^{(k_n)}$ als Leitterm besitzt. Analog erhalten wir auch für die restlichen differentiellen Unbestimmten entsprechende Polynome in I, so dass die Bedingungen aus Satz 2.4.7 erfüllt sind. □

Zuletzt wollen wir noch kurz auf diejenigen Derivate eingehen, die als Leitterm eines Polynoms in einem differentiellen Ideal I auftreten können. Hier lässt sich ein interessanter Zusammenhang zu der Theorie der differentiellen Pseudo-Gröbnerbasen herstellen.

Satz 2.4.10. *Sei $I \subseteq D$ ein differentielles Ideal und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$, die auf $\mathbb{D}^n$ ein ordentliches Ranking definiert. Weiter seien $G_1, \ldots, G_r \subseteq D$ reduzierte differentielle σ-Pseudo-Gröbnerbasen von differentiellen Primidealen, so dass gilt $\sqrt{I} = \bigcap_{i=1}^{r}(\langle G_i \rangle_\partial : h_{G_i}^\infty)$. Ist $y^{(k)} \in \mathrm{LT}_\sigma(I)$ für ein $k \geq 0$ und ein $y \in \{y_1, \ldots, y_n\}$, so existiert für $i = 1, \ldots, r$ ein Polynom $g_i \in G_i$ mit $\mathrm{LV}_\sigma(g_i) = y$.*

Beweis. Sei $f \in I \backslash \{0\}$ mit $\mathrm{LT}_\sigma(f) = y^{(k)}$. Angenommen, es existiert ein $j \in \{1, \ldots, r\}$, so dass $\mathrm{LV}(g) \neq y$ für alle $g \in G_j$ gilt. Wir schreiben $f = y^{(k)} + \tilde{f}$, wobei y in $\tilde{f} \in D$ höchstens zur Ordnung $k - 1$ und jede andere differentielle Unbestimmte höchstens zur Ordnung k vorkommt. Dies ist möglich, da σ auf $\mathbb{D}^n$ ein ordentliches Ranking definiert. In einem Pseudo-Reduktionsschritt mit einem $g \in G_j$ werden nun Summanden von $\mathrm{in}_\tau(g^{(l)})f$ der Ordnung kleiner oder gleich k durch ein Polynom der Ordnung kleiner oder gleich k ersetzt. Wegen $y^{(k)} >_\sigma u$ für alle $u \in \mathbb{D}(g^{(l)})$ bleibt dabei $y^{(k)}$ als Derivat des neuen Polynoms erhalten. Ebenso ist $\mathrm{in}_\tau(g^{(l)})y^{(k)}$ wegen der Pseudo-Reduziertheit von G_j pseudo-reduziert bzgl. G_j. Da das zugehörige Pseudo-Ersetzungssystem noethersch ist, erhalten wir nach endlich vielen solcher Pseudo-Reduktionsschritte ein von Null verschiedenes bzgl. G_j pseudo-reduziertes Polynom, im Widerspruch zu Satz 1.6.4. □

Besitzt das Ideal I in der obigen Situation eine endliche differentielle σ-Gröbnerbasis, so können wir die differentiellen Unbestimmmten voraussagen, für die ein Derivat im Leittermideal von I enthalten ist. Denn nach Korollar 1.8.11 gilt für jede Menge G_i mit minimaler Mächtigkeit gerade $n - |G_i| = \dim(D/I)$. Dabei stimmt die Menge der differentiellen Unbestimmten, die nicht Leitderivate sind, für alle diese Mengen G_i überein und liefert das Gesuchte.

2.5 Der differentielle Buchberger-Algorithmus

Nachdem wir im letzten Abschnitt die Eigenschaften differentieller Gröbnerbasen ausgiebig diskutiert haben, steht nun deren Berechnung im Vordergrund. Zobnins Algorithmus für differentielle Ideale $I \subseteq K\{y\}$ verwendet rein algebraische Hilfsmittel. Er bestimmt iterativ eine Gröbnerbasis des Ideals I_k für aufsteigendes $k \in \mathbb{N}_0$, wobei dazu jeweils eine unbestimmte, aber endliche Anzahl von Gröbnerbasisberechnungen notwendig ist. Da in $K\{y\}$ nur null-dimensionale differentielle Ideale zu betrachten sind, ist ein Terminieren dieses Algorithmus im Falle der Existenz einer endlichen differentiellen Gröbnerbasis gesichert. Seine Idee lässt sich damit nicht ohne Weiteres auf den allgemeinen Fall übertragen. Zudem stellt sich die Frage, ob die Bestimmung einer differentiellen Gröbnerbasis durch beliebig viele algebraische Gröbnerbasisberechnungen sinnvoll ist.

Ein anderes, für uns wesentlich interessanteres Konzept wird in [18] vorgestellt. Ollivier entwickelt darin eine differentielle Version des Buchberger-Algorithmus, jedoch lediglich für Berechnungen von differentiellen Gröbnerbasen bzgl. strikt stabilen differentiellen Termordnungen. Dies soll hier zunächst verallgemeinert werden. Aber auch wir werden uns im späteren Verlauf auf die Kategorie der strikt stabilen differentiellen Termordnungen konzentrieren, da sich für diese weitaus bessere Ergebnisse erzielen lassen.

Die Grundidee bei der Berechnung ist ein Analogon zum klassischen Buchberger-Kriterium. Dazu betrachten wir sogenannte fundamentale kritische Paare, die die Rolle der kritischen Paare aus der üblichen Gröbnerbasistheorie übernehmen. Hierbei erweitern wir die Definition von fundamentalen kritischen Paaren entscheidend gegenüber der von Ollivier. Zudem formulieren wir den resultierenden differentiellen Buchberger-Algorithmus und geben, im Gegensatz zu Ollivier, Kriterien an, unter denen dieser endet. Diese Prozedur ermöglicht u.a. die Berechnung einer endlichen differentiellen Gröbnerbasis für null-dimensionale differentielle Ideale, für die eine solche existiert. Hingegen ist der Algorithmus in [18] eher theoretischer Natur, da dieser unendliche Mengen von kritischen Paaren auf Kriterien hin untersucht und ein Terminieren somit praktisch ausgeschlossen ist.

Im Folgenden sei wieder $D = K\{y_1, \dots, y_n\}$ der differentielle Polynomring und σ eine differentielle Termordnung auf $\mathbb{T}^n$.

Definition 2.5.1. Sei $G = \{g_1, \dots, g_s\} \subseteq D\backslash\{0\}$ eine Menge von Polynomen und σ eine differentielle Termordnung auf $\mathbb{T}^n$.

1) Für alle $i, j \in \{1, \dots, s\}$, $i \leq j$ und $k, l \in \mathbb{N}_0$ mit $(i,k) \neq (j,l)$ heißt $((i,k),(j,l))$ ein *kritisches Paar* von G.
2) Ist $((i,k),(j,l))$ ein kritisches Paar von G, so heißt das differentielle Polynom

$$S((i,k),(j,l)) = S(g_i^{(k)}, g_j^{(l)}) = \tfrac{1}{\mathrm{LC}_\sigma(g_i^{(k)})} t_i g_i^{(k)} - \tfrac{1}{\mathrm{LC}_\sigma(g_j^{(l)})} t_j g_j^{(l)}$$

das zugehörige *S-Polynom*, wobei $t_i, t_j \in \mathbb{T}^n$ bzgl. σ minimal gewählt sind mit $t_i \,\mathrm{LT}_\sigma(g_i^{(k)}) = t_j \,\mathrm{LT}_\sigma(g_j^{(l)})$. Den Term $t_i \,\mathrm{LT}_\sigma(g_i^{(k)})$ bezeichnen wir auch mit $t_{(i,k),(j,l)}$ oder mit $t_{S((i,k),(j,l))}$.

Um etwaige Fallunterscheidungen zu vermeiden, trennen wir im Folgenden nicht zwischen den Paaren $((i,k),(j,l))$ und $((j,l),(i,k))$. Eine Polynommenge G ist nun genau dann eine differentielle σ-Gröbnerbasis, wenn alle S-Polynome von G bzgl. G zu Null reduzieren. Diese differentielle Version des Buchberger-Kriteriums lässt sich auf die algebraische zurückführen, indem wir statt G die Menge $\{\partial^k g \mid g \in G,\, k \geq 0\}$ betrachten.

Satz 2.5.2 (Differentielles Buchberger-Kriterium).
Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$, $G \subseteq D\backslash\{0\}$ und I das von G differentiell erzeugte Ideal von D. Dann sind die folgenden Aussagen äquivalent:

a) Die Menge G ist eine differentielle σ-Gröbnerbasis von I.
b) Für jedes kritische Paar von G reduziert das zugehörige S-Polynom bzgl. G zu Null.

Beweis. Zunächst ist G genau dann eine differentielle σ-Gröbnerbasis von I, wenn die Menge $\widetilde{G} = \{\partial^k g \mid g \in G, k \geq 0\}$ eine σ-Gröbnerbasis des algebraischen Ideals I ist. Dies ist aber nach [14], Korollar 2.5.3 genau dann der Fall, wenn für jedes kritische Paar von $\widetilde{G}$ das zugehörige S-Polynom bzgl. $\widetilde{G}$ algebraisch zu Null reduziert. Letzteres ist schließlich äquivalent zu Aussage b). □

Im Gegensatz zur algebraischen Gröbnerbasistheorie sind hier für eine differentielle Gröbnerbasisberechnung stets unendlich viele kritische Paare zu prüfen. Damit ist klar, dass der Buchberger-Algorithmus in unserer Situation im Allgemeinen nicht terminiert. Durch Hinzunahme der üblichen Kriterien aus der klassischen Gröbnerbasistheorie zur Vermeidung unnötiger kritischer Paare lässt sich die Menge der Paare in bestimmten Fällen entscheidend reduzieren und der Algorithmus endet gegebenenfalls.

Lemma 2.5.3. *Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$ und $G \subseteq D$. Weiter seien $g_1, g_2, g_3 \in G\backslash\{0\}$ und $k_1, k_2 \in \mathbb{N}_0$.*

a) Sind $\mathrm{LT}_\sigma(g_1^{(k_1)})$ und $\mathrm{LT}_\sigma(g_2^{(k_2)})$ teilerfremd, so gilt $S(g_1^{(k_1)}, g_2^{(k_2)}) \xrightarrow{G} 0$.
b) Seien $t_1, t_2 \in \mathbb{T}^n$ Terme mit $S(g_1^{(k_1)}, g_2^{(k_2)}) = \frac{1}{\mathrm{LC}_\sigma(g_1^{(k_1)})} t_1 g_1^{(k_1)} - \frac{1}{\mathrm{LC}_\sigma(g_2^{(k_2)})} t_2 g_2^{(k_2)}$. Existiert eine Zahl $k_3 \in \mathbb{N}_0$, so dass $\mathrm{LT}_\sigma(g_3^{(k_3)})$ ein Teiler von $t_1 \, \mathrm{LT}_\sigma(g_1^{(k_1)})$ ist und sowohl $S(g_1^{(k_1)}, g_3^{(k_3)}) \xrightarrow{G} 0$ als auch $S(g_2^{(k_2)}, g_3^{(k_3)}) \xrightarrow{G} 0$ erfüllt ist, so gilt auch $S(g_1^{(k_1)}, g_2^{(k_2)}) \xrightarrow{G} 0$.

Beweis. Siehe [14], Proposition 2.5.8 bzw. [7], Abschnitt 3. □

Wir sind nun in der Lage, eine erste differentielle Version des Buchberger-Algorithmus zu formulieren. Dabei handelt es sich eigentlich nur um eine Prozedur, da ein Terminieren im Allgemeinen nicht gesichert ist.

Satz 2.5.4 (Differentieller Buchberger-Algorithmus).
Sei σ eine differentielle Termordnung auf $\mathbb{T}^n$ und $F = \{f_1, \ldots, f_s\} \subseteq D\backslash\{0\}$ eine Menge von Polynomen. Wir betrachten die folgenden Instruktionen:

1) Setze $G = F$, $\tilde{s} = s$ und B als die Menge der kritischen Paare von G.
2) Entferne aus B jedes kritische Paar, das einer der Bedingungen aus Lemma 2.5.3 genügt.
3) Gilt $B = \emptyset$, so gib G aus und stoppe.
4) Wähle ein kritisches Paar aus B unter Verwendung einer fairen Strategie. Berechne das zugehörige S-Polynom und dessen differentiellen Rest $g_{\tilde{s}+1}$ bzgl. $(\sigma, \mathcal{G})$. Ist $g_{\tilde{s}+1} = 0$, so fahre mit 3) fort.
5) Füge $g_{\tilde{s}+1}$ zu G und die Paare $\{((i,k), (\tilde{s}+1, l)) \mid 1 \leq i \leq \tilde{s}+1, k, l \geq 0\}$ zu B hinzu. Ersetze $\tilde{s}$ durch $\tilde{s}+1$ und fahre mit 2) fort.

Dies ist eine Prozedur, die, falls sie endet, eine differentielle σ-Gröbnerbasis von $\langle F \rangle_\partial$ ausgibt.

Beweis. Endet die Prozedur, so wurde jedes kritische Paar von G abgearbeitet, d.h. das zugehörige S-Polynom reduziert bzgl. G zu Null. Nach Satz 2.5.2 ist damit G eine differentielle σ-Gröbnerbasis von $\langle G\rangle_\partial = \langle F\rangle_\partial$. □

Leider genügen die Kriterien aus Lemma 2.5.3 in den meisten Fällen nicht aus, um die Menge der zu betrachtenden kritischen Paare entscheidend zu verkleinern. Unsere Situation können wir jedoch wesentlich verbessern, wenn wir uns auf die Klasse der strikt stabilen differentiellen Termordnungen einschränken. Denn in diesem Fall genügt bereits die Betrachtung von speziellen kritischen Paaren.

Definition 2.5.5. Sei $G = \{g_1, \ldots, g_s\} \subseteq D\backslash\{0\}$ eine Menge von Polynomen. Ein kritisches Paar $((i,k),(j,l))$ von G heißt *fundamental*, falls keine Zahlen $\tilde{k}, \tilde{l}, m \in \mathbb{N}_0$ existieren, so dass $t_{(i,k),(j,l)} = t\,\mathrm{LT}_\sigma(\partial^m(t_{(i,\tilde{k}),(j,\tilde{l})}))$ für einen Term $t \in \mathbb{T}^n$ und zusätzlich $(\tilde{k},\tilde{l}) <_{\texttt{Lex}} (k,l)$ gilt, falls $m = 0$ und $t = 1$ ist.

Leider kann es zwischen zwei Polynomen auch unendlich viele fundamentale kritische Paare geben. Jedoch existiert in einem Großteil der Fälle höchstens ein fundamentales kritisches Paar. Genauer gilt das Folgende.

Satz 2.5.6. *Seien σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$, $G \subseteq D\backslash\{0\}$ und $g_i, g_j \in G$ zwei verschiedene Polynome mit $\mathrm{LT}_\sigma(g_i^{(k)}) = t_i u_i^{(k)}$ und $\mathrm{LT}_\sigma(g_j^{(k)}) = t_j u_j^{(k)}$ für jedes $k \geq 0$ und gewisse $t_i, t_j \in \mathbb{T}^n$, $u_i, u_j \in \mathbb{D}^n$.*

a) Für ein fundamentales kritisches Paar $((i,k),(i,l))$ von G gilt $|k-l| = 1$.
b) Zwischen g_i und g_j existieren genau dann endlich viele fundamentale kritische Paare, wenn eine der folgenden Bedingungen erfüllt ist:
C1) $\deg_{u_i}(\mathrm{LT}_\sigma(g_i)) \leq \deg_{u_i}(\mathrm{LT}_\sigma(g_j))$ oder $\deg_{u_j}(\mathrm{LT}_\sigma(g_j)) \leq \deg_{u_j}(\mathrm{LT}_\sigma(g_i))$,
C2) $\deg_{u_i}(\mathrm{LT}_\sigma(g_i)) > \deg_{u_i}(\mathrm{LT}_\sigma(g_j))$ und $u_i^{(l)} \in \mathbb{D}(\mathrm{LT}_\sigma(g_j))$ oder $\deg_{u_j}(\mathrm{LT}_\sigma(g_j)) > \deg_{u_j}(\mathrm{LT}_\sigma(g_i))$ und $u_j^{(l)} \in \mathbb{D}(\mathrm{LT}_\sigma(g_i))$ für ein $l > 0$.
c) Zwischen g_i und g_j existieren entweder unendlich viele oder genau ein fundamentales kritisches Paar.

Beweis. Für den Beweis von a) sei $((i,k),(i,l))$ ein kritisches Paar und O.B.d.A. gelte $0 \leq k < l$. Dann ist $S(g_i^{(k)}, g_i^{(l)}) = c_k u_i^{(l)} g_i^{(k)} - c_l u_i^{(k)} g_i^{(l)}$ mit $c_j = (\mathrm{LC}_\sigma(g_i^{(j)}))^{-1}$ für $j \in \{k,l\}$. Würde hierbei $l > k+1$ gelten, so wäre $t_i u_i^{(k)} u_i^{(l)}$ nach Satz 2.1.12 c) der Leitterm von $\partial(t_i u_i^{(k)} u_i^{(l-1)})$ bzgl. σ, womit $((i,k),(i,l))$ nicht fundamental wäre.

Um b) zu zeigen, nehmen wir zuerst an, dass eine der Bedingungen erfüllt ist. Im Fall $\deg_{u_i}(\mathrm{LT}_\sigma(g_i)) \leq \deg_{u_i}(\mathrm{LT}_\sigma(g_j))$ ist dann $t_{(i,0),(j,0)} = \mathrm{kgV}(t_i,t_j)u_j$. Gilt zusätzlich $\deg_{u_i}(\mathrm{LT}_\sigma(g_i)) \leq \deg_{u_i}(t_j)$, so erhalten wir für ein kritisches Paar $((i,k_i),(j,k_j))$ den Term $t_{(i,k_i),(j,k_j)} = \mathrm{kgV}(t_i,t_j)(u_i^{(k_i)})^\varepsilon u_j^{(k_j)}$ mit $\varepsilon \in \{0,1\}$, wobei $\varepsilon = 0$ genau dann gilt, wenn $\deg_{u_i^{(k_i)}}(\mathrm{LT}_\sigma(g_i^{(k_i)})) \leq \deg_{u_i^{(k_i)}}(\mathrm{LT}_\sigma(g_j^{(k_j)}))$ ist. Es kann nun $((i,k_i),(j,k_j))$ nur dann ein fundamentales kritisches Paar von G sein, wenn $k_j = 0$ und $\varepsilon = 0$ gilt. Wegen

$t_{(i,0),(j,0)} = t_{(i,k_i),(j,0)}$ und $(0,0) \leq_{\texttt{Lex}} (k_i, 0)$ ist daher $((i,0),(j,0))$ das einzige fundamentale kritische Paar zwischen g_i und g_j. Gilt hingegen $\deg_{u_i}(\mathrm{LT}_\sigma(g_i)) > \deg_{u_i}(t_j)$, so folgt $u_i = u_j$. Damit ist $t_{(i,k_i),(j,k_j)}$ ein Vielfaches von $\mathrm{kgV}(t_i, t_j) u_j^{(\max\{k_i,k_j\})}$ und $((i,k_i),(j,k_j))$ nur dann fundamental, wenn $\max\{k_i, k_j\} = 0$, also $k_i = k_j = 0$ gilt.

Da sich die Aussage für den Fall $\deg_{u_j}(\mathrm{LT}_\sigma(g_j)) \leq \deg_{u_j}(\mathrm{LT}_\sigma(g_i))$ analog zeigen lässt, bleibt noch die Bedingung C2) zu betrachten. O.B.d.A. habe $\mathrm{LT}_\sigma(g_i)$ einen größeren Grad in u_i als $\mathrm{LT}_\sigma(g_j)$. Zusätzlich sei $u_i^{(l)} \in \mathbb{D}(\mathrm{LT}_\sigma(g_j))$ für ein minimales $l > 0$. Es ergibt sich nun $t_{(i,l),(j,0)} = \mathrm{kgV}(t_i, t_j) u_j$ bzw. $t_{(i,k_i),(j,k_j)} = \mathrm{kgV}(t_i, t_i)(u_i^{(k_i)})^\varepsilon u_j^{(k_j)}$ mit $\varepsilon \in \{0, 1\}$, wobei $\varepsilon = 0$ genau dann gilt, wenn $\deg_{u_i^{(k_i)}}(\mathrm{LT}_\sigma(g_i^{(k_i)})) \leq \deg_{u_i^{(k_i)}}(\mathrm{LT}_\sigma(g_j^{(k_j)}))$ gilt. Ist $((i,k_i),(j,k_j))$ fundamental, so muss also $k_j = 0$ und $\varepsilon = 0$ gelten. Zudem ist $k_i \geq l$, d.h. $(l, 0) \leq_{\texttt{Lex}} (k_i, 0)$ und damit $((i,l),(j,0))$ wieder einziges fundamentales kritisches Paar zwischen g_i und g_j. Damit haben wir insbesondere c) gezeigt.

Für den Beweis der Umkehrung nehmen wir an, dass keine der Bedingungen erfüllt ist. Dann erhalten wir für ein kritisches Paar $((i,k_i),(j,k_j))$ stets den zugehörigen Term $t_{(i,k_i),(j,k_j)} = \mathrm{kgV}(t_i, t_j) u_i^{(k_i)} u_j^{(k_j)}$. Also ist das Paar $((i,0),(j,0))$ auf jeden Fall fundamental. Damit ist aber auch das Paar mit dem Term $\mathrm{kgV}(t_i, t_j) \min_\sigma\{u_i^{(1)} u_j, u_i u_j^{(1)}\}$ ein fundamentales. Sei dies O.B.d.A. das Paar $((i,0),(j,1))$. Dann ist entweder $((i,1),(j,1))$ oder $((i,0),(j,2))$ ein weiteres fundamentales kritisches Paar. Auf diese Weise können wir Schritt für Schritt immer wieder ein neues fundamentales kritisches Paar konstruieren. Also haben wir b) bewiesen. □

Die Aussage a) des obigen Satzes gibt an, wie die fundamentalen kritischen Paare von Polynomen mit sich selbst aussehen. Es wird insbesondere deutlich, dass es in diesem Fall stets unendlich viele solcher Paare gibt. Dass diese nicht immer notwendigerweise betrachtet werden müssen, zeigt der Fall der Polynome, deren Leitterm bzgl. σ ein Derivat ist. Denn dann sind die Leitterme der entsprechenden Derivationen stets teilerfremd.

Bemerkung 2.5.7. Sei $((i,k_i),(j,k_j))$ ein kritisches und $((i,l_i),(j,l_j))$ ein fundamentales kritisches Paar zwischen g_i und g_j, so dass $t_{(i,k_i),(j,k_j)}$ für ein $m \geq 0$ ein Vielfaches von $\mathrm{LT}_\sigma(\partial^m t_{(i,l_i),(j,l_j)})$ ist. Dann gilt immer $l_i + m = k_i$ oder $l_j + m = k_j$. Denn ist eine Bedingung aus Teil b) des obigen Satzes erfüllt, so geht dies direkt aus dem Beweis hervor. Ist dies nicht der Fall, so gilt $t_{(i,k_i),(j,k_j)} = \mathrm{kgV}(t_i, t_j) u_i^{(k_i)} u_j^{(k_j)}$. Weiter erhalten wir als Leitterm von $\partial^m t_{(i,l_i),(j,l_j)}$ den Term $\mathrm{kgV}(t_i, t_j) \max_\sigma\{u_i^{(l_i+m)} u_j^{(l_j)}, u_i^{(l_i)} u_j^{(l_j+m)}\}$. Also folgt entweder $l_i + m = k_i$ und $l_j = k_j$ oder $l_i = k_i$ und $l_j + m = k_j$. Ist $l_i + m = k_i$, so gilt in beiden Fällen zusätzlich $\mathrm{LT}_\sigma(\partial^m t_{(i,l_i),(j,l_j)}) = \frac{t_{(i,l_i),(j,l_j)}}{\mathrm{LT}_\sigma(g_i^{(l_i)})} \mathrm{LT}_\sigma(g_i^{(l_i+m)})$.

Beispiel 2.5.8. Wir betrachten den differentiellen Polynomring $\mathbb{Q}\{y_1, y_2\}$ versehen mit der differentiellen Termordnung `DegLex` mit $y_1^{(k)} < y_2$ für alle $k \geq 0$. Für die Polynome $g_1 = y_1^{(1)} y_2 + y_2$, $g_2 = (y_2^{(1)})^2 + y_1^{(1)}$ und $g_3 = y_1^{(2)} + y_1^{(1)} + 1$ ergeben sich dann die folgenden fundamentalen kritischen Paare. Für g_1 und g_2 ist die Bedingung C2) erfüllt, denn

$\deg_{y_2}(\mathrm{LT}_\sigma(g_1)) = 1 > 0 = \deg_{y_2}(\mathrm{LT}_\sigma(g_2))$ und $y_2^{(1)} \in \mathbb{D}((y_2^{(1)})^2)$. Also ist $((1,1),(2,0))$ das einzige fundamentale kritische Paar zwischen g_1 und g_2.

Hingegen ist für g_1 und g_3 bzw. g_2 und g_3 weder C1) noch C2) erfüllt, d.h. es gibt jeweils unendlich viele fundamentale kritische Paare der Form $((1,0),(3,k))$ bzw. $((2,0),(3,k))$ mit $k \geq 0$. Schließlich existieren für $i = 1,2,3$ noch unendlich viele solcher Paare zwischen g_i und g_i der Form $((i,k+1),(i,k))$ mit $k \geq 0$.

Bevor wir das Buchberger-Kriterium in einer neuen Version formulieren, benötigen wir noch ein technisches Detail. Dabei betrachten wir den sogenannten *Rang* eines Polynoms.

Definition 2.5.9. Sei $G \subseteq D\backslash\{0\}$ eine Menge von Polynomen und $f \in \langle G\rangle_\partial\backslash\{0\}$. Weiter sei $f = \sum_{i=1}^s c_i t_i g_i^{(k_i)}$ mit $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}^n$, $k_i \in \mathbb{N}_0$ und $g_i \in G$ für $i = 1,\ldots,s$ eine Darstellung von f, so dass der Term $\max_\sigma\{\mathrm{LT}_\sigma(t_i g_i^{(k_i)}) \mid i = 1,\ldots,s\}$ bzgl. σ minimal ist. Dann heißt dieser der *Rang* von f bzgl. G und wird mit $\mathrm{rg}_{\sigma,G}(f)$ bezeichnet. Wir setzen zusätzlich $\mathrm{rg}_{\sigma,G}(0) = 1$.

Es ergeben sich zunächst einige grundlegende Eigenschaften für den Rang eines Polynoms.

Lemma 2.5.10. *Sei $G \subseteq D\backslash\{0\}$ eine Menge von Polynomen, und seien $f, g \in \langle G\rangle_\partial\backslash\{0\}$.*

a) Es ist $\mathrm{rg}_{\sigma,G}(fg) \leq_\sigma \mathrm{rg}_{\sigma,G}(f)\,\mathrm{rg}_{\sigma,G}(g)$ und $\mathrm{rg}_{\sigma,G}(f+g) \leq_\sigma \max_\sigma\{\mathrm{rg}_{\sigma,G}(f), \mathrm{rg}_{\sigma,G}(g)\}$.
b) Es gilt $\mathrm{rg}_{\sigma,G}(f) \geq_\sigma \mathrm{LT}_\sigma(f)$. Dabei gilt Gleichheit, wenn f bzgl. G zu Null reduziert.
c) Für jedes kritisches Paar $((i,k),(j,l))$ von G gilt $\mathrm{rg}_{\sigma,G}(S(g_i^{(k)}, g_j^{(l)})) \leq_\sigma t_{(i,k),(j,l)}$.

Beweis. Alle Aussagen folgen direkt aus der Definition des Rangs eines Polynoms, aus der Definition eines Reduktionsschritts und der des S-Polynoms. □

Unter Verwendung des Rangbegriffs erhalten wir nun für jedes S-Polynom S eine Darstellung in ausgewählten S-Polynomen zu fundamentalen kritischen Paaren, die es uns ermöglicht, von Aussagen über letztere auf Aussagen über S zu schließen. Dies ist von besonderem Interesse, da wir im Folgenden nur noch die fundamentalen kritischen Paare betrachten wollen.

Lemma 2.5.11. *Sei $G \subseteq D\backslash\{0\}$ und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Weiter sei $((i,k_i),(j,k_j))$ ein kritisches Paar von G mit S-Polynom S.*

a) Es existieren S-Polynome $S_1,\ldots,S_r$ zu fundamentalen kritischen Paaren von G der Form $((i_1,l_1),(i_2,l_2))$ mit $i_1,i_2 \in \{i,j\}$, $l_1,l_2 \geq 0$ und ein Polynom $g \in \langle G\rangle_\partial$, so dass sich S schreiben lässt als $S = \sum_{i=1}^r c_i t_i S_i^{(m_i)} + g$ mit $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}^n$, $m_i \in \mathbb{N}_0$, $t_i\,\mathrm{LT}_\sigma(t_{S_i}^{(m_i)}) \leq_\sigma t_S$ für $i = 1,\ldots,r$ und $\mathrm{rg}_{\sigma,G}(g) <_\sigma t_S$.
b) Es gilt $\mathrm{rg}_{\sigma,G}(S) <_\sigma t_S$, falls für jedes fundamentale kritische Paar $((i_1,l_1),(i_2,l_2))$ von G mit $t_{(i_1,l_1),(i_2,l_2)} \leq_\sigma t_S$ der Rang des zugehörigen S-Polynoms bzgl. σ echt kleiner als $t_{(i_1,l_1),(i_2,l_2)}$ ist.

Beweis. Gilt $\operatorname{rg}_{\sigma,G}(S) <_\sigma t_S$ oder ist $((i,k_i),(j,k_j))$ ein fundamentales kritisches Paar, so ist a) offensichtlich erfüllt. Andernfalls existiert ein fundamentales kritisches Paar $((i,l_i),(j,l_j))$ mit $l_i, l_j \geq 0$ und ein $m \geq 0$, so dass $t_{(i,k_i),(j,k_j)} = t\,\mathrm{LT}_\sigma(\partial^m t_{(i,l_i),(j,l_j)})$ für einen Term $t \in \mathbb{T}^n$ gilt. Ist $g_i = g_j$, so folgt $|l_i - l_j| = 1$ mit Satz 2.5.6. Sei O.B.d.A. $l_j = l_i + 1$ und seien $t_i \in \mathbb{T}^n$, $u_i \in \mathbb{D}^n$, so dass $\mathrm{LT}_\sigma(g_i^{(k_i)}) = t_i u_i^{(k_i)}$. Dann ergibt sich

$$t_{(i,k_i),(j,k_j)} = u_i^{(k_j)} t_i u_i^{(k_i)} = t t_i u_i^{(l_i)} u_i^{(l_i+1+m)},$$

d.h. $t = 1$ und O.B.d.A. gelte $k_i = l_i$ bzw. $k_j = l_i + 1 + m$. Wir erhalten mit

$$\begin{aligned}
&S - \partial^m(S(g_i^{(l_i)}, g_j^{(l_i+1)})) \\
&= \left(c_i u_i^{(k_j)} g_i^{(k_i)} - c_j u_i^{(k_i)} g_i^{(k_j)}\right) - \partial^m \left(c_i u_i^{(l_i+1)} g_i^{(l_i)} - c_j u_i^{(l_i)} g_i^{(l_i+1)}\right) \\
&= -\sum_{k=0}^{m-1} \binom{m}{k} c_i u_i^{(l_i+1+k)} g_i^{(l_i+m-k)} + \sum_{k=0}^{m-1} \binom{m}{k} c_j u_i^{(l_i+m-k)} g_i^{(l_i+1+k)},
\end{aligned}$$

wobei $c_l = \frac{1}{\mathrm{LC}_\sigma(g_l^{(k_l)})}$ für $l = i, j$, ein Polynom mit einem echt kleinerem Rang als t_S.

Sei nun $g_i \neq g_j$ und O.B.d.A. sei der Leitterm von $\partial^m t_{(i,l_i),(j,l_j)}$ bzgl. σ ein Vielfaches von $\mathrm{LT}_\sigma(g_i^{(l_i+m)})$, d.h. $k_i = l_i + m$. Dann gilt $S - ct\partial^m(S(g_i^{(l_i)}, g_j^{(l_j)})) = \tilde{t} S(g_j^{(k_j)}, g_j^{(l_j+k)}) + g$ für geeignete $c \in K\backslash\{0\}$, $\tilde{t} \in \mathbb{T}^n$, $k \in \{0, m\}$ und ein $g \in \langle G \rangle_\partial$ mit $\operatorname{rg}_{\sigma,G}(g) <_\sigma t_S$. Für das S-Polynom $S(g_j^{(k_j)}, g_j^{(l_j+k)})$ wissen wir bereits, dass es eine Darstellung der Form $S(g_j^{(k_j)}, g_j^{(l_j+k)}) = \sum_{i=1}^r c_i t_i S_i^{(m_i)} + \tilde{g}$ besitzt mit $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}^n$, $m_i \in \mathbb{N}_0$, $g \in \langle G \rangle_\partial$, $t_i\,\mathrm{LT}_\sigma(t_{S_i}^{(m_i)}) \leq_\sigma t_S$ für $i = 1, \ldots, r$ und $\operatorname{rg}_{\sigma,G}(\tilde{t}\tilde{g}) <_\sigma t_S$. Also gilt dies auch für S.

Für den Beweis von b) schreiben wir S als $S = \sum_{i=1}^r c_i t_i S_i^{(m_i)} + g$ mit $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}^n$, $m_i \in \mathbb{N}_0$, $g \in \langle G \rangle_\partial$, $t_i\,\mathrm{LT}_\sigma(t_{S_i}^{(m_i)}) \leq_\sigma t_S$ für $i = 1, \ldots, r$ und $\operatorname{rg}_{\sigma,G}(g) <_\sigma t_S$. Nach Voraussetzung gilt für $i = 1, \ldots, r$ dabei $\operatorname{rg}_{\sigma,G}(S_i) <_\sigma t_{S_i}$. Daher folgt nun aus

$$t_S \geq_\sigma t_i\,\mathrm{LT}_\sigma(\partial^{m_i} t_{S_i}) >_\sigma t_i\,\mathrm{LT}_\sigma(\partial^{m_i} \operatorname{rg}_{\sigma,G}(S_i)) \geq_\sigma t_i \operatorname{rg}_{\sigma,G}(S_i^{(m_i)})$$

für $i = 1, \ldots, r$ zunächst $t = \max_\sigma\{t_i\,\mathrm{LT}_\sigma(\partial^{m_i} \operatorname{rg}_{\sigma,G}(S_i)) \mid i = 1, \ldots, r\} <_\sigma t_S$ und daraus schließlich $\operatorname{rg}_{\sigma,G}(S) \leq_\sigma \max_\sigma\{t, \operatorname{rg}_{\sigma,G}(g)\} <_\sigma t_S$. □

Die Aussage in b) hat nun unmittelbar zur Folge, dass jedes S-Polynom S bzgl. G zu Null reduziert, falls dies bereits für all diejenigen S-Polynome erfüllt ist, deren Rang bzgl. σ kleiner oder gleich t_s ist und die zu fundamentalen kritischen Paaren gehören.

Für strikt stabile differentielle Termordnungen erhalten wir daraus die folgende Version des differentiellen Buchberger-Kriteriums.

Satz 2.5.12. *Sei σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$, $G \subseteq D\backslash\{0\}$ und I das von G differentiell erzeugte Ideal von D. Dann sind die folgenden Aussagen äquivalent:*

a) *Die Menge G ist eine differentielle σ-Gröbnerbasis von I.*
b) *Für jedes fundamentale kritische Paar von G reduziert das zugehörige S-Polynom bzgl. G zu Null.*

Beweis. Da die Implikation a) $\Rightarrow$ b) eine direkte Folgerung aus Satz 2.5.2 ist, genügt es, die Umkehrung zu beweisen. Für einen Widerspruchsbeweis nehmen wir an, dass es ein bzgl. G reduziertes Polynom $f \in I\backslash\{0\}$ gibt. Wir wählen f nun mit minimalem Rang und derart, dass in der Darstellung $f = \sum_{i=1}^{s} c_i t_i g_i^{(k_i)}$ mit $c_i \in K\backslash\{0\}$, $t_i \in \mathbb{T}^n$, $k_i \in \mathbb{N}_0$, $g_i \in G$ für $i = 1, \ldots, s$ und $\mathrm{rg}_{\sigma,G}(f) = \max_\sigma\{\mathrm{LT}_\sigma(t_i g_i^{(k_i)}) \mid i = 1, \ldots, s\}$ die Anzahl s der Summanden minimal ist. Es gilt offensichtlich $s \geq 2$. O.B.d.A. nehme dabei $\mathrm{LT}_\sigma(t_1 g_1^{(k_1)})$ das Maximum an. Ist $f_1 = f - c_1 t_1 g_1^{(k_1)}$, so reduziert f_1 wegen der Wahl von f bzgl. G zu Null und wir können f_1 schreiben als $f_1 = ctg^{(k)} + f_2$ für ein $c \in K\backslash\{0\}$, $t \in \mathbb{T}^n$, $k \in \mathbb{N}_0$, $g \in G$ und ein Polynom f_2, das $\mathrm{rg}_{\sigma,G}(f_2) <_\sigma \mathrm{rg}_{\sigma,G}(f)$ erfüllt. Insgesamt ergibt sich also $f = c_1 t_1 g_1^{(k_1)} + ctg^{(k)} + f_2$, wobei wegen der Reduziertheit von f bzgl. G gerade $\mathrm{LM}_\sigma(t_1 g_1^{(k_1)}) + \mathrm{LM}_\sigma(tg^{(k)}) = 0$ gelten muss. Daher ist $f - f_2$ ein Vielfaches eines S-Polynoms, und nach obigem Lemma gilt $\mathrm{rg}_{\sigma,G}(f - f_2) <_\sigma \mathrm{LT}_\sigma(t_1 g_1^{(k_1)}) = \mathrm{rg}_{\sigma,G}(f)$. Die Voraussetzungen des Lemmas sind dabei erfüllt, da für jedes fundamentale kritische Paar das zugehörige S-Polynom bzgl. G zu Null reduziert. Dies impliziert schließlich $\mathrm{rg}_{\sigma,G}(f) \leq_\sigma \max_\sigma\{\mathrm{rg}_{\sigma,G}(f - f_2), \mathrm{rg}(f_2)\} <_\sigma \mathrm{rg}_{\sigma,G}(f)$, ein Widerspruch. □

Wir können die Menge derjenigen kritischen Paare, die betrachtet werden müssen, noch weiter verkleinern. Dazu formulieren wir ein neues Kriterium, welches strukturell an die Bedingung aus Lemma 2.5.3 b) angelehnt ist. Für den Leitterm von $g_i \in G$ gelte wieder $\mathrm{LT}_\sigma(g_i^{(k)}) = t_i u_i^{(k)}$ mit $t_i \in \mathbb{T}^n$ und $u_i \in \mathbb{D}^n$ für $i = 1, \ldots, s$ und für alle $k \geq 0$.

Satz 2.5.13. *Sei σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$, $G = \{g_1, \ldots, g_s\}$ eine Polynommenge in $D\backslash\{0\}$, so dass $\mathrm{LT}_\sigma(g_i)$ für $i = 1, \ldots, s$ bzgl. $G\backslash\{g_i\}$ reduziert ist, und $I = \langle G\rangle_\partial$. Weiter sei B die Menge der fundamentalen kritischen Paare $((i, k_i), (j, k_j))$ von G, die nicht die folgende Bedingung erfüllen:*

C3) *Es existieren ein $g_l \in G$ mit $g_i \neq g_l \neq g_j$ und fundamentale kritische Paare $((i, \tilde{k}_i), (l, l_1))$, $((j, \tilde{k}_j), (l, l_2))$ von G, so dass gilt $t_l \mid \mathrm{kgV}(t_i, t_j)$ und*

$$t_{(i,k_i),(j,k_j)} = \tilde{t}_1\, \mathrm{LT}_\sigma(\partial^{m_1} t_{(i,\tilde{k}_i),(l,l_1)}) = \tilde{t}_2\, \mathrm{LT}_\sigma(\partial^{m_2} t_{(j,\tilde{k}_j),(l,l_2)})$$

mit $\tilde{t}_1, \tilde{t}_2 \in \mathbb{T}^n$, $m_1, m_2 \in \mathbb{N}_0$ und mit

$$\begin{cases} m_1 > 0,\ m_2 > 0, & \text{falls } i = j \\ \tilde{t}_1 >_\sigma 1 \text{ oder } m_1 > 0 \text{ oder } \mathrm{ggT}(\mathrm{LT}_\sigma(g_i^{(\tilde{k}_i)}), \mathrm{LT}_\sigma(g_l^{(l_1)})) = 1, & \text{falls } i \neq j \\ \tilde{t}_2 >_\sigma 1 \text{ oder } m_2 > 0 \text{ oder } \mathrm{ggT}(\mathrm{LT}_\sigma(g_j^{(\tilde{k}_j)}), \mathrm{LT}_\sigma(g_l^{(l_2)})) = 1. & \end{cases}$$

Reduziert für jedes kritische Paar aus B das zugehörige S-Polynom bzgl. G zu Null, so ist G eine differentielle σ-Gröbnerbasis von I.

Beweis. Wir werden zeigen, dass der Rang des S-Polynoms S jedes fundamentalen kritischen Paares von G bzgl. σ echt kleiner als t_S ist. Dann folgt die Behauptung mit Lemma 2.5.11 wie im Beweis von Satz 2.5.12. Dabei genügt es, dies für jedes kritische Paar $((i,k_i),(j,k_j)) \notin B$ zu zeigen, da für alle übrigen nach Voraussetzung das S-Polynom bzgl. G zu Null reduziert. Angenommen, es gibt ein solches Paar, welches die Rangbedingung nicht erfüllt. Dann wählen wir unter diesen dasjenige, für das der Term $t_{(i,k_i),(j,k_j)}$ bzgl. σ minimal ist, und unter diesen das mit minimalem $|i-j|$, minimalem i und schließlich minimalem k_i. Da das kritische Paar offensichtlich nicht C3) erfüllt, existieren also fundamentale kritische Paare $((i,\tilde{k}_i),(l,l_1))$, $((j,\tilde{k}_j),(l,l_2))$ von G wie in C3). Wir betrachten zunächst den Fall $i=j$. Dann ist O.B.d.A. $k_j = k_i+1$. Des Weiteren ist t_l ein Teiler von t_i und $u_l^{(k)} = u_i^{(k_i)}$ für ein $k < k_i$ wegen $m_1 > 0$ bzw. der Reduziertheit von $\mathrm{LT}_\sigma(g_i)$ bzgl. $\{g_l\}$. Wir können nun schreiben

$$\begin{aligned} S(g_i^{(k_i)}, g_i^{(k_i+1)}) &= \tfrac{1}{\mathrm{LC}_\sigma(g_i^{(k_i)})} u_i^{(k_i+1)} g_i^{(k_i)} - \tfrac{1}{\mathrm{LC}_\sigma(g_l^{(k)})} t u_i^{(k_i+1)} g_l^{(k)} \\ &\quad + \tfrac{1}{\mathrm{LC}_\sigma(g_l^{(k+1)})} t u_i^{(k_i)} g_l^{(k+1)} - \tfrac{1}{\mathrm{LC}_\sigma(g_i^{(k_i+1)})} u_i^{(k_i)} g_i^{(k_i+1)} + tS(g_l^{(k)}, g_l^{(k+1)}) \\ &= u_i^{(k_i+1)} S(g_i^{(k_i)}, g_l^{(k)}) - u_i^{(k_i)} S(g_i^{(k_i+1)}, g_l^{(k+1)}) + tS(g_l^{(k)}, g_l^{(k+1)}) \end{aligned} \tag{2.1}$$

für ein $t \in \mathbb{T}^n$. Wegen $t_{(i,k_i),(l,k)} <_\sigma t_{(i,k_i),(i,k_i+1)}$ bzw. $t_{(i,k_{i+1}),(l,k+1)} <_\sigma t_{(i,k_i),(i,k_i+1)}$ und der Wahl von $((i,k_i),(j,k_j))$ gilt sowohl

$$\begin{aligned} \mathrm{rg}_{\sigma,G}(u_i^{(k_i+1)} S(g_i^{(k_i)}, g_l^{(k)})) &= u_i^{(k_i+1)} \,\mathrm{rg}_{\sigma,G}(S(g_i^{(k_i)}, g_l^{(k)})) \\ &<_\sigma u_i^{(k_i+1)} t_{(i,k_i),(l,k)} \\ &= t_{(i,k_i),(i,k_i+1)} \end{aligned}$$

als auch $\mathrm{rg}_{\sigma,G}(u_i^{(k_i)} S(g_i^{(k_i+1)}, g_l^{(k+1)})) <_\sigma t_{(i,k_i),(i,k_i+1)}$. Schließlich gilt die Gleichheit in $t_{(l,k),(l,k+1)} \leq_\sigma t_{(i,k_i),(i,k_i+1)}$ nur dann, wenn $t=1$ ist und die Leitterme von $g_i^{(k_i)}$ und $g_l^{(k)}$ bzgl. σ übereinstimmen. Dann wäre aber entweder $\mathrm{LT}_\sigma(g_i^{(k_i)})$ reduzibel bzgl. $G\backslash\{g_i\}$ oder $\mathrm{LT}_\sigma(g_l^{(k)})$ bzgl. $G\backslash\{g_l\}$ im Widerspruch zur Voraussetzung. Insgesamt erhalten wir also $\mathrm{rg}_{\sigma,G}(S(g_i^{(k_i)}, g_i^{(k_i+1)})) <_\sigma t_{(i,k_i),(i,k_i+1)}$.

O.B.d.A. sei nun $i<j$. Dann ergibt sich

$$\begin{aligned} &S(g_i^{(k_i)}, g_j^{(k_j)}) - \tilde{c}_1 \tilde{t}_1 \partial^{m_1} S(g_i^{(\tilde{k}_i)}, g_l^{(l_1)}) - \tilde{c}_2 \tilde{t}_2 \partial^{m_2} S(g_j^{(\tilde{k}_j)}, g_l^{(l_2)}) \\ &= c_i \bar{t}_i S_i + c_j \bar{t}_j S_j + c_l \bar{t}_l S_l + g \end{aligned} \tag{2.2}$$

für gewisse $\tilde{c}_1, \tilde{c}_2, c_i, c_j, c_l \in K$, $\bar{t}_i, \bar{t}_j, \bar{t}_l \in \mathbb{T}^n$, $g \in \langle G \rangle_\partial$ mit $\mathrm{rg}_{\sigma,G}(g) <_\sigma t_{(i,k_i),(j,k_j)}$ und für S-Polynome S_i, S_j, S_l von g_i, g_j bzw. g_l mit sich selbst, wobei für die zugehörigen Terme $\bar{t}_i t_{S_i} = \bar{t}_j t_{S_j} = \bar{t}_l t_{S_l} = t_{(i,k_i),(j,k_j)}$ gilt. Sind die den S-Polynomen zugrunde liegenden kritischen Paare fundamental, so ist wegen $i \neq j$ und der Wahl von $((i,k_i),(j,k_j))$ der Rang von $\bar{t}_i S_i$, $\bar{t}_j S_j$ bzw. $\bar{t}_l S_l$ bzgl. σ jeweils echt kleiner als $t_{(i,k_i),(j,k_j)}$. Andernfalls lässt sich das entsprechende S-Polynom wie im Beweis von Lemma 2.5.11 schreiben als $\partial^m \widetilde{S} + \tilde{g}$ mit einem Polynom $\tilde{g} \in \langle G \rangle_\partial$ und dem S-Polynom $\widetilde{S}$ zu einem fundamentalen kritischen Paar, so dass $\mathrm{rg}_{\sigma,G}(\tilde{g}) <_\sigma t_{(i,k_i),(j,k_j)}$ bzw. $\mathrm{LT}_\sigma(\partial^m t_{\widetilde{S}}) \leq_\sigma t_{(i,k_i),(j,k_j)}$ gilt. Also erfüllen die Polynome $\bar{t}_i S_i$, $\bar{t}_j S_j$ und $\bar{t}_l S_l$ die Rangbedingung. Dies gilt nach Voraussetzung auch für die Polynome $\tilde{c}_1 \tilde{t}_1 \partial^{m_1} S(g_i^{(\tilde{k}_i)}, g_l^{(l_1)})$ und $\tilde{c}_2 \tilde{t}_2 \partial^{m_2} S(g_j^{(\tilde{k}_j)}, g_l^{(l_2)})$. Insgesamt erhalten wir demnach $\mathrm{rg}_{\sigma,G}(S(g_i^{(k_i)}, g_j^{(k_j)})) <_\sigma t_{(i,k_i),(j,k_j)}$. □

Bemerkung 2.5.14. Erfüllt ein fundamentales kritisches Paar $((i,k_i),(j,k_j))$ die Bedingung C3), so auch jedes fundamentale kritische Paar $((i,l_i),(j,l_j))$ mit $l_i > k_i$ und $l_j \geq k_j$ oder $l_i \geq k_i$ und $l_j > k_j$. Denn wegen $t_l \mid \mathrm{kgV}(t_i, t_j)$ gilt $\mathrm{LT}_\sigma(g_l^{(k)}) \mid \mathrm{kgV}(t_i, t_j)$, $u_l^{(k)} = u_i^{(k_i)}$ oder $u_l^{(k)} = u_j^{(k_j)}$ für ein $k \geq 0$. In jedem Fall ergibt sich

$$t_{(i,l_i),(j,l_j)} = \frac{u_j^{(l_j)}}{u_j^{(k_j)}} \tilde{t}_1 \, \mathrm{LT}_\sigma(\partial^{m_1 + l_i - k_i} t_{(i,\tilde{k}_i),(l,l_1)}) = \frac{u_i^{(l_i)}}{u_i^{(k_i)}} \tilde{t}_2 \, \mathrm{LT}_\sigma(\partial^{m_2 + l_j - k_j} t_{(j,\tilde{k}_j),(l,l_2)})$$

mit $m_1 + l_i - k_i \geq m_1$ und $m_2 + l_j - k_j \geq m_2$.

Um zu testen, ob eine Menge von Polynomen eine differentielle Gröbnerbasis bildet, müssen also lediglich diejenigen fundamentalen kritischen Paare betrachtet werden, die nicht Kriterium C3) erfüllen. Jedoch verbleiben in den meisten Fällen immer unendlich viele solcher Paare. Daher ist es zwingend notwendig, eine Systematik zur Abarbeitung der Paare zu entwickeln, bei der zu jedem Zeitpunkt nur endlich viele Paare betrachtet werden.

Aber selbst wenn im Laufe der Prozedur zu einem Zeitpunkt nur noch endlich viele zu betrachtende kritische Paare verbleiben, muss die Prozedur auch in günstigen Fällen nicht enden. Denn es können beliebig viele neue Gröbnerbasiselemente gefunden werden, die wiederum neue kritische Paare erzeugen, da im differentiellen Fall monomiale Ideale nicht notwendigerweise endlich erzeugt sind. Werden also die kritischen Paare in beliebiger oder ungünstiger Reihenfolge wie in [18] abgearbeitet, so terminiert die Prozedur höchstens zufällig.

Eine sinnvolle Strategie basiert nun auf der Tatsache, dass eine Zahl $k \in \mathbb{N}_0$ existiert, so dass die gesuchte differentielle σ-Gröbnerbasis G in dem von $\{\partial^j f \mid f \in F, 0 \leq j \leq k\}$ erzeugten Ideal liegt. Werden die zugehörige S-Polynome hierbei geeignet abgearbeitet, so wird die Menge G nach endlich vielen Schritten gefunden. Da k jedoch unbekannt ist, schließt sich eine gradweise Vorgehensweise wegen $\deg(f) = \deg(\partial f)$ aus. Eine geeignete Größe stellt stattdessen das Gewicht eines Polynoms dar. Dazu definieren wir, in Anlehnung an den „Phantomgrad“ eines Polynoms (siehe [8]), das *Phantomgewicht* wie folgt. Für jedes $f \in F \backslash \{0\}$ setzen wir zunächst $\mathrm{pw}(f) = w(f)$. Weiter sei $\mathrm{pw}(tf) = w(t) + \mathrm{pw}(f)$, $\mathrm{pw}(f+g) = \max\{\mathrm{pw}(f), \mathrm{pw}(g)\}$ und $\mathrm{pw}(f^{(k)}) = \mathrm{pw}(f) + k$ für alle $t \in \mathbb{T}^n$, $g \in D \backslash \{0\}$ und $k \geq 0$. Auf diese Weise wird eine Gewichtshomogenisierung der beteiligten Polynome simuliert. Dabei ist zu beachten, dass bei einem Reduktionsschritt das Phantomgewicht des jeweiligen Polynoms ansteigen kann.

Das Phantomgewicht liefert uns nun ein Auswahlkriterium für die als nächstes zu betrachtenden fundamentalen kritischen Paare. Hierfür bezeichnen wir mit dem Phantomgewicht eines kritischen Paares das des zugehörigen S-Polynoms. Entscheidend ist, dass es für jedes $w \in \mathbb{N}_0$ nur jeweils endlich viele fundamentale kritische Paare mit Phantomgewicht w gibt. Darauf werden wir später aber noch genauer eingehen.

Wir sind nun in der Lage, eine wesentlich effizientere Prozedur als in Satz 2.5.4 anzugeben. Für eine Menge $G = \{g_1, \ldots, g_s\}$ von Polynomen bezeichnen wir dabei mit $\mathcal{G}$ das zugehörige Tupel $(g_1, \ldots, g_s)$ aller von Null verschiedenen Polynome in G. Für $i = 1, \ldots, s$ sei dann $\mathcal{G}_i = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_s)$ das Tupel der von Null und g_i verschiedenen Polynome in G.

Satz 2.5.15. *Sei $F = \{g_1, \ldots, g_s\} \subseteq D\backslash\{0\}$ und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Dabei sei $\mathrm{LT}_\sigma(g_i^{(k)}) = t_i u_i^{(k)}$ für $i = 1, \ldots, s$ und jedes $k \geq 0$. Wir betrachten die durch die folgenden Instruktionen definierte Prozedur* `DiffGB`(F):

1) *Setze $G = F$, $w = 0$ und $\mathrm{pw}(g_i) = w(g_i)$ für $i = 1, \ldots, s$. Weiter sei $\tilde{s} = s$ und $B = \{(i,j) \mid 1 \leq i \leq j \leq s\}$.*
2) *Existieren Indizes $i, j \in \{1, \ldots, \tilde{s}\}$ mit $i \neq j$, so dass $\mathrm{LT}_\sigma(g_i)$ bzgl. $\{g_j\}$ reduzibel ist, so ersetze g_i durch $\mathrm{DR}_{\sigma,\mathcal{G}_i}(g_i)$ und entferne jedes Paar (i_1, i_2) mit $i_1 = i$ oder $i_2 = i$ aus B. Gilt dabei $\mathrm{DR}_{\sigma,\mathcal{G}_i}(g_i) \neq 0$, so erweitere B um die Menge der Paare $\{(k,i) \mid 1 \leq k \leq i,\ g_k \neq 0\} \cup \{(i,k) \mid i+1 \leq k \leq \tilde{s},\ g_k \neq 0\}$. Fahre mit 2) fort.*
3) *Entferne aus B jedes Paar (i,i), für das $\mathrm{LT}_\sigma(g_i)$ ein Derivat ist, und jedes Paar (i,j), für das sowohl $\mathrm{LT}_\sigma(g_i)$ und $\mathrm{LT}_\sigma(g_j)$ teilerfremd als auch u_i und u_j Derivate unterschiedlicher differentieller Unbestimmter sind. Gilt $B = \emptyset$, so gib $G\backslash\{0\}$ aus und stoppe.*
4) *Bestimme die Menge B_w der fundamentalen kritischen Paare $((i,k_i),(j,k_j))$ von G mit Phantomgewicht w und $(i,j) \in B$.*
5) *Gilt $B_w = \emptyset$, so erhöhe w um Eins und fahre mit 2) fort. Ansonsten wähle ein kritisches Paar $((i,k_i),(j,k_j))$ aus B_w und entferne es aus B_w. Erfüllt es eines der Kriterien C1)–C3), so entferne (i,j) aus B. Ist C3) erfüllt, so fahre mit 5) fort.*
6) *Bestimme das zugehörige S-Polynom S und $g_{\tilde{s}+1} = \mathrm{DR}_{\sigma,\mathcal{G}}(S)$. Ist $g_{\tilde{s}+1} = 0$, so fahre mit 5) fort.*
7) *Füge $g_{\tilde{s}+1}$ zu G hinzu und ersetze $\tilde{s}$ durch $\tilde{s}+1$. Erweitere B um die Menge der Paare $\{(i,\tilde{s}) \mid 1 \leq i \leq \tilde{s},\ g_i \neq 0\}$ und B_w um alle fundamentalen kritischen Paare $((i,k_i),(\tilde{s},k_{\tilde{s}}))$ mit Phantomgewicht w und $(i,\tilde{s}) \in B$. Fahre mit 5) fort.*

Dies ist eine Prozedur, die, falls sie endet, eine endliche differentielle σ-Gröbnerbasis von $\langle F\rangle_\partial$ ausgibt.

Beweis. Wir zeigen, dass die Voraussetzungen von Satz 2.5.13 erfüllt sind, wenn die Prozedur terminiert. Zunächst ist wegen $B = \emptyset$ und Schritt 2) für jedes $g \in G$ der Leitterm von g reduziert bzgl. $G\backslash\{g\}$. Es bleibt nun noch zu zeigen, dass für jedes fundamentale kritische Paar von G das zugehörige S-Polynom bzgl. G zu Null reduziert oder die Bedingung C3) erfüllt ist. Seien dazu $i, j \in \{1, \dots, \tilde{s}\}$ mit $i \leq j$. Sind die Bedingungen aus Schritt 3) erfüllt, so reduziert jedes S-Polynom $S(g_i^{(k)}, g_j^{(l)})$ mit $k, l \in \mathbb{N}_0$ nach Lemma 2.5.3 bzgl. G zu Null. Ist dies nicht der Fall, so wird für ein $w \in \mathbb{N}_0$ das Paar (i, j) in Schritt 5) aus B entfernt, d.h. das entsprechende fundamentale kritische Paar $((i, k_i), (j, k_j))$ erfüllt eine der Bedingungen C1)–C3) und alle S-Polynome mit kleinerem Phantomgewicht reduzieren bzgl. G zu Null. Ist C1) oder C2) erfüllt, so ist es das einzige fundamentale kritische Paar zwischen g_i und g_j. Dann gilt zugleich $\mathrm{DR}_{\sigma,\mathcal{G}}(S(g_i^{(k_i)}, g_j^{(k_j)})) = 0$ oder das Kriterium C3). Erfüllt es C3), so gilt dies nach Bemerkung 2.5.14 auch für alle verbleibenden fundamentalen kritischen Paare zwischen g_i und g_j, denn für jedes solche Paar $((i, l_i), (j, l_j))$ mit Phantomgewicht größer oder gleich w gilt entweder $l_i > k_i$ und $l_j \geq k_j$ oder $l_i \geq k_i$ und $l_j > k_j$. Dabei spielt es im Übrigen keine Rolle, ob das zugehörige Polynom g_l im Laufe der Prozedur durch einen differentiellen Rest in Schritt 2) ersetzt wurde, da auf jeden Fall ein Polynom g_m mit $m \neq l$ in G verbleibt, für das $\mathrm{LT}_\sigma(g_m^{(k_m)})$ für ein $k_m \geq 0$ ein Teiler von $\mathrm{LT}_\sigma(g_l)$ ist. Somit bleibt das Kriterium C3) auch weiterhin erfüllt. □

Terminiert die Prozedur `DiffGB`, so ist die Ausgabe G sogar eine *minimale* differentielle σ-Gröbnerbasis, d.h. G hat minimale Länge und die Menge der Leitterme aller Polynome in G entspricht derjenigen der reduzierten differentiellen σ-Gröbnerbasis. Dies garantiert Schritt 2) der Prozedur, in der für jedes $w \in \mathbb{N}_0$ die jeweils aktuellen Polynome der Menge G entsprechend reduziert werden.

Beispiel 2.5.16. Wir betrachten wieder die Polynome $g_1 = y_1^{(1)} y_2 + y_2$, $g_2 = (y_2^{(1)})^2 + y_1^{(1)}$ und $g_3 = y_1^{(2)} + y_1^{(1)} + 1$ aus Beispiel 2.5.8. Für $\sigma =$ `DegLex` mit $y_1^{(k)} <_\sigma y_2$ und $F = \{g_1, g_2, g_3\}$ folgen wir den Instruktionen aus Satz 2.5.15, wobei wir nicht alle Zwischenschritte explizit angeben.

1) Wir setzen $G = \{g_1, g_2, g_3\}$, $w = 0$, $\mathrm{pw}(g_1) = 1$, $\mathrm{pw}(g_2) = 2$, $\mathrm{pw}(g_3) = 2$ und $\tilde{s} = 3$. Zudem ist $B = \{(1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$.
2) Da $\mathrm{LT}_\sigma(g_i)$ für $i = 1, 2, 3$ bzgl. $G \backslash \{g_i\}$ reduziert ist, bleibt B unverändert.
3) Die Bedingung aus 3) ist für die Paare $(3,3)$, $(1,3)$ und $(2,3)$ erfüllt, also setzen wir $B = \{(1,1), (1,2), (2,2)\}$.
4) Es ist $B_0 = \emptyset$. Da auch $B_1 = \emptyset$ gilt, fahren wir mit $w = 2$ fort.
4) Wir setzen $B_2 = \{((1,1), (1,0))\}$.
5) Wir wählen das kritische Paar $((1,1), (1,0))$, entfernen es aus B_2 und erhalten $B_2 = \emptyset$. Das Paar erfüllt keines der Kriterien C1)–C3).
6) Es ergibt sich $S((1,1), (1,0)) = y_2 g_1^{(1)} - y_2^{(1)} g_1 = y_1^{(2)} y_2^2$ und die Reduktionskette $S((1,1), (1,0)) \xrightarrow{g_3} -y_1^{(1)} y_2^2 - y_2^2 \xrightarrow{g_1} 0$. Wir fahren also mit 5) fort.
5) Wegen $B_2 = \emptyset$ erhöhen wir w um Eins. Da sich G und B nicht verändert haben, fahren wir direkt mit 4) fort.
4) Wir setzen $B_3 = \{((1,1), (2,0))\}$.
5) Wir wählen das kritische Paar $((1,1), (2,0))$ und entfernen es aus B_3. Dieses Paar erfüllt Kriterium C2), d.h. wir entfernen $(1,2)$ aus B.

6) Es ist $S((1,1),(2,0)) = y_2^{(1)} g_1^{(1)} - y_1^{(1)} g_2 = y_1^{(2)} y_2 y_2^{(1)} + (y_2^{(1)})^2 - (y_1^{(1)})^2$ das zugehörige S-Polynom und durch

$$\begin{aligned} S((1,1),(2,0)) &\xrightarrow{g_3} y_1^{(1)} y_2 y_2^{(1)} - y_2 y_2^{(1)} + (y_2^{(1)})^2 - (y_1^{(1)})^2 \\ &\xrightarrow{g_1} (y_2^{(1)})^2 - (y_1^{(1)})^2 \\ &\xrightarrow{g_2} -(y_1^{(1)})^2 - y_1^{(1)} = g_4 \end{aligned}$$

ergibt sich ein von Null verschiedener differentieller Rest mit $\mathrm{pw}(g_4) = 3$.

7) Also setzen wir $G = \{g_1, g_2, g_3, g_4\}$, $\tilde{s} = 4$ und zugleich

$$B = \{(1,1),(2,2),(1,4),(2,4),(3,4),(4,4)\}$$

bzw. $B_3 = \{((1,0),(4,0))\}$.

5) Für das kritische Paar $((1,0),(4,0))$ ergibt sich für das zugehörige S-Polynom direkt $S((1,0),(4,0)) = y_1^{(1)} g_1 + y_2 g_4 = 0$. Also setzen wir $w = 4$.

3) Wir streichen das Paar $(2,4)$ aus B.

4) Es ist $B_4 = \{((1,2),(1,1)),((2,1),(2,0)),((1,0),(4,1)),((3,0),(4,1))\}$.

6) Das kritische Paar $((1,2),(1,1))$ erfüllt keines der Kriterien C1)–C3) und für das S-Polynom $S((1,2),(1,1)) = y_2^{(1)} g_1^{(2)} - y_2^{(2)} g_1^{(1)} = 2y_1^{(2)} (y_2^{(1)})^2 + y_1^{(3)} y_2 y_2^{(1)} - y_1^{(2)} y_2 y_2^{(2)}$ erhalten wir durch

$$\begin{aligned} S((1,2),(1,1)) &\xrightarrow{g_3} y_1^{(1)} y_2 y_2^{(2)} + y_2 y_2^{(2)} + 2y_1^{(2)} (y_2^{(1)})^2 + y_1^{(3)} y_2 y_2^{(1)} \\ &\xrightarrow{g_1} 2y_1^{(2)} (y_2^{(1)})^2 + y_1^{(3)} y_2 y_2^{(1)} \\ &\xrightarrow{g_2} -2y_1^{(1)} y_1^{(2)} + y_1^{(3)} y_2 y_2^{(1)} \\ &\xrightarrow{g_3} -2y_1^{(1)} y_1^{(2)} - y_1^{(2)} y_2 y_2^{(1)} \\ &\xrightarrow{g_3} -2y_1^{(1)} y_1^{(2)} + y_1^{(1)} y_2 y_2^{(1)} + y_2 y_2^{(1)} \\ &\xrightarrow{g_1} -2y_1^{(1)} y_1^{(2)} \\ &\xrightarrow{g_4} y_1^{(2)} \\ &\xrightarrow{g_3} -y_1^{(1)} - 1 = g_5 \end{aligned}$$

ein neues Element von G mit $\mathrm{pw}(g_5) = 4$. Wir fügen die Paare $(1,1),\ldots,(1,5)$ zu B und $((1,0),(5,0))$ zu B_4 hinzu.

6) Für das S-Polynom $S((2,1),(2,0)) = \frac{1}{2}\, y_2^{(1)} g_2^{(1)} - y_2^{(2)} g_2 = \frac{1}{2}\, y_1^{(2)} y_2^{(1)} - y_1^{(1)} y_2^{(2)}$ ergibt sich durch die Reduktion

$$\begin{aligned} S((2,1),(2,0)) &\xrightarrow{g_1} \tfrac{5}{2}\, y_1^{(2)} y_2^{(1)} + y_1^{(3)} y_2 + y_2^{(2)} \\ &\xrightarrow{g_3} -\tfrac{5}{2}\, y_1^{(1)} y_2^{(1)} - \tfrac{5}{2}\, y_2^{(1)} + y_1^{(3)} y_2 + y_2^{(2)} \\ &\xrightarrow{g_1} \tfrac{5}{2}\, y_1^{(2)} y_2 + y_1^{(3)} y_2 + y_2^{(2)} \\ &\xrightarrow{g_3} \tfrac{3}{2}\, y_1^{(2)} y_2 + y_2^{(2)} \\ &\xrightarrow{g_3} -\tfrac{3}{2}\, y_1^{(1)} y_2 - \tfrac{3}{2}\, y_2 + y_2^{(2)} \\ &\xrightarrow{g_1} y_2^{(2)} = g_6 \end{aligned}$$

ein weiteres Element von G mit Phantomgewicht $\mathrm{pw}(g_6) = 4$.

7) Wir erweitern B um die Paare $(1,6), \dots, (6,6)$.
5) Die kritischen Paare $((1,0),(4,1))$ und $((3,0),(4,1))$ erfüllen Kriterium C3) jeweils mit g_5, d.h. wir entfernen diese aus B_4 und die Paare $(1,4),(3,4)$ aus B. Schließlich genügt $((1,0),(5,0))$ Kriterium C2) mit $S((1,0),(5,0)) = g_1 + y_2 g_5 = 0$. Es ist nun $B_4 = \emptyset$, $B = \{(1,1),(2,2),(4,4),(2,5),\dots,(5,5),(1,6),\dots,(6,6)\}$ und $w = 5$.
2) Es reduzieren g_1, g_3 und g_4 bzgl. $\{g_5\}$ zu Null, d.h. wir haben $\mathcal{G} = (0, g_2, 0, 0, g_5, g_6)$ und $B = \{(2,2),(2,5),(5,5),(2,6),(5,6),(6,6)\}$.
3) Wir setzen $B = \{(2,2),(2,6)\}$ und $B_5 = \{((2,2),(2,1)),((2,1),(6,0))\}$.
5) Für das erste kritische Paar ist C3) mit g_6 erfüllt und C2) für das zweite mit $\mathrm{DR}_{\sigma,\mathcal{G}}(S((2,1),(6,0))) = 0$. Wegen $B_5 = \emptyset$ und $B = \emptyset$ stoppt die Prozedur und gibt die Menge $G = \{g_2, g_5, g_6\}$ aus.

Die Tatsache, dass die Prozedur im obigen Beispiel terminiert, ist kein Zufall. Denn das differentielle Ideal $\langle g_1, g_2, g_3\rangle_\partial$ ist null-dimensional und für solche Ideale gibt `DiffGB` stets nach endlich vielen Schritten eine differentielle Gröbnerbasis aus. Um diese und weitere Aussagen treffen zu können, wollen wir zunächst das Verhalten der Prozedur genauer studieren. Dazu bezeichnen wir im Weiteren mit G_w für jedes $w \in \mathbb{N}_0$ die Menge G in der Prozedur nach Abarbeitung aller S-Polynome mit Phantomgewicht w.

Satz 2.5.17. *Sei $F = \{g_1, \dots, g_s\} \subseteq D \backslash \{0\}$ und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Es werde die Prozedur* `DiffGB` *auf F angewendet.*

a) Für jedes $w \in \mathbb{N}_0$ werden nur endlich viele fundamentale kritische Paare zu B_w hinzugefügt.
b) Für jedes $w \in \mathbb{N}_0$ und jedes S-Polynom S von G_w existiert ein $\widetilde{w} \geq w$, so dass gilt $\mathrm{rg}_{\sigma, G_{\widetilde{w}}}(S) <_\sigma t_S$.
c) Für jedes Polynom $f \in \langle F\rangle_\partial \backslash \{0\}$ existiert ein $w \in \mathbb{N}_0$, so dass f bzgl. G_w zu Null reduziert.

Beweis. Für den Beweis von a) sei $w \in \mathbb{N}_0$ und B_w die Menge aller fundamentaler kritischer Paare von G_{w-1}, wobei $G_{-1} = G$ ist. Dann ist B_w zunächst endlich, da es zwischen g_i und g_j für $g_i, g_j \in G_{w-1}$ jeweils höchstens ein fundamentales kritisches Paar mit Phantomgewicht w gibt. Es genügt nun zu zeigen, dass zu G_{w-1} nur endlich viele Polynome mit Phantomgewicht w hinzugefügt werden. Dies folgt aber direkt aus der Tatsache, dass lediglich reduzierte Elemente hinzugefügt werden und alle Polynome in G_w Elemente des noetherschen Rings D_w sind.

Um b) zu zeigen, genügt es nach Lemma 2.5.11, die Aussage für das S-Polynom S eines fundamentalen kritischen Paares $((i,k_i),(j,k_j))$ von G_w zu beweisen. Des Weiteren ist zu berücksichtigen, dass g_i oder g_j in Schritt 2) ersetzt werden könnten, bevor das kritische Paar abgearbeitet wird. Ist dies der Fall, O.B.d.A. für g_i, so existiert ein $g_m \in G_{\overline{w}}$ mit $m \neq i$ und $\overline{w} \leq \mathrm{pw}(S)$, so dass $\mathrm{LT}_\sigma(g_m^{(k_m)})$ für ein $k_m \geq 0$ ein Teiler von $\mathrm{LT}_\sigma(g_i)$ ist. Das Polynom S kann dann geschrieben werden als $S = tS(g_m^{(\tilde{k}_m)}, g_j^{(k_j)}) + g$ für ein $t \in \mathbb{T}^n$,

$\tilde{k}_m \geq k_m$ und ein $g \in \langle G \rangle_\partial$ mit $\mathrm{rg}_{\sigma, G_{\overline{w}}}(g) <_\sigma t_S$. Nach Lemma 2.5.11 a) gilt weiter $S = \sum_{i=1}^{r} c_i t_i S_i^{(m_i)} + \tilde{g}$ mit $c_i \in K \backslash \{0\}$, $t_i \in \mathbb{T}^n$, $m_i \in \mathbb{N}_0$ für $i = 1, \ldots, r$, $\tilde{g} \in \langle G \rangle_\partial$ und $\mathrm{rg}_{\sigma, G_{\overline{w}}}(\tilde{g}) <_\sigma t_S$, sowie S-Polynomen $S_1, \ldots, S_r$ von fundamentalen kritischen Paaren von $G_{\overline{w}}$ der Form $((i_1, l_1), (i_2, l_2))$ mit $i_1, i_2 \in \{m, j\}$, $l_1, l_2 \geq 0$ und $\mathrm{LT}_\sigma(t_{S_i}^{(m_i)}) \leq_\sigma t_S$ für $i = 1, \ldots, r$. Wird für eines dieser S-Polynome g_{i_1} oder g_{i_2} wieder ersetzt, bevor das zugehörige Paar abgearbeitet wird, so können wir es durch eine entsprechende Summe in der Darstellung von S ersetzen. Dies kann insgesamt nur endlich oft vorkommen, da bei einer Ersetzung wie oben von g_i das beteiligte Polynom g_m einen bzgl. σ echt kleineren Leitterm als $\mathrm{LT}_\sigma(g_i)$ besitzt. Also dürfen wir nun annehmen, dass das kritische Paar $((i, k_i), (j, k_j))$ abgearbeitet wird, ohne dass g_i oder g_j zuvor ersetzt wurde.

Erfüllt das Paar nun im entsprechenden Durchlauf von Schritt 5) nicht Kriterium C3), so reduziert S bzgl. $G_{\mathrm{pw}(S)+1}$ zu Null. Andernfalls existiert ein Polynom $g_l \in G_{\mathrm{pw}(S)+1}$ wie in C3). Ist $i = j$, so können wir S wie in (2.1) als Summe von Polynomen der Form $\tilde{t}\tilde{S}$ schreiben, wobei $\tilde{t} \in \mathbb{T}^n$ und $\tilde{S}$ ein S-Polynom von $G_{\mathrm{pw}(S)+1}$ zwischen g_i und g_l oder g_l und g_l ist mit $t_{\tilde{S}} <_\sigma t_S$. Nach Lemma 2.5.11 a) erhalten wir daraus eine Darstellung $S = \sum_{i=1}^{r} c_i t_i S_i^{(m_i)} + g$ mit $c_i \in K \backslash \{0\}$, $t_i \in \mathbb{T}^n$, $m_i \in \mathbb{N}_0$ für $i = 1, \ldots, r$, $g \in \langle G \rangle_\partial$ und $\mathrm{rg}_{\sigma, G_{\mathrm{pw}(S)+1}}(g) <_\sigma t_S$, sowie S-Polynomen $S_1, \ldots, S_r$ von fundamentalen kritischen Paaren von $G_{\mathrm{pw}(S)+1}$ der Form $((i_1, l_1), (i_2, l_2))$ mit $i_1, i_2 \in \{i, l\}$, $l_1, l_2 \geq 0$ und $t_{S_i} <_\sigma t_S$ für $i = 1, \ldots, r$. Die gleiche Aussage können wir nun auch für den Fall $i \neq j$ mit Hilfe von (2.2) treffen, wobei S_k jeweils ein S-Polynom eines fundamentalen kritischen Paares der Form $((i_1, l_1), (i_2, l_2))$ mit $i_1, i_2 \in \{i, j, l\}$ und $l_1, l_2 \geq 0$ ist. Die beschriebene Vorgehensweise können wir wieder auf jedes der S-Polynome $S_1, \ldots, S_r$ anwenden. Nach endlich vielen Wiederholungen reduziert jedes der beteiligten S-Polynome für ein genügend großes $\widetilde{w} \in \mathbb{N}$ bzgl. $G_{\widetilde{w}}$ zu Null, denn die Terme t_S liefern eine echt absteigende Kette von Termen.

Für c) genügt es zu zeigen, dass zu jedem Polynom $f \in \langle F \rangle_\partial \backslash \{0\}$ ein $w \in \mathbb{N}_0$ existiert, so dass f bzgl. G_w reduzibel ist. Denn dann würde dies auch auf $\mathrm{DR}_{\sigma, \mathcal{G}_w}(f)$ zutreffen und die Behauptung aus der Wohlordnungseigenschaft von σ auf $\mathbb{T}^n$ und der Tatsache folgen, dass $\xrightarrow{G_w}$ für jedes $w \in \mathbb{N}_0$ noethersch ist. Wir schreiben nun das Polynom f zunächst als $f = \sum_{j=1}^{r} c_j t_j g_{i_j}^{(k_j)}$ mit $c_j \in K \backslash \{0\}$, $t_j \in \mathbb{T}^n$, $k_j \geq 0$, $g_{i_j} \in G$ und $t_j \, \mathrm{LT}_\sigma(g_{i_j}^{(k_j)}) \leq_\sigma \mathrm{rg}_{\sigma, G}(f)$ für $j = 1, \ldots, r$. Gilt dabei $\mathrm{rg}_{\sigma, G}(f) = \mathrm{LT}_\sigma(f)$, so ist f bereits bzgl. G reduzibel. Im Fall $\mathrm{rg}_{\sigma, G}(f) >_\sigma \mathrm{LT}_\sigma(f)$ bezeichne $\mathcal{I} \subseteq \{1, \ldots, r\}$ die Menge aller Indizes j mit $t_j \, \mathrm{LT}_\sigma(g_{i_j}^{(k_j)}) = \mathrm{rg}_{\sigma, G}(f)$. Dann ist das Polynom $\tilde{f} = \sum_{j \in \mathcal{I}} c_j t_j g_{i_j}^{(k_j)}$ eine Summe von S-Polynomen, d.h. $\tilde{f} = \sum_{j=1}^{|\mathcal{I}|-1} \tilde{c}_j \tilde{t}_j S_j$ mit $\tilde{c}_j \in K \backslash \{0\}$, $\tilde{t}_j \in \mathbb{T}^n$ und S-Polynomen S_j zwischen den Polynomen aus $\{g_{i_j} \mid j \in \mathcal{I}\}$ für $j = 1, \ldots, |\mathcal{I}| - 1$. Nach b) besitzen letztere bzgl. G_w einen Rang echt kleiner als t_{S_j} für ein genügend großes $w \in \mathbb{N}$, also gilt $\mathrm{rg}_{\sigma, G_w}(f) <_\sigma \mathrm{rg}_{\sigma, G}(f)$. Mit f und G_w können wir unser obiges Vorgehen wiederholen und erhalten ein $\widetilde{w} \geq w$, so dass $\mathrm{rg}_{\sigma, G_{\widetilde{w}}}(f) <_\sigma \mathrm{rg}_{\sigma, G_w}(f)$ erfüllt ist. Da σ eine Wohlordnung ist, endet dieses Verfahren nach endlich vielen Schritten. $\square$

Satz 2.5.18. *Sei σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Weiter sei $F = \{g_1, \ldots, g_s\} \subseteq D\backslash\{0\}$ eine Menge von Polynomen, so dass das von F differentiell erzeugte Ideal $I \subseteq D$ eine endliche differentielle σ-Gröbnerbasis besitzt.*

a) Wird die Prozedur `DiffGB` *auf F angewendet, so berechnet diese in endlich vielen Schritten eine endliche differentielle σ-Gröbnerbasis von I.*

b) Ist I null-dimensional, so terminiert `DiffGB`(F) *in endlich vielen Schritten mit der Ausgabe einer endlichen differentiellen σ-Gröbnerbasis von I.*

Beweis. Für den Beweis von a) sei G eine endliche differentielle σ-Gröbnerbasis von $\langle F\rangle_\partial$. Nach Satz 2.5.17 c) existiert dann ein $w \in \mathbb{N}_0$, so dass jedes Polynom aus G bzgl. G_w zu Null reduziert. Insbesondere existiert damit zu jedem $g \in G$ ein $\tilde{g} \in G_w$, so dass $\mathrm{LT}_\sigma(g)$ für ein $k \geq 0$ ein Vielfaches von $\mathrm{LT}_\sigma(\tilde{g}^{(k)})$ ist. Also ist G_w eine endliche differentielle σ-Gröbnerbasis von $\langle F\rangle_\partial$.

Um b) zu zeigen, dürfen wir nach a) annehmen, dass G_w für ein $w \in \mathbb{N}_0$ eine differentielle σ-Gröbnerbasis von I ist. Nach Satz 2.4.6 existiert in G_w für $i = 1, \ldots, n$ insbesondere ein Polynom h_i, so dass $\mathrm{LT}_\sigma(h_i) = y_i^{(l_i)}$ für ein $l_i \geq 0$ gilt. Es genügt nun zu beweisen, dass die Anzahl der fundamentalen kritischen Paare, die im Laufe der Prozedur noch betrachtet werden, endlich ist. Angenommen, es existiert ein Paar $(i, j) \in B$, so dass es unendlich viele fundamentale kritische Paare $((i, k_i), (j, k_j))$ gibt. Für diese sind dann jeweils die Kriterien C1) und C2) nicht erfüllt. Wir zeigen nun, dass hingegen mindestens eines das Kriterium C3) erfüllt. Dazu sei wieder $\mathrm{LT}_\sigma(g_l^{(k)}) = t_l u_l^{(k)}$ mit $t_l \in \mathbb{T}^n$, $u_l \in \mathbb{D}^n$ für $l = i, j$ und jedes $k \geq 0$. Wie bereits erwähnt, existieren nach Satz 2.4.6 und unter Berücksichtigung von Schritt 2) Polynome $f_1, f_2 \in G_w$ mit $u_i^{(l_i)} = \mathrm{LT}_\sigma(f_1)$ und $u_j^{(l_j)} = \mathrm{LT}_\sigma(f_2)$ für gewisse $l_i, l_j \in \mathbb{N}$. Nun ist entweder $((i, l_i), (j, k))$ oder $((i, k), (j, l_j))$ für ein $k \in \mathbb{N}_0$ ein fundamentales kritisches Paar von G_w. O.B.d.A. sei dies $((i, l_i), (j, k))$ mit S-Polynom S_{ij}. Zwischen g_i und f_1 existiert genau ein fundamentales kritisches Paar mit S-Polynom $S = S(g_i^{(l_i)}, f_1)$. Zudem ist $t_{(i,l_i),(j,k)}$ ein echtes Vielfaches von t_S, und die Leitterme von $g_j^{(l)}$ und f_1 sind für jedes $l \geq 0$ teilerfremd. Also ist das Kriterium C3) für $((i, l_i), (j, k))$ erfüllt. □

Die Prozedur `DiffGB` berechnet also in endlich vielen Schritten eine differentielle Gröbnerbasis von $\langle F\rangle_\partial$. Leider fehlt aber ein Kriterium, welches auch für höher dimensionale Ideale garantiert, dass die Prozedur in diesem Fall abbricht. Denn obgleich eine differentielle Gröbnerbasis gefunden wurde, kann die Menge der noch zu betrachtenden fundamentalen kritischen Paare unendlich sein und bleiben. Betrachten wir z.B. die Menge $G = \{y_1^{(1)}, y_1 y_2\}$ aus Beispiel 2.4.5, so ist der Faktorring $\mathbb{Q}\{y_1, y_2\}/\langle G\rangle_\partial$ eindimensional und G für jedes Ranking τ auf $\mathbb{D}^n$ mit $y_1 <_\tau y_2$ eine endliche differentielle τ`Lex`-Gröbnerbasis von $\langle G\rangle_\partial$. Jedoch existieren unendlich viele fundamentale kritische Paare, die durch keines der Kriterien eliminiert werden können.

Das dies nicht das einzige Beispiel eines Erzeugendensystems ist, für das die Prozedur `DiffGB` nicht terminiert, zeigt der folgende Satz. Er stellt einen Zusammenhang zwischen dem Terminieren der Prozedur und der Gestalt der reduzierten differentiellen

Gröbnerbasis her, also eine eindeutige Charakterisierung aller Erzeugendensysteme, deren differentielles Erzeugnis zwar eine endliche differentielle Gröbnerbasis besitzt, diese aber nicht von der Prozedur ausgegeben wird. Für ein Polynom $g_i \in D\backslash\{0\}$ sei wieder $\mathrm{LT}_\sigma(g_i^{(k)}) = t_i u_i^{(k)}$ für ein $t_i \in \mathbb{T}^n$, $u_i \in \mathbb{D}^n$ und jedes $k \geq 0$.

Satz 2.5.19. *Sei $F \subseteq D\backslash\{0\}$ eine endliche Polynommenge und σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$. Die auf F angewandte Prozedur* `DiffGB` *terminiert genau dann, wenn die reduzierte differentielle σ-Gröbnerbasis von $\langle F\rangle_\partial$ die Gestalt $\{g_1, \dots, g_s\}$ besitzt mit $s \geq N = n - \dim(D/I)$, $\mathrm{LT}_\sigma(g_j) = y_{i_j}^{(k_j)}$ für ein $k_j \geq 0$, $i_j \in \{1, \dots, n\}$ und $j = 1, \dots, N$ und $\mathrm{LV}_\sigma(u_i) \in \{y_{i_1}, \dots, y_{i_N}\}$ für $i = N+1, \dots, s$.*

Beweis. Terminiert die Prozedur, so ist deren Ausgabe G eine endliche und minimale differentielle σ-Gröbnerbasis von $\langle F\rangle_\partial$, die nach Satz 2.4.6 genau N Polynome enthält, deren Leitterme bzgl. σ Derivate paarweise verschiedener differentieller Unbestimmter $y_{i_1}, \dots, y_{i_N}$ sind. Angenommen, es gibt in der reduzierten differentiellen σ-Gröbnerbasis, und damit auch in G, ein weiteres Polynom g_j mit $\mathrm{LV}_\sigma(u_j) \notin \{y_{i_1}, \dots, y_{i_N}\}$. Dabei sei g_j derart gewählt, dass der Term t_j minimal bzgl. σ ist. Dann ist der Leitterm von g_j kein Derivat, und g_j besitzt unendlich viele fundamentale kritische Paare mit sich selbst, von denen keines Kriterium C3) erfüllt. Denn würde ein fundamentales kritisches Paar $((j, k_j), (j, k_j + 1))$ und ein Polynom $g_l \in G$ wie in C3) existieren, so würde t_l ein Teiler von t_j und $\mathrm{LT}_\sigma(g_l^{(k)})$ für ein $k \geq 0$ ein Teiler von $\mathrm{LT}_\sigma(g_j^{(k_j)})$ sein. Da $\mathrm{LT}_\sigma(g_j)$ bzgl. $G\backslash\{g_j\}$ reduziert ist, kann $\mathrm{LT}_\sigma(g_l^{(k)})$ nicht t_j teilen, d.h. es gilt $u_l^{(k)} = u_j^{(k_j)}$. Wegen der Minimalität von t_j folgt daraus $t_l = t_i$. Dann ist aber $\mathrm{LT}_\sigma(g_l)$ oder $\mathrm{LT}_\sigma(g_j)$ reduzibel bzgl. $\{g_j\}$ bzw. bzgl. $\{g_l\}$, ein Widerspruch.

Sei nun umgekehrt die reduzierte differentielle σ-Gröbnerbasis G von $\langle F\rangle_\partial$ von der angegebenen Gestalt. Dann existiert nach Satz 2.5.18 ein $w \in \mathbb{N}_0$, so dass G_w eine differentielle σ-Gröbnerbasis von $\langle F\rangle_\partial$ mit der gleichen Leittermmenge wie G ist. Zu jedem verbliebenen Paar $(i, j) \in B$ gibt es nun entweder genau ein fundamentales kritisches Paar zwischen g_i und g_j oder unendlich viele, von denen mindestens eines Kriterium C3) erfüllt. Für letzteres verweisen wir auf den Beweis von Satz 2.5.18 b). □

In einigen Fällen ist zu einem bestimmten Zeitpunkt erkennbar, dass die Anzahl der noch zu untersuchenden fundamentalen kritischen Paare unendlich bleiben und die Prozedur `DiffGB` demnach nie terminieren wird. In diesen Fällen weist die aktuelle Polynommenge G eine spezielle Struktur auf. Genauer gilt das Folgende.

Korollar 2.5.20. *Sei σ eine strikt stabile differentielle Termordnung auf $\mathbb{T}^n$, $F \subseteq D\backslash\{0\}$ eine endliche Menge von Polynomen, auf die die Prozedur* `DiffGB` *angewendet wird, und $N = \dim(D/\langle F\rangle_\partial)$. Existieren ein $w \in \mathbb{N}_0$ und Polynome $g_1, \dots, g_{N+1} \in G_w$, so dass gilt $\mathrm{LT}_\sigma(g_j) = y_{i_j}^{(k_j)}$ und $y_{i_j}^{(k)} \notin \mathbb{D}(\mathrm{LT}_\sigma(g_{N+1}))$ mit $k_j \geq 0$, paarweise verschiedenen $i_j \in \{1, \dots, n\}$ für $j = 1, \dots, N$ und jedes $k \geq 0$, dann terminiert die Prozedur nicht.*

Beweis. Angenommen, die Prozedur endet nach endlich vielen Schritten. Dann muss es in der ausgegebenen Menge ein Polynom g geben, so dass $\mathrm{LT}_\sigma(g^{(k)})$ für ein $k \geq 0$ ein Teiler von $\mathrm{LT}_\sigma(g_{N+1})$ ist. Dies impliziert wiederum, dass jedes Derivat in $\mathrm{LT}_\sigma(g)$ nicht Derivat einer der differentiellen Unbestimmten $y_{i_1}, \ldots, y_{i_N}$ ist. Aber dies widerspricht der Aussage in Satz 2.5.19. □

Kapitel 3

Anwendungen

Im letzten Kapitel haben wir die wesentlichen Charakteristika von differentiellen Gröbnerbasen und eine Methode für deren Berechnung kennen gelernt. Wir wollen uns nun mit einigen Anwendungsgebieten der differentiellen Gröbnerbasistheorie beschäftigen.

Beginnen werden wir dabei mit der Eliminationstheorie, insbesondere mit einer differentiellen Version des Hauptsatzes der Eliminationstheorie und der Berechnung von Eliminationsidealen. Anschließend befassen wir uns mit Homomorphismen differentieller Algebren und deren Kern. Spezielle Betrachtung finden hierbei Einsetzhomomorphismen, da sich mit deren Hilfe zum Beispiel die differentiellen Relationen zwischen Polynomen bestimmen lassen. Das Thema des dritten Abschnitts ist die Berechnung aller Lösungen von differentiellen Gleichungssystemen, die durch Polynome $f_1, \dots, f_s$ aus $K\{y_1, \dots, y_n\}$ gegeben sind. Hierbei gehen wir nur auf solche Systeme ein, deren Lösungsmenge endlich ist. Wie sich umgekehrt zu einer endlichen Menge von Punkten alle Polynome finden lassen, die auf dieser verschwinden, werden wir im darauffolgenden Abschnitt studieren. Eine Antwort auf diese Frage liefert eine differentielle Version des Buchberger-Möller-Algorithmus. Zum Abschluss dieses Kapitels befassen wir uns schließlich mit der Problematik, die differentiellen Relationen zwischen unendlich oft differenzierbaren Funktionen zu finden, von denen lediglich die Funktionswerte an endlich vielen Stellen bis zu einer festgelegten Ordnung bekannt sind. Dazu folgen wir einem Ansatz aus [17] und erhalten eine geeignete Variation des differentiellen Buchberger-Möller-Algorithmus. Welche Auswirkungen dabei die Verwendung von empirischen Daten zur Folge hat und wie diese gehandhabt werden können, werden wir mit Hilfe numerischer Methoden diskutieren.

3.1 Differentielle Gröbnerbasen von Eliminationsidealen

In diesem Abschnitt wollen wir unsere Überlegungen zu Eliminationsidealen fortführen. In Abschnitt 1.7 haben wir bereits diskutiert, wie sich Eliminationsideale von differentiellen Prim- und Radikalidealen mit Hilfe von differentiellen Pseudo-Gröbnerbasen berechnen lassen. Um in ähnlicher Weise eine differentielle Gröbnerbasis angeben zu können, werden wir sogenannte differentielle Eliminationsordnungen betrachten. Denn ist G eine differentielle Gröbnerbasis bzgl. einer solchen differentiellen Termordnung, so bilden diejenigen Elemente in G, die kein Derivat der zu eliminierenden differentiellen Unbestimmten enthalten, eine differentielle Gröbnerbasis des zugehörigen Eliminationsideals. Ist die Termordnung schließlich noch strikt stabil und ∂-lexikographisch, so lässt sich im Falle der Endlichkeit von G jedes Eliminationsideal von $\langle G \rangle_\partial$ berechnen.

Im Folgenden sei $L \subseteq \{y_1, \ldots, y_n\}$, $\widehat{D}$ der differentielle Polynomring in den differentiellen Unbestimmten $\{y_1, \ldots, y_n\} \backslash L$ über K und $\widehat{\mathbb{T}}^n$ das Monoid aller Terme in $\widehat{D}$.

Definition 3.1.1. Eine differentielle Termordnung σ auf $\mathbb{T}^n$ heißt *differentielle Eliminationsordnung* für L, falls jedes Polynom $f \in D \backslash \{0\}$ mit $\mathrm{LT}_\sigma(f) \in \widehat{\mathbb{T}}^n$ bereits in $\widehat{D}$ enthalten ist.

Ist σ eine differentielle Eliminationsordnung für $L \subseteq \{y_1, \ldots, y_n\}$ und ist $y \in L$, so gilt offensichtlich $y >_\sigma \tilde{y}^{(k)}$ für jedes $k \geq 0$ und jede differentielle Unbestimmte $\tilde{y} \in \{y_1, \ldots, y_n\} \backslash L$. Damit ist das durch σ induzierte Ranking auf $\mathbb{D}^n$ auch stets ein Eliminationsranking für L.

Umgekehrt lässt sich aus einem Eliminationsranking auf einfache Weise eine differentielle Eliminationsordnung gewinnen, wie das folgende Beispiel zeigt.

Beispiel 3.1.2. Sei τ das Ranking auf $\mathbb{D}^n$ mit $y_i^{(k)} <_\sigma y_j$ für alle $k \geq 0$ und $i < j$. Dann ist die differentielle Termordnung $\tau\mathtt{Lex}$ auf $\mathbb{T}^n$ für jedes $i \in \{1, \ldots, n\}$ eine differentielle Eliminationsordnung für $L = \{y_i, \ldots, y_n\}$.

Diese Konstruktion einer differentiellen lexikographischen Eliminationsordnung funktioniert nicht nur für das Ranking aus dem obigen Beispiel, sondern für jedes beliebige Eliminationsranking auf $\mathbb{D}^n$.

Lemma 3.1.3. *Ist σ eine differentielle Termordnung auf $\mathbb{T}^n$, so ist die Restriktion $\widehat{\sigma}$ von σ auf $\widehat{\mathbb{T}}^n$ eine differentielle Termordnung auf $\widehat{\mathbb{T}}^n$.*

Beweis. Da $\widehat{\mathbb{T}}^n$ als Untermonoid von $\mathbb{T}^n$ angesehen werden kann, ist die Behauptung offensichtlich erfüllt. □

Wie für differentielle Pseudo-Gröbnerbasen gilt auch hier die folgende Version des Hauptsatzes der Eliminationstheorie.

Satz 3.1.4. *Sei $I \subseteq D$ ein differentielles Ideal, σ eine differentielle Eliminationsordnung für $L \subseteq \{y_1, \ldots, y_n\}$ auf $\mathbb{T}^n$ und $G \subseteq I \backslash \{0\}$ eine differentielle σ-Gröbnerbasis von I. Dann ist $\widehat{G} = G \cap \widehat{D}$ eine differentielle $\widehat{\sigma}$-Gröbnerbasis des differentiellen Eliminationsideals $\widehat{I}$ von I bzgl. L.*

Beweis. Sei $f \neq 0$ ein differentielles Polynom in $\widehat{I} \subseteq I$. Dann existiert nach Voraussetzung ein Polynom $g \in G$ und ein $k \in \mathbb{N}_0$, so dass $\mathrm{LT}_\sigma(f)$ ein Vielfaches von $\mathrm{LT}_\sigma(g^{(k)})$ ist, d.h. es ist $\mathrm{LT}_\sigma(g^{(k)})$ und damit auch $\mathrm{LT}_\sigma(g)$ ein Element von $\widehat{D}$. Da σ eine Eliminationsordnung für L ist, impliziert dies gerade $g \in \widehat{D}$. Also ist $g \in \widehat{G}$ und $\widehat{G}$ eine differentielle $\widehat{\sigma}$-Gröbnerbasis von $\widehat{I}$. □

Bei einer geeigneten Wahl von L können wir für das zugehörige Eliminationsideal sogar eine endliche differentielle Gröbnerbasis berechnen, falls eine solche existiert.

Satz 3.1.5. *Sei $F \subseteq D \backslash \{0\}$ eine endliche Menge von Polynomen, $Y \subseteq \{y_1, \ldots, y_n\}$ maximal differentiell unabhängig modulo $\langle F \rangle_\partial$ und σ eine strikt stabile, ∂-lexikographische, differentielle Eliminationsordnung für $\{y_1, \ldots, y_n\} \backslash Y$. Besitzt $\langle F \rangle_\partial$ eine endliche differentielle σ-Gröbnerbasis, so endet die Prozedur* `DiffGB`*, angewandt auf F, mit der Ausgabe einer solchen.*

Beweis. Es genügt zu zeigen, dass die reduzierte differentielle σ-Gröbnerbasis G von $\langle F \rangle_\partial$ die in Satz 2.5.19 angegebene Gestalt besitzt. Zunächst umfasst G nach Satz 2.4.6 genau $N = n - \dim(D/\langle F \rangle_\partial) = n - |Y|$ Polynome, deren Leitterme Derivate paarweise verschiedener differentieller Unbestimmter $y_{i_1}, \ldots, y_{i_N} \in \{y_1, \ldots, y_n\} \backslash Y$ sind. Sei nun $g \in G$ beliebig und $\mathrm{LT}_\sigma(g^{(k)}) = tu^k$ für ein $t \in \mathbb{T}^n$ und ein $u \in \mathbb{D}^n$. Da σ eine Eliminationsordnung für $\{y_1, \ldots, y_n\} \backslash Y$ ist, gibt es wegen $\langle F \rangle_\partial \cap K\{Y\} = \emptyset$ ein Derivat $y^{(l)} \in \mathbb{D}(\mathrm{LT}_\sigma(g))$ mit $y \in \{y_{i_1}, \ldots, y_{i_N}\}$. Dies ist insbesondere für u der Fall, da σ nach Voraussetzung ∂-lexikographisch ist. □

Abschließend wollen wir uns noch mit einer anderen Art von Elimination beschäftigen. Für ein differentielles Ideal $I \subseteq D$ und für ein $k \geq 0$ ist es oftmals interessant, das algebraische Ideal $I_k = I \cap D_k$ zu betrachten, also die Menge aller Polynome in I, deren Ordnung k nicht übersteigt. Dies lässt sich auch als Elimination aller Derivate mit Ordnung echt größer als k verstehen. Wählen wir nun statt einer differentiellen Eliminationsordnung eine stabile, ordnungskompatible, differentielle Termordnung, so erhalten wir das folgende Resultat.

Satz 3.1.6. *Sei $I \subseteq D$ ein differentielles Ideal, σ eine stabile, ordnungskompatible, differentielle Termordnung auf $\mathbb{T}^n$ und $G \subseteq D \backslash \{0\}$ eine differentielle σ-Gröbnerbasis von I. Dann ist $G_k = \{g^{(l)} \mid g \in G, l \geq 0\} \cap D_k$ für jedes $k \in \mathbb{N}$ eine σ_k-Gröbnerbasis von I_k, wobei σ_k die von σ induzierte Termordnung auf $\mathbb{T}^n_k = \mathbb{T}^n \cap D_k$ ist.*

Beweis. Ist $f \in I_k$ ein von Null verschiedenes Polynom, so existiert nach Voraussetzung ein $g \in G$, so dass der Leitterm von f bzgl. σ für ein $l \geq 0$ ein Vielfaches von $\mathrm{LT}_\sigma(g^{(l)})$ ist. Wegen der Ordnungskompatibilität von σ gilt dabei

$$\mathrm{ord}(g^{(l)}) = \mathrm{ord}(\mathrm{LT}_\sigma(g^{(l)})) \leq \mathrm{ord}(\mathrm{LT}_\sigma(f)) = \mathrm{ord}(f),$$

also insbesondere $g^{(l)} \in G_k$. □

Damit lässt sich nun für jedes $k \geq 0$ und jedes null-dimensionale Ideal $I \subseteq D$, das für eine strikt stabile differentielle Termordnung σ auf $\mathbb{T}^n$ eine endliche differentielle σ-Gröbnerbasis besitzt, das zugehörige Ideal $I_k = I \cap D_k$ berechnen. Denn für jede strikt stabile, ordnungskompatible, differentielle Termordnung existiert nach Korollar 2.4.9 eine endliche differentielle Gröbnerbasis von I, wonach mit Satz 2.5.18 die Prozedur `DiffGB` terminiert.

3.2 Differentielle Algebrenhomomorphismen

Der differentielle Polynomring $K\{y_1, \dots, y_n\}$ ist, genauer betrachtet, mehr als ein differentieller Ring. Er erfüllt zusätzlich die Bedingungen einer K-Algebra, womit wir bei dem Begriff der *differentiellen K-Algebra* angelangt sind. Diesen wollen wir genauer studieren, wobei wir uns auf endlich erzeugte differentielle K-Algebren beschränken, da sich diese wieder als differentielle Faktorringe von $K\{y_1, \dots, y_n\}$ auffassen lassen. Konzentrieren werden wir uns dabei auf die Berechnung des Kerns von Homomorphismen zwischen solchen Algebren. Eine Anwendung stellt in diesem Zusammenhang die Bestimmung der differentiellen Relationen zwischen Polynomen $f_1, \dots, f_n \in K[x_1, \dots, x_m]$ dar.

In diesem Abschnitt bezeichne wieder $D = K\{y_1, \dots, y_n\}$ den differentiellen Polynomring und σ eine differentielle Termordnung auf $\mathbb{T}^n$.

Definition 3.2.1. Seien (R, ∂) und (A, δ) differentielle Ringe.

1) Der Ring A heißt *differentielle R-Algebra*, falls A eine R-Algebra mit $\delta|_R = \partial$ ist.
2) Eine differentielle R-Algebra A heißt *endlich erzeugt*, falls Elemente $a_1, \dots, a_n \in A$ existieren, so dass sich jedes $a \in A$ schreiben lässt als $a = \sum_{i=1}^n \sum_{k\in\mathbb{N}_0} r_{ik}\delta^k a_i$, wobei nur endlich viele $r_{ik} \in R$ von Null verschieden sind. In diesem Fall schreiben wir $A = R\{a_1, \dots, a_n\}$.

Für eine differentielle R-Algebra unterscheiden wir im Folgenden nicht zwischen der Derivation der R-Algebra und der des zugrunde liegenden Rings.

Definition 3.2.2. Sei R ein differentieller Ring und seien (A_1, ∂_1), (A_2, ∂_2) differentielle R-Algebren. Ein R-Algebrenhomomorphismus $\psi : A_1 \longrightarrow A_2$ heißt *differentieller R-Algebrenhomomorphismus*, falls $\psi(\partial_1 a) = \partial_2(\psi(a))$ für alle $a \in A_1$ gilt.

Wie gewohnt existiert zu jeder endlich erzeugten differentiellen R-Algebra A ein differentielles Ideal $I \subseteq R\{y_1, \dots, y_n\}$ für ein $n \in \mathbb{N}$, so dass A und $R\{y_1, \dots, y_n\}/I$ als differentielle R-Algebren isomorph sind. Ist $A = R\{a_1, \dots, a_n\}$ für gewisse Elemente $a_1, \dots, a_n \in A$, so erfüllt der Kern des differentiellen R-Algebrenhomomorphismus $R\{y_1, \dots, y_n\} \longrightarrow A$, $y_i \mapsto a_i$ das Gewünschte. Hierzu verweisen wir auf die universelle Eigenschaft von differentiellen Polynomringen.

Satz 3.2.3. *Sei R ein differentieller Ring und A eine differentielle R-Algebra. Weiter seien $n \geq 1$ und $a_1, \dots, a_n \in A$. Dann existiert genau ein differentieller R-Algebrenhomomorphismus $\psi : R\{y_1, \dots, y_n\} \longrightarrow A$ mit $\psi|_R = id|_R$ und $\psi(y_i) = a_i$ für $i = 1, \dots, n$.*

Beweis. Für ein Polynom $f = \sum_{i=0}^d c_i(y_1^{(k_i)})^i$ mit $c_0, \dots, c_d \in R$ und $k_0, \dots, k_d \in \mathbb{N}_0$ setzen wir $\psi(f) = \sum_{i=0}^d c_i(a_1^{(k_i)})^i$. Dies definiert offensichtlich auf eindeutige Weise einen differentiellen R-Algebrenhomomorphismus, der die obigen Bedingungen erfüllt. Die Behauptung folgt nun induktiv. $\square$

Da jeder differentielle Algebrenhomomorphismus insbesondere ein differentieller Ringhomomorphismus ist, ist dessen Kern stets ein differentielles Ideal. Wir wollen nun den Kern eines differentiellen Algebrenhomomorphismus explizit bestimmen. Dazu betrachten wir zunächst den Spezialfall des Einsetzhomomorphismus.

Satz 3.2.4. *Sei R ein differentieller Ring und $R\{y_1, \ldots, y_n\}$ der differentielle Polynomring in $y_1, \ldots, y_n$ über R. Weiter seien $f_1, \ldots, f_n \in R$ und $\psi : R\{y_1, \ldots, y_n\} \longrightarrow R$ der durch $\psi(y_i) = f_i$ für $i = 1, \ldots, n$ definierte differentielle R-Algebrenhomomorphismus. Dann ist das differentielle Ideal $\langle y_1 - f_1, \ldots, y_n - f_n\rangle_\partial \subseteq R\{y_1, \ldots, y_n\}$ der Kern von ψ.*

Beweis. Für das Ideal $I = \langle y_1 - f_1, \ldots, y_n - f_n\rangle_\partial$ gilt offensichtlich $I \subseteq \ker(\psi)$. Sei nun umgekehrt $g \in \ker(\psi)$. Wir betrachten den differentiellen R-Algebrenhomomorphismus $\varphi : R\{y_1, \ldots, y_n\} \longrightarrow R\{y_1, \ldots, y_n\}$ mit $\varphi(y_i) = y_i + f_i$ für $i = 1, \ldots, n$. Als Bild von g erhalten wir $\varphi(g) = g(y_1+f_1, \ldots, y_n+f_n) = h+r$ für ein $r \in R$ und ein $h \in R\{y_1, \ldots, y_n\}$ mit $h(0, \ldots, 0) = 0$. Also gilt $r = g(f_1, \ldots, f_n) = 0$. Mit dem zu φ inversen differentiellen R-Algebrenhomomorphismus $\widetilde{\varphi} : R\{y_1, \ldots, y_n\} \longrightarrow R\{y_1, \ldots, y_n\}$ mit $\widetilde{\varphi}(y_i) = y_i - f_i$ für $i = 1, \ldots, n$ ergibt sich schließlich $g = \widetilde{\varphi}(\varphi(g)) = \widetilde{\varphi}(h) = h(y_1 - f_1, \ldots, y_n - f_n) \in I$. □

Wir sind nun in der Lage, alle differentiellen Relationen zwischen Polynomen aus $K[x_1, \ldots, x_m]$ zu bestimmen. Die Menge aller solcher Relationen bildet offensichtlich ein differentielles Ideal, welches gerade der Kern eines geeigneten Einsetzhomomorphismus ist. Dazu betrachten wir den Polynomring als differentiellen Ring mit Derivation ∂, wobei wir $\partial x_i = 1$ für $i = 1, \ldots, m$ setzen.

Korollar 3.2.5. *Seien $f_1, \ldots, f_n \in K[x_1, \ldots, x_m]$ und $\psi : D \longrightarrow K[x_1, \ldots, x_m]$ der durch $\psi(y_i) = f_i$ für $i = 1, \ldots, n$ definierte differentielle K-Algebrenhomomorphismus. Weiter sei $\mathbb{D} = \{y_i^{(k_i)} \mid i = 1, \ldots, n,\ 0 \le k_i \le \deg(f_i)\} \cup \{x_1, \ldots, x_m\}$, σ eine differentielle Termordnung auf $\mathbb{T}^n$ und τ eine Eliminationsordnung auf $\mathbb{T}(\mathbb{D})$ für $\{x_1, \ldots, x_m\}$, so dass die Einschränkungen von σ und τ auf $\mathbb{T}(\mathbb{D}\backslash\{x_1, \ldots, x_m\})$ identisch sind. Ist G eine τ-Gröbnerbasis des Ideals*

$$\langle y_i^{(k_i)} - f_i^{(k_i)} \mid i = 1, \ldots, n, 0 \le k_i \le \deg(f_i)\rangle \subseteq K[\mathbb{D}],$$

so ist $\widetilde{G} = G \cap K[\mathbb{D}\backslash\{x_1, \ldots, x_m\}]$ eine differentielle σ-Gröbnerbasis von $\ker(\psi)$.

Beweis. Ist $I = \langle y_1 - f_1, \ldots, y_n - f_n\rangle_\partial \subseteq K[x_1, \ldots, x_m]\{y_1, \ldots, y_n\}$, so folgt mit obigem Satz für $R = K[x_1, \ldots, x_m]$ gerade $\ker(\psi) = I \cap D$. Wegen $\partial^k f_i = 0$ für $k > \deg(f_i)$ lässt sich I schreiben als

$$\begin{aligned} I &= \langle \partial^k(y_i - f_i) \mid i = 1, \ldots, n, k \in \mathbb{N}_0\rangle \\ &= \langle y_i^{(k_i)} - f_i^{(k_i)} \mid i = 1, \ldots, n, 0 \le k_i \le \deg(f_i)\rangle + \langle y_1^{(\deg(f_1)+1)}, \ldots, y_n^{(\deg(f_n)+1)}\rangle_\partial. \end{aligned}$$

Ist nun G eine τ-Gröbnerbasis von $\langle y_i^{(k_i)} - f_i^{(k_i)} \mid i = 1, \ldots, n, 0 \le k_i \le \deg(f_i)\rangle$, so erhalten wir mit $G \cup \{y_i^{(k_i)} \mid i = 1, \ldots, n, k_i > \deg(f_i)\}$ eine τ-Gröbnerbasis von I. Da τ

eine Eliminationsordnung für $\{x_1, \ldots, x_m\}$ ist und die Derivate $y_1^{(\deg(f_1))}, \ldots, y_n^{(\deg(f_n))}$ als Leitterme von Polynomen aus G bzgl. τ auftreten, ist die Menge $G \cap D$ eine differentielle σ-Gröbnerbasis von $\ker(\psi)$. $\square$

Durch eine differentielle Interreduktion der Menge $\widetilde{G}$ lässt sich zusätzlich die reduzierte differentielle σ-Gröbnerbasis des Kerns angeben, die insbesondere endlich ist.

Beispiel 3.2.6. Wir betrachten die Neilsche Parabel in $\mathbb{R}^2$, also die Menge der Punkte $\{(t^2, t^3) \mid t \in \mathbb{R}\}$. Wir wollen nun alle differentiellen Relationen finden, die die Parabel beschreiben. Für den differentiellen Polynomring $\mathbb{R}\{y_1, y_2\}$ wählen wir die ordnungskompatible differentielle Termordnung $\tau\mathtt{Lex}$ mit $y_1 >_\tau y_2$ und entsprechend die Termordnung $\mathtt{Lex}$ mit $t > y_1^{(k)} > y_2^{(k)}$ für alle $k \geq 0$ auf dem Monoid der Terme in $\mathbb{R}[t, y_1, y_1^{(1)}, y_1^{(2)}, y_2, y_2^{(1)}, y_2^{(2)}, y_2^{(3)}]$. Als reduzierte $\mathtt{Lex}$-Gröbnerbasis des Ideals

$$I = \langle y_1 - t^2, y_1^{(1)} - 2t, y_1^{(2)} - 2, y_2 - t^3, y_2^{(1)} - 3t^2, y_2^{(2)} - 6t, y_2^{(3)} - 6\rangle$$

von $\mathbb{R}[t, y_1, y_1^{(1)}, y_1^{(2)}, y_2, y_2^{(1)}, y_2^{(2)}, y_2^{(3)}]$ erhalten wir dann

$$\begin{aligned} G = \{&y_1^3 - y_2^2, y_2^{(1)} - 3y_1, y_1^{(1)}y_2 - 2y_1^2, y_1y_1^{(1)} - 2y_2, (y_1^{(1)})^2 - 4y_1, \\ &y_2^{(2)} - 3y_1^{(1)}, y_1^{(2)} - 2, y_2^{(3)} - 6, t - \tfrac{1}{2}y_1^{(1)}\} \end{aligned}$$

und nach Interreduktion schließlich

$$\widetilde{G} = \{y_1^3 - y_2^2, y_2^{(1)} - 3y_1, y_1^{(1)}y_2 - 2y_1^2, y_1y_1^{(1)} - 2y_2, (y_1^{(1)})^2 - 4y_1\}$$

als reduzierte differentielle $\tau\mathtt{Lex}$-Gröbnerbasis des Ideals aller differentiellen Relationen zwischen t^2 und t^3. Insbesondere umfasst dieses Ideal die algebraische Relation $y_1^3 - y_2^2$.

Über den Kern eines differentiellen Homomorphismus zwischen beliebigen differentiellen K-Algebren kann die folgende Aussage getroffen werden.

Satz 3.2.7. *Seien $D_1 = K\{y_1, \ldots, y_n\}$, $D_2 = K\{z_1, \ldots, z_m\}$ differentielle Polynomringe über K und $I_1 \subseteq D_1$, $I_2 \subseteq D_2$ differentielle Ideale. Seien weiter $f_1, \ldots, f_n \in D_2$ und $\varphi : D_1/I_1 \longrightarrow D_2/I_2$ der durch $\varphi(y_i + I_1) = f_i + I_2$ für $i = 1, \ldots, n$ definierte differentielle K-Algebrenhomomorphismus. Ist J das von $\{y_1 - f_1, \ldots, y_n - f_n\}$ und I_2 erzeugte differentielle Ideal von $K\{y_1, \ldots, y_n, z_1, \ldots, z_m\}$, so ist der Kern von φ das Bild von $J \cap D_1$ in D_1/I_1.*

Beweis. Die Derivationen von D_1 und D_2 induzieren eine Derivation des differentiellen Polynomrings $K\{y_1, \ldots, y_n, z_1, \ldots, z_m\}$. Nach Satz 3.2.4 mit $R = K\{z_1, \ldots, z_m\}$ ist $\langle y_1 - f_1, \ldots, y_n - f_n\rangle_\partial \subseteq J$ der Kern des differentiellen K-Algebrenhomomorphismus $\psi : K\{y_1, \ldots, y_n, z_1, \ldots, z_m\} \longrightarrow D_2$ mit $\psi(y_i) = f_i$ für $i = 1, \ldots, n$. Für ein Polynom $f \in D$ mit $f + I_1 \in \ker(\varphi)$ ist dann $f(f_1, \ldots, f_n) \in I_2$ und $f - f(f_1, \ldots, f_n)$ ein Element von $\ker(\psi) \subseteq J$, also $f \in J \cap D_1$.

Umgekehrt gilt für jedes Polynom $f \in J \cap D_1$ offensichtlich $\psi(f) \in I_2$ und damit $\varphi(f + I_1) = f(f_1, \ldots, f_n) + I_2 = \psi(f) + I_2 = I_2$. $\square$

3.3 Systeme differentieller Relationen

In diesem Abschnitt wollen wir differentielle Gleichungssysteme $\mathcal{S}$ der Form

$$\begin{aligned} f_1(y_1,\dots,y_n) &= 0 \\ &\vdots \\ f_s(y_1,\dots,y_n) &= 0 \end{aligned}$$

mit $f_1,\dots,f_s \in D\backslash\{0\}$ studieren. Dabei gilt unser Interesse der Menge aller Lösungen eines solchen Systems in K^n. In [14], Kapitel 3.7 wird für algebraische Gleichungssysteme dargestellt, wie bei Existenz von nur endlich vielen Lösungen diese bestimmt bzw. beschrieben werden können. Diese Erkenntnisse können wir auch auf unsere Situation anwenden, denn jede Nullstelle von $f_1,\dots,f_s$ ist Nullstelle von $\langle f_1,\dots,f_s\rangle_\partial$ und damit auch von $\langle f_1,\dots,f_s\rangle_\partial \cap D_0$. Es bleibt lediglich zu entscheiden, wann ein System eine endliche Lösungsmenge besitzt. Aber dies ist gerade dann der Fall, wenn das differentielle Ideal $\langle f_1,\dots,f_s\rangle_\partial$ null-dimensional ist und Ordnung Null besitzt.

Nach dem differentiellen Nullstellensatz besitzen $I = \langle f_1,\dots,f_s\rangle_\partial$ und sein Radikal $\sqrt{I}$ die gleiche Nullstellenmenge. Zudem haben beide die gleiche Ordnung und die zugehörigen Faktorringe die gleiche Dimension. Für die Untersuchung des Systems $\mathcal{S}$ hinsichtlich der Existenz von nur endlich vielen Lösungen können wir I also als das Verschwindungsideal einer Punktmenge $\mathbb{X} \subseteq K^n$ annehmen.

Satz 3.3.1. *Sei $\mathbb{X} = \{p_1,\dots,p_s\} \subset K^n$ eine endliche Menge von Punkten.*

a) Das Verschwindungsideal $\mathcal{I}(\mathbb{X}) \subseteq D$ von $\mathbb{X}$ ist null-dimensional.
b) Es gilt $\operatorname{ord}(\mathcal{I}(\mathbb{X})) = 0$.
c) Für jede stabile differentielle Termordnung σ auf $\mathbb{T}^n$ besitzt $\mathcal{I}(\mathbb{X})$ eine endliche differentielle σ-Gröbnerbasis.

Beweis. Wie in Bemerkung 1.3.2 gesehen, gilt $\mathcal{I}(\mathbb{X}) \cap K[y_i] \neq \{0\}$ für $i = 1,\dots,n$, falls $\mathbb{X}$ eine endliche Punktmenge ist. Also ist das Ideal $\mathcal{I}(\mathbb{X})$ insbesondere null-dimensional.

Weiter sei $f_i \in \mathcal{I}(\mathbb{X}) \cap K[y_i]$ für $i = 1,\dots,n$ ein von Null verschiedenes Polynom und $\mathfrak{p} \subseteq D$ ein differentielles Primideal, welches in der Primidealzerlegung von $\mathcal{I}(\mathbb{X})$ vorkommt. Ist τ ein ordentliches Ranking auf $\mathbb{D}^n$ und $G \subseteq D$ eine reduzierte differentielle τ-Pseudo-Gröbnerbasis von $\mathfrak{p}$, so pseudo-reduziert jedes f_i nach Satz 1.6.4 bzgl. G zu Null. Wegen $\operatorname{ord}(f_i) = 0$ für $i = 1,\dots,n$ existieren also Polynome $g_1,\dots,g_n \in G$, so dass $\mathrm{LD}_\tau(g_i) = y_i$ und damit $\operatorname{ord}(g_i) = 0$ für $i = 1,\dots,n$ gilt. Da G höchstens n Elemente umfasst, folgt $G \subseteq K[y_1,\dots,y_n]$, d.h das Ideal $\mathfrak{p}$ besitzt die Ordnung Null und daher auch $\mathcal{I}(\mathbb{X})$.

Für Aussage c) genügt es nach Satz 2.4.7 zu zeigen, dass für $i = 1,\dots,n$ eine Zahl $k_i \in \mathbb{N}_0$ existiert, so dass $y_i^{(k_i)}$ im Leittermideal von $\mathcal{I}(\mathbb{X})$ liegt. Dazu schreiben wir $p_i = (p_{i1},\dots,p_{in})$ mit $p_{i1},\dots,p_{in} \in K$ für $i = 1,\dots,s$ und betrachten für ein festes $i \in \{1,\dots,n\}$ die Vektoren $v_j = (p_{1i}^{(j-1)},\dots,p_{si}^{(j-1)}) \in K^s$ für $j = 1,\dots,s+1$. Sei nun

$r \in \{1, \ldots, s+1\}$ minimal mit der Eigenschaft, dass $v_1, \ldots, v_r$ über K linear abhängig sind. Dann existieren $\lambda_1, \ldots, \lambda_{r-1} \in K$, so dass die Gleichung $v_r - \sum_{j=1}^{r-1} \lambda_j v_j = 0$ erfüllt ist. Damit ist das Polynom $g_i = y_i^{(r)} - \sum_{j=1}^{r-1} \lambda_j y_i^{(j)}$ ein Element von $\mathcal{I}(\mathbb{X})$ mit $\mathrm{LT}_\sigma(g_i) = y_i^{(r)}$. □

Ist das differentielle Ideal $\langle f_1, \ldots, f_s \rangle_\partial$ nicht null-dimensional oder besitzt es eine von Null verschiedene Ordnung, so existieren also unendlich viele Lösungen des zugehörigen Systems $\mathcal{S}$. Beides können wir mit den Ergebnissen aus Abschnitt 1.8 nachprüfen.

Der folgende Satz stellt nun zusätzlich einen Zusammenhang zu dem algebraischen Ideal $\langle f_1, \ldots, f_s \rangle_\partial \cap D_0$ her, der den Schlüssel zur eigentlichen Berechnung der Lösungsmenge liefert.

Satz 3.3.2. *Sei $\mathbb{X} \subseteq K^n$ eine Menge von Punkten. Dann sind die folgenden Aussagen äquivalent:*

a) Die Menge $\mathbb{X}$ ist endlich.
b) Das algebraische Ideal $\mathcal{I}(\mathbb{X})_i \subseteq D_i$ ist für jedes $i \in \mathbb{N}_0$ null-dimensional.
c) Das Ideal $\mathcal{I}(\mathbb{X})$ ist null-dimensional und besitzt Ordnung Null.
d) Es ist $D_i/\mathcal{I}(\mathbb{X})_i$ für jedes $i \in \mathbb{N}_0$ ein endlich-dimensionaler K-Vektorraum.
e) Es ist $D/\mathcal{I}(\mathbb{X})$ ein endlich-dimensionaler K-Vektorraum.

Beweis. Für die Äquivalenz von a), b) und d) verweisen wir auf [14], Proposition 3.7.1. Weiter folgt c) aus a) nach obigem Satz, und c) impliziert wiederum b), da mit $\mathcal{I}(\mathbb{X})$ insbesondere $\mathcal{I}(\mathbb{X})_0$ null-dimensional ist.

Da auch d) offensichtlich aus e) folgt, genügt es, die Implikation c) $\Rightarrow$ e) zu zeigen. Dazu betrachten wir die Nicht-Leitterme von $\mathcal{I}(\mathbb{X})$ bzgl. einer strikt stabilen differentiellen Termordnung σ auf $\mathbb{T}^n$, da deren Restklassen nach Macaulays Basissatz eine Basis des K-Vektorraums $D/\mathcal{I}(\mathbb{X})$ bilden. Da $\mathcal{I}(\mathbb{X})$ null-dimensional und damit $\mathbb{X}$ endlich ist, besitzt $\mathcal{I}(\mathbb{X})$ nach obigem Satz eine endliche differentielle σ-Gröbnerbasis. Dies impliziert $y_i^{(k_i)} \in \mathrm{LT}_\sigma(\mathcal{I}(\mathbb{X}))$ nach Satz 2.4.6 für $i = 1, \ldots, n$ und gewisse $k_1, \ldots, k_n \in \mathbb{N}_0$. Also sind alle Nicht-Leitterme Elemente von D_k mit $k = \max\{k_1, \ldots, k_n\}$. Da der Vektorraum $D_k/\mathcal{I}(\mathbb{X})_k$ nach d) aber endliche Dimension hat, kann es auch nur endlich viele solcher Nicht-Leitterme geben. □

Besitzt das System $\mathcal{S}$ endlich viele Lösungen, so ist die Nullstellenmenge des algebraischen Ideals $I_0 = \langle f_1, \ldots, f_s \rangle_\partial \cap D_0$ also ebenfalls endlich. Letzteres können wir nun mit Satz 3.1.6 bestimmen. Dazu wählen wir eine strikt stabile ordnungskompatible differentielle Termordnung σ auf $\mathbb{T}^n$ und berechnen mit der Prozedur `DiffGB` eine zugehörige differentielle σ-Gröbnerbasis G. Die Prozedur terminiert dabei, da das differentielle Ideal $\langle f_1, \ldots, f_s \rangle_\partial$ null-dimensional ist und nach Satz 3.3.1 eine endliche differentielle σ-Gröbnerbasis besitzt. Dann ist $G_0 = G \cap D_0$ eine Gröbnerbasis des Ideal I_0 und wir können mit [14], Korollar 3.7.26 alle Lösungen des algebraischen Systems $\mathcal{S}_0$, bestehend aus den Gleichungen $g(y_1, \ldots, y_n) = 0$ mit $g \in G_0$, bestimmen. Diejenigen Lösungen, die auch $\mathcal{S}$ erfüllen, bilden schließlich die Lösungsmenge von $\mathcal{S}$.

3.4 Der differentielle Buchberger-Möller-Algorithmus

In diesem Abschnitt wollen wir uns mit einer weiteren klassischen Anwendung der Gröbnerbasistheorie befassen. Dabei handelt es sich um die Frage, wie das Verschwindungsideal einer Punktemenge $\mathbb{X} = \{p_1, \ldots, p_s\} \subset K^n$ bestimmt werden kann, also gerade die Umkehrung der Problemstellung des vorherigen Abschnitts. Eine Antwort darauf liefert der sogenannte Buchberger-Möller-Algorithmus. Wie in [4] beschrieben, berechnet dieser mit Mitteln der linearen Algebra eine Gröbnerbasis des zugehörigen Verschwindungsideals in $K[x_1, \ldots, x_n]$.

Wir wollen nun die beschriebenen Überlegungen auf den differentiellen Fall übertragen und eine entsprechende Version des Algorithmus formulieren. Es sei daran erinnert, dass zu jeder Koordinate eines Punktes p_i auch deren Derivationen unter ∂ definiert sind. Gesucht ist nun das Verschwindungsideal $\mathcal{I}(\mathbb{X})$ von $\mathbb{X}$, wobei hier für jedes Element $f \in \mathcal{I}(\mathbb{X})$ auch $f^{(k)}(p_i) = 0$ gilt für alle $k \geq 0$ und $i = 1, \ldots, s$.

Schließlich befassen wir uns noch mit der Frage, wie das Ideal $\mathcal{I}(\mathbb{X})$ berechnet werden kann, falls für jeden Punkt $p_i \in \mathbb{X}$ nur die Werte $p_i^{(0)}, \ldots, p_i^{(N)}$ für ein $N \in \mathbb{N}_0$ bekannt sind. Diese Fragestellung tritt zum Beispiel auf, wenn die differentiellen Unbestimmten reelle Funktionen in einer Unbestimmten darstellen, deren Funktionswerte nur bis zur Ordnung N bestimmt werden können.

In diesem Abschnitt sei wieder $D = K\{y_1, \ldots, y_n\}$ der differentielle Polynomring und σ eine differentielle Termordnung auf $\mathbb{T}^n$. Weiter sei $s \geq 1$ und $\mathbb{X} = \{p_1, \ldots, p_s\} \subset K^n$ eine Menge von Punkten.

In Abschnitt 1.3 haben wir bereits gesehen, dass das Verschwindungsideal $\mathcal{I}(\mathbb{X})$ ein differentielles Radikalideal ist. Ferner besitzt dieses nach Satz 3.3.1 für jede stabile differentielle Termordnung eine endliche differentielle Gröbnerbasis. Eine solche liefert nun der folgende Algorithmus.

Satz 3.4.1 (Differentieller Buchberger-Möller-Algorithmus).
Sei $\mathbb{X} = \{p_1, \ldots, p_s\} \subset K^n$ und σ eine stabile differentielle Termordnung auf $\mathbb{T}^n$. Wir betrachten die folgenden Instruktionen:

1) *Setze $O = \{1\}$, $t_1 = 1$, $G = \emptyset$, $r = 1$ und $v_1 = (1, \ldots, 1) \in K^s$.*
2) *Gilt $\mathbb{T}^n \backslash O = \{t\, \mathrm{LT}_\sigma(g^{(k)}) \mid t \in \mathbb{T}^n, g \in G, k \in \mathbb{N}_0\}$, so gib (G, O) aus und stoppe. Ansonsten sei t_{r+1} der bzgl. σ kleinste Term in $\mathbb{T}^n \backslash O$, der nicht in der Menge $\{t\, \mathrm{LT}_\sigma(g^{(k)}) \mid t \in \mathbb{T}^n, g \in G, k \in \mathbb{N}_0\}$ enthalten ist.*
3) *Bestimme $v_{r+1} = (t_{r+1}(p_1), \ldots, t_{r+1}(p_s)) \in K^s$ und prüfe $v_1, \ldots, v_{r+1}$ auf lineare Unabhängigkeit. Sind die Vektoren linear abhängig, so füge $g = t_{r+1} - c_1 t_1 - \cdots - c_r t_r$ zu G hinzu, wobei $v_{r+1} = c_1 v_1 + \cdots + c_r v_r$ mit $c_1, \ldots, c_r \in K$, und fahre mit 2) fort.*
4) *Füge den Term t_{r+1} zu O hinzu, ersetze r durch $r + 1$ und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten ein Paar (G, O) ausgibt, wobei G eine endliche differentielle σ-Gröbnerbasis von $\mathcal{I}(\mathbb{X})$ ist und die Restklassen der Elemente von O eine Basis des K-Vektorraums $D/\mathcal{I}(\mathbb{X})$ bilden.

Beweis. Wir beweisen zunächst, dass der Algorithmus terminiert. Dafür ist zu zeigen, dass die Schritte 3) und 4) nur endlich oft ausgeführt werden. Für Schritt 4) ist dies offensichtlich der Fall, denn es können maximal s Vektoren linear unabhängig sein. Es bleibt noch zu zeigen, dass die Menge G nur endlich oft vergrößert wird. O.B.d.A. sei dazu y_1 die bzgl. σ kleinste differentielle Unbestimmte. Angenommen, $y_1^{(s)}$ ist zu keinem Zeitpunkt ein Element der Menge $T = \{t\,\mathrm{LT}_\sigma(g^{(k)}) \mid t \in \mathbb{T}^n, g \in G, k \in \mathbb{N}_0\}$. Dies würde bedeuten, dass $y_1^{(s)}$ und damit auch die Derivate $y_2^{(s)}, \ldots, y_n^{(s)}$ nie in Schritt 2) ausgewählt werden, da dann bereits $1, y_1, \ldots, y_1^{(s-1)}$ in O lägen. Also sind alle Terme, die in Schritt 3) betrachtet werden, Elemente von D_{s-1}. In $\mathbb{T}_{s-1}$ gilt aber Dicksons Lemma, d.h. die Menge $\mathrm{LT}_\sigma\{G\}$ kann nur endlich oft vergrößert und damit nur endlich oft ein Polynom zu G hinzugefügt werden, womit wir einen Widerspruch erhalten. Analog folgt $y_i^{(s)} \in T$ auch für jedes $i \in \{2, \ldots, n\}$. Damit ist G zu jedem Zeitpunkt eine Teilmenge von D_s, kann also nur endlich oft vergrößert werden.

Für den Beweis der Korrektheit des Algorithmus nehmen wir an, dass es ein Polynom $f \in \mathcal{I}(\mathbb{X})\backslash\{0\}$ gibt, welches bzgl. G nicht zu Null reduziert. Wegen $G \subseteq \mathcal{I}(\mathbb{X})$ dürfen wir zunächst f als bzgl. G reduziert voraussetzen. Dann wird jeder Term $t \in \mathrm{Supp}(f)$ im Laufe des Algorithmus zu O hinzugefügt. Die zugehörigen Vektoren $(t(p_1), \ldots, t(p_s))$ sind damit linear unabhängig im Widerspruch zu $(f(p_1), \ldots, f(p_s)) = (0, \ldots, 0)$.

Schließlich bildet die Menge der Restklassen der Elemente in O offensichtlich eine Basis von $D/\mathcal{I}(\mathbb{X})$, denn jeder Term, der nicht Element von T ist, wird in Schritt 4) des Algorithmus zu O hinzugefügt. □

Es ist noch zu erwähnen, dass in dem Algorithmus nicht beschrieben wird, auf welche Weise in Schritt 2) die Mengengleichheit $\mathbb{T}^n = \{t\,\mathrm{LT}_\sigma(g^{(k)}) \mid t \in \mathbb{T}^n, g \in G, k \in \mathbb{N}_0\} \cup O$ überprüft und der als nächstes zu betrachtende Term t_{r+1} ermittelt wird. Wir wollen daher eine neue Version des differentiellen Buchberger-Möller-Algorithmus angeben, in der wir aus Effizienzgründen zudem mehrere Terme gleichzeitig abarbeiten. Dabei bezeichne wie gewohnt $\mathbb{T}_i^n$ für jedes $i \in \mathbb{N}_0$ die Menge aller Terme der Ordnung i, wobei wir zusätzlich $\mathbb{T}_{-1}^n = \emptyset$ setzen.

Satz 3.4.2. *Sei $\mathbb{X} = \{p_1, \ldots, p_s\} \subset K^n$ und σ eine strikt stabile ordnungskompatible differentielle Termordnung auf $\mathbb{T}^n$, die auf $\mathbb{T}_i^n \backslash \mathbb{T}_{i-1}^n$ für jedes $i \in \mathbb{N}_0$ gradkompatibel ist. Wir betrachten die folgenden Instruktionen:*

1) *Setze $O = \{1\}$, $g_1 = 1$, $Q = \{g_1\}$, $G = \emptyset$ und $r = 1$. Weiter sei $i = 0$, $d = 1$ und $\mathcal{M} = (1, \ldots, 1) \in \mathrm{Mat}_{1,s}(K)$.*
2) *Sei $\mathcal{T} = \{t_1, \ldots, t_l\} \subseteq \mathbb{T}_i^n \backslash \mathbb{T}_{i-1}^n$ die Menge aller Terme vom Grad d, die nicht in $\{t\,\mathrm{LT}_\sigma(g^{(k)}) \mid t \in \mathbb{T}^n, g \in G, k \in \mathbb{N}_0\}$ enthalten sind. Gilt $\mathcal{T} = \emptyset$ und $d = 1$, so gib (G, O) aus und stoppe. Gilt $\mathcal{T} = \emptyset$ und $d > 1$, so ersetze i durch $i + 1$, d durch 1 und fahre mit 2) fort.*
3) *Forme die Matrix*

$$\mathcal{A} = \begin{pmatrix} \mathcal{M} \\ (t_j(p_k))_{\substack{j=1,\ldots,l \\ k=1,\ldots,s}} \end{pmatrix}$$

mit $t_1 <_\sigma t_2 <_\sigma \cdots <_\sigma t_l$ *und bestimme eine Matrix* $\mathcal{C} = (c_{ij}) \in \mathrm{Mat}_{r+l}(K)$ *mit*

$$\begin{pmatrix} \mathcal{M} \\ (b_j)_{j=1,\ldots,l} \end{pmatrix} = \mathcal{CA},$$

so dass für $j = 1, \ldots, l$ *der erste von Null verschiedene Eintrag* b_{jk} *von* b_j *gleich Eins und zugleich der einzige von Null verschiedene Eintrag der* k*-ten Spalte von* $\mathcal{CA}$ *ist.*

4) *Berechne* $g_j = t_j - \sum_{k=1}^{r+j-1} c_{jk} g_k$ *für aufsteigendes* $j = 1, \ldots, l$. *Gilt* $b_j = (0, \ldots, 0)$, *so füge das Polynom* g_j *zu* G *hinzu. Andernfalls füge* $g_{r+1} = g_j$ *zu* Q, *den Term* t_j *zu* O *sowie* b_j *zu* $\mathcal{M}$ *hinzu und ersetze* r *durch* $r + 1$.
5) *Ersetze* d *durch* $d + 1$ *und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten ein Paar (G, O) *ausgibt, wobei* G *eine endliche differentielle* σ*-Gröbnerbasis von* $\mathcal{I}(\mathbb{X})$ *ist und die Restklassen der Elemente von* O *eine Basis des* K*-Vektorraums* $D/\mathcal{I}(\mathbb{X})$ *bilden.*

Beweis. Der Algorithmus terminiert aus denselben Gründen wie der differentielle Buchberger-Möller-Algorithmus, denn auch hier werden die verbliebenen Terme aufsteigend bzgl. σ abgearbeitet. Gilt dabei zu einem Zeitpunkt $\mathcal{T} = \emptyset$, so ist jeder Term in $\mathbb{T}_i^n$ vom Grad d bereits Element der Menge $\{t\,\mathrm{LT}_\sigma(g^{(k)}) \mid t \in \mathbb{T}^n, g \in G, k \in \mathbb{N}_0\}$. Da jeder Term in $\mathbb{T}_i^n$ höheren Grades Vielfaches eines Terms in $\mathbb{T}_i^n$ vom Grad d ist, gilt dies also auch für alle übrigen Terme der Ordnung i und es kann mit der Betrachtung der Terme in $\mathbb{T}_{i+1}^n$ fortgefahren werden. Gilt schließlich $\mathcal{T} = \emptyset$ und $d = 1$, so ist jeder Term der Ordnung größer oder gleich i Vielfaches des Terms $\mathrm{LT}_\sigma(g^{(k)})$ für ein $g \in G$ und ein $k \geq 0$. Auch die Korrektheit des Algorithmus folgt analog zu Satz 3.4.1. □

Der Algorithmus berechnet zunächst das algebraische Verschwindungsideal $\mathcal{I}(\mathbb{X})_0$. Für $i \geq 1$ werden dann die zusätzlichen differentiellen Relationen der Punkte bestimmt. Zudem erhalten wir eine differentielle Gröbnerbasis mit Elementen möglichst kleiner Ordnung.

Bemerkung 3.4.3. Die Vorgehensweise bei der Wahl der als nächstes zu betrachtenden Terme kann je nach Bedarf auch angepasst werden.

a) Ist eine differentielle Gröbnerbasis aus gradkleinen Polynomen gesucht, so wählen wir eine strikt stabile gradkompatible differentielle Termordnung, die auf der Menge aller Terme eines Grades ordnungskompatibel ist. Zudem ist der zweite Schritt derart abzuändern, dass der Algorithmus stoppt, sobald $\mathcal{T} = \emptyset$ und $i = 0$ gilt, oder im Fall $i > 0$ den Grad d erhöht. Entsprechend wird in Schritt 5) die Ordnung i durch $i + 1$ ersetzt.
b) Alternativ kann auch eine strikt stabile differentielle Termordnung σ verwendet werden, die kompatibel mit der Abbildung $\omega : \mathbb{T}^n \longrightarrow \mathbb{N}_0$, $\omega(t) = \deg(t) + w(t)$ ist. In diesem Fall umfasst $\mathcal{T}$ in Schritt 2) jeweils diejenigen Terme, für die ω den gleichen Wert liefert. Der Algorithmus stoppt dann genau an dem Zeitpunkt, an dem $\mathcal{T}$ in Schritt 2) als leere Menge initialisiert wird.

Im verbleibenden Teil dieses Abschnitts wollen wir uns mit der Situation beschäftigen, dass die differentiellen Unbestimmten $y_1, \dots, y_n$ Funktionen in einer zusätzlichen Unbestimmten x sind. Mit Hilfe einer solchen Betrachtungsweise lassen sich viele Anwendungsprobleme beschreiben. Eine differentielle Unbestimmte y_i kann zum Beispiel einer physikalischen Größe wie Druck oder Temperatur entsprechen, die wiederum von der Zeit abhängen kann. Das Derivat $y_i^{(1)}$ steht dann offensichtlich für die zeitliche Veränderung der Messgröße.

Im Folgenden betrachten wir also unendlich oft differenzierbare Funktionen $\varphi_1, \dots, \varphi_n$ mit $\varphi_i : K \longrightarrow K$ für $i = 1, \dots, n$, die nicht explizit gegeben sind, sondern deren Funktionswerte für feste Werte $x_1, \dots, x_s \in K$ bekannt sind. Darüber hinaus seien auch die Werte für deren Ableitungen bis zu einer gewissen Ordnung verfügbar, d.h. es gibt eine Zahl $N \in \mathbb{N}_0$, so dass für $i = 1, \dots, n$ und $j = 1, \dots, s$ die Werte $\varphi_i^{(k)}(x_j)$ für $0 \le k \le N$ gegeben sind.

Wir suchen nun wieder nach allen differentiellen Relationen zwischen $\varphi_1, \dots, \varphi_n$, also nach allen Polynomen $f \in D$, für die die Einsetzung $y_i^{(k)} \mapsto \varphi_i^{(k)}$ für alle $k \ge 0$ und $i = 1, \dots, n$ Null ergibt. Wir notieren die Menge dieser Polynome im Folgenden mit $\mathcal{I}(\varphi_1, \dots, \varphi_n)$. Für die Berechnung von $\mathcal{I}(\varphi_1, \dots, \varphi_n)$ haben wir aber lediglich die Funktionswerte an den Stellen $x_1, \dots, x_s$ zur Verfügung. Ein erster Ansatz ist nun die Bestimmung des zugehörigen algebraischen Verschwindungsideals im Polynomring $K[\, y_i^{(k)} \mid i = 1, \dots, n, 0 \le k \le N]$. Damit ergeben sich aber auch Polynome, deren Derivationen keine Relationen liefern, also Polynome, die mit Sicherheit nicht zu $\mathcal{I}(\varphi_1, \dots, \varphi_n)$ gehören. Demnach wäre es vernünftig, zusätzliche Bedingungen an die gesuchten Polynome zu stellen. So müssten also für jedes f auch deren Derivationen $f^{(k)}$ im algebraischen Verschwindungsideal liegen. Diese Idee wurde bereits in [17] verfolgt. Marinari, Möller und Mora geben dazu einen verallgemeinerten Buchberger-Möller-Algorithmus an, der für ein durch Funktionale bestimmtes Verschwindungsideal eine Gröbnerbasis berechnet.

In unserer Situation ergeben sich hierbei zunächst zwei weitere Probleme. Zum einen haben wir für jedes $i \in \{1, \dots, n\}$ nur Informationen über die ersten N Derivationen von φ_i, und zum anderen sind die Werte $\partial(\varphi_i^{(k)}(x_j))$ und $\varphi_i^{(k+1)}(x_j)$ im Allgemeinen verschieden. Daher verwenden wir im Weiteren die Einsetzhomomorphismen $\psi_1, \dots, \psi_s$ mit

$$\begin{aligned} \psi_j : D &\longrightarrow K \\ y_i^{(k)} &\longmapsto \begin{cases} \varphi_i^{(k)}(x_j) & \text{, falls } k \le N \\ 0 & \text{, falls } k > N \end{cases} \end{aligned}$$

für $i = 1, \dots, n$ und $j = 1, \dots, s$ bzw. den K-Algebrenhomomorphismus

$$\begin{aligned} \psi : D &\longrightarrow K^s \\ f &\longmapsto (\psi_1(f), \dots, \psi_s(f)). \end{aligned}$$

Es bleibt jetzt lediglich noch die Frage zu beantworten, wie Derivate der Ordnung echt größer als N behandelt werden sollen. Hierfür gibt es zunächst mehrere Ansätze.

Eine erste Möglichkeit besteht darin, die Werte der Funktionen $\varphi_1, \ldots, \varphi_n$ als verschwindend klein anzunehmen. Diese Annahme würde zur Berechnung des differentiellen Ideals $\ker(\psi)$ führen. Jedoch muss ein Polynom $f \in \mathcal{I}(\varphi_1, \ldots, \varphi_n)$ nicht notwendigerweise in $\ker(\psi)$ liegen. Dies ist Folge der zusätzlichen Bedingung $\varphi_i(f^{(k)}) = 0$ für $k > N - \operatorname{ord}(f)$.

Einen möglichen Ausweg könnte nun die Beschränkung unserer Forderung an $f^{(k)}$ auf alle $k \in \mathbb{N}_0$, für die $\operatorname{ord}(f^{(k)}) \leq N$ gilt, liefern. Leider bildet die Menge

$$\{f \in D_N \mid f^{(k)} \in \ker(\psi) \text{ für alle } k \geq 0 \text{ mit } \operatorname{ord}(f^{(k)}) \leq N\}$$

dieser Polynome kein Ideal von D_N. Denn für zwei solcher Polynome in $D_N \backslash D_{N-1}$ kann deren Summe in $D_{N-1} \backslash \ker(\psi \circ \partial)$ liegen.

Daher verbleibt nur der mit den Überlegungen in [17] konforme Ansatz, die Polynommenge

$$\begin{aligned} I_m &= \{f \in D_m \mid f^{(k)} \in \ker(\psi) \text{ für } 0 \leq k \leq N - m\} \\ &= \ker(\psi) \cap \ker(\psi \circ \partial) \cap \cdots \cap \ker(\psi \circ \partial^{N-m}) \cap D_m \end{aligned}$$

für ein $m \in \mathbb{N}_0$ mit $m \leq N$ zu berechnen. Dabei entspricht I_N gerade dem algebraischen Verschwindungsideal der Punkte $p_1, \ldots, p_s \in K^{n(N+1)}$ in D_N, wobei wir

$$p_j = (\varphi_1^{(0)}(x_j), \ldots, \varphi_1^{(N)}(x_j), \ldots, \varphi_n^{(0)}(x_j), \ldots, \varphi_n^{(N)}(x_j))$$

für $j = 1, \ldots, s$ setzen. Letzteres bezeichnen wir im Folgenden mit $\mathcal{I}(\{p_1, \ldots, p_s\})$.

Die verschiedenen Verschwindungsideale hängen nun wie folgt zusammen.

Satz 3.4.4. *Sei $m \in \mathbb{N}_0$ mit $m \leq N$.*

a) Es ist I_m ein Ideal von D_m.
b) Ist $m < N$, so gilt $I_m \subseteq I_{m+1} \cap D_m$.
c) Es gilt $\mathcal{I}(\varphi_1, \ldots, \varphi_n) \cap D_m \subseteq I_m \subseteq \mathcal{I}(\{p_1, \ldots, p_s\}) \cap D_m$.

Beweis. Die Aussage b) folgt direkt aus der Definition der Menge I_m und c) aus der Tatsache, dass für jedes $f \in \mathcal{I}(\varphi_1, \ldots, \varphi_n) \cap D_m$ und jedes $k \geq 0$ das Polynom $f^{(k)}$ ein Element des Kerns von ψ ist.

Es bleibt noch a) zu zeigen. Wir betrachten dazu Polynome $f, g \in I_m$. Wegen der Additivität von ψ und ∂^k für $k = 0, \ldots, N - m$ gilt dann auch $f + g \in I_m$. Des Weiteren ergibt sich für jedes $h \in D_m$ aus $\psi_j(\partial^k(hf)) = \sum_{i=0}^{k} \psi_j(h^{(i)})\psi_j(f^{(k-i)})$ für $j = 1, \ldots, s$ schließlich $hf \in I_m$. □

Eine geeignete Anpassung des üblichen Buchberger-Möller-Algorithmus ermöglicht nun die Berechnung des Ideals I_m für $0 \leq m \leq N$. Dazu betrachten wir für einen Term $t \in \mathbb{T}_m^n$ anstatt des Auswertungsvektors $\psi(t)$ den Vektor $(\psi(t), \psi(t^{(1)}), \ldots, \psi(t^{N-m)}))$, um genau die Polynome in $\mathcal{I}(\{p_1, \ldots, p_s\})$ zu finden, die auch den zusätzlichen derivativen Bedingungen genügen.

Satz 3.4.5. *Sei $m \in \mathbb{N}_0$ mit $m \leq N$ und σ eine Termordnung auf $\mathbb{T}^n_m$. Wir betrachten die folgenden Instruktionen:*

1) *Setze $O = \{1\}$, $t_1 = 1$, $G = \emptyset$, $r = 1$ und $v_1 = (v_{11}, \ldots, v_{1,(N-m+1)s}) \in K^{(N-m+1)s}$ mit $v_{1i} = 1$ für $i = 1, \ldots, s$ und $v_{1j} = 0$ für $j = s+1, \ldots, (N-m+1)s$.*
2) *Bestimme den bzgl. σ kleinsten Term t_{r+1} in $\mathbb{T}^n_m \backslash \{t\,\mathrm{LT}_\sigma(g) \mid t \in \mathbb{T}^n_m, g \in G\}$. Existiert solch ein Term nicht, so gib (G, O) aus und stoppe.*
3) *Bestimme $v_{r+1} = (\psi(t^{(k)}_{r+1}))_{k=0,\ldots,N-m} \in K^{(N-m+1)s}$ und prüfe $v_1, \ldots, v_{r+1}$ auf lineare Unabhängigkeit. Sind die Vektoren linear abhängig, so füge das Polynom $g = t_{r+1} - c_1 t_1 - \cdots - c_r t_r$ zu G hinzu, wobei $v_{r+1} = c_1 v_1 + \cdots + c_r v_r$ ist mit $c_1, \ldots, c_r \in K$, und fahre mit 2) fort.*
4) *Füge den Term t_{r+1} zu O hinzu, ersetze r durch $r+1$ und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten ein Paar (G, O) ausgibt, wobei G eine σ-Gröbnerbasis von I_m ist und die Restklassen der Elemente von O eine Basis des K-Vektorraums D_m/I_m bilden.

Beweis. Der Algorithmus terminiert, da es in $K^{(N-m+1)s}$ höchstens $(N-m+1)s$ linear unabhängige Vektoren geben kann und zu G nur endlich viele Polynome hinzugefügt werden können. Letzteres folgt aus der Tatsache, dass die Menge $\mathrm{LT}_\sigma\{G\}$ wegen Dicksons Lemma im Verlauf des Algorithmus nur endlich oft erweitert werden kann.

Für den Beweis der Korrektheit sei $f \in I_m \backslash \{0\}$. Es ist f algebraisch reduzibel bzgl. G, denn die Vektoren $(\psi(t^{(0)}), \ldots, \psi(t^{(N-m)}))$ mit $t \in \mathrm{Supp}(f)$ sind offensichtlich linear abhängig. Damit ist G eine σ-Gröbnerbasis von I_m und O eine K-Basis von D_m/I_m. □

Für $m = N$ berechnet der obige Algorithmus gerade das algebraische Verschwindungsideal $\mathcal{I}(\{p_1, \ldots, p_s\}) \subseteq D_N$. Zudem geht aus dem Beweis hervor, dass die Dimension des K-Vektorraums D_m/I_m stets kleiner oder gleich $(N-m+1)s$ ist. In praxisnahen Beispielen gilt hierbei zumeist die Gleichheit, im Allgemeinen jedoch nicht.

Wie für den differentiellen Buchberger-Möller-Algorithmus können wir auch hier eine Modifikation vornehmen, so dass in einem Schritt mehrere Terme zugleich bearbeitet werden. Dabei liegt es nahe, schrittweise alle Terme eines Grades zu betrachten. Notwendigerweise müssen wir uns dazu auf gradkompatible Termordnungen beschränken.

Korollar 3.4.6. *Sei $m \in \mathbb{N}_0$ mit $m \leq N$ und σ eine gradkompatible Termordnung auf $\mathbb{T}^n_m$. Wir betrachten die folgenden Instruktionen:*

1) *Setze $O = \{1\}$, $g_1 = 1$, $Q = \{g_1\}$, $G = \emptyset$ und $r = 1$. Weiter sei $d = 1$ und $\mathcal{M} = (1, \ldots, 1) \in \mathrm{Mat}_{1,(N-m+1)s}(K)$.*
2) *Sei $\mathcal{T} = \{t_1, \ldots, t_l\} \subseteq \mathbb{T}^n_m$ die Menge aller Terme vom Grad d, die nicht in $\{t\,\mathrm{LT}_\sigma(g) \mid t \in \mathbb{T}^n_m,\ g \in G\}$ enthalten sind. Gilt $\mathcal{T} = \emptyset$, so gib (G, O) aus und stoppe.*
3) *Forme die Matrix*

$$\mathcal{A} = \begin{pmatrix} \mathcal{M} \\ (\psi(t^{(k)}_j))_{\substack{j=1,\ldots,l \\ k=0,\ldots,N-m}} \end{pmatrix}$$

mit $t_1 <_\sigma t_2 <_\sigma \cdots <_\sigma t_l$ und bestimme eine Matrix $\mathcal{C} = (c_{ij}) \in \mathrm{Mat}_{r+l}(K)$ mit

$$\begin{pmatrix} \mathcal{M} \\ (b_j)_{j=1,\dots,l} \end{pmatrix} = \mathcal{C}\mathcal{A},$$

so dass für $j = 1, \dots, l$ der erste von Null verschiedene Eintrag b_{jk} von b_j gleich Eins und zugleich der einzige von Null verschiedene Eintrag der k-ten Spalte von $\mathcal{C}\mathcal{A}$ ist.

4) *Berechne $g_j = t_j - \sum_{k=1}^{r+j-1} c_{jk} g_k$ für aufsteigendes $j = 1, \dots, l$. Gilt $b_j = (0, \dots, 0)$, so füge das Polynom g_j zu G hinzu. Andernfalls füge $g_{r+1} = g_j$ zu Q, den Term t_j zu O sowie b_j zu $\mathcal{M}$ hinzu und ersetze r durch $r + 1$.*
5) *Ersetze d durch $d + 1$ und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten ein Paar (G, O) ausgibt, wobei G eine σ-Gröbnerbasis von I_m ist und die Restklassen der Elemente von O eine Basis des K-Vektorraums D_m/I_m bilden.

Beweis. Das Terminieren und die Korrektheit des Algorithmus folgen wie im Beweis zu Satz 3.4.5. □

Beispiel 3.4.7.

a) Wir betrachten die Funktionen $\varphi_1 : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ und $\varphi_2 : \mathbb{R} \to \mathbb{R}, x \mapsto x^3$ aus Beispiel 3.2.6, deren Funktionswerte an den Stellen $x_1 = 0$, $x_2 = 1$ und $x_3 = -1$ bis zur Ordnung 2 vorliegen. Wir wählen $m = 1$ und verwenden für $\mathbb{R}[y_1, y_1^{(1)}, y_2, y_2^{(1)}]$ wieder die Termordnung `Lex` mit $y_1^{(1)} > y_2^{(1)} > y_1 > y_2$. Wenden wir nun den Algorithmus aus Satz 3.4.5 an, so ergeben sich für die Terme $1, y_2, y_2^2, y_2^3, y_2^4$ die linear unabhängigen Vektoren

$$\begin{aligned} v_1 &= (1, 1, 1, 0, 0, 0) \\ v_2 &= (0, 1, -1, 0, 3, 3) \\ v_3 &= (0, 1, 1, 0, 6, -6) \\ v_4 &= (0, 1, -1, 0, 9, 9) \\ v_5 &= (0, 1, 1, 0, 12, -12) \end{aligned}$$

Für y_2^5 liegt der zugehörige Vektor $v = (0, 1, -1, 0, 15, 15)$ in $\langle v_1, \dots, v_5 \rangle_\mathbb{R}$, genauer gilt $v = -v_2 + 2v_4$. Also ist $y_2^5 - 2y_2^3 + y_2$ das erste Element von G. Auf die gleiche Weise finden wir auch die übrigen Polynome und erhalten für G die Menge

$$\{y_2^5 - 2y_2^3 + y_2, y_2^{(1)} + 2y_2^4 - 5y_2^2, y_1 + \tfrac{2}{3}y_2^4 - \tfrac{5}{3}y_2^2,$$
$$y_1^{(1)}y_2 + \tfrac{2}{3}y_2^4 - \tfrac{8}{3}y_2^2, (y_1^{(1)})^2 + \tfrac{8}{3}y_2^4 - \tfrac{20}{3}y_2^2\}$$

Jedes Polynom in $\mathcal{I}(\varphi_1, \varphi_2) \cap \mathbb{R}[y_1, y_1^{(1)}, y_2, y_2^{(1)}]$ reduziert nun bzgl. G zu Null. Zudem ist $\langle G \rangle$ eine echte Teilmenge des algebraischen Verschwindungsideals

$$\langle y_2^3 - y_2, y_1 - y_2^2, y_2^{(1)} - 3y_2^2, y_1^{(1)} - 2y_2 \rangle.$$

b) Wir suchen nun alle differentiellen Relationen der Sinus- und Cosinusfunktion bis zur Ordnung Eins. Dazu seien die Werte beider Funktionen an den Stellen $x_1 = 0$, $x_2 = \frac{\pi}{2}, x_3 = \pi$ und $x_4 = \frac{3\pi}{2}$ bis zur zweiten Ordnung gegeben. Wir wollen nun Korollar 3.4.6 mit $m = 1$ anwenden und wählen daher die Termordnung `DegLex` mit $y_2^{(1)} > y_1^{(1)} > y_2 > y_1$. Im Schritt $d = 1$ betrachten wir nun die Terme $y_1, y_2, y_1^{(1)}, y_2^{(1)}$ und die Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 0 & 1 & -1 & 0 & 1 & 0 \end{pmatrix}$$

mit Zeilenstufenform

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 0 & 0 & -2 & -2 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Da sich zwei Nullzeilen ergeben, werden die zugehörigen Polynome $y_1^{(1)} - y_2$ und $y_2^{(1)} + y_1$ zu G hinzugefügt. Zudem wird die Menge Q um y_1 und $y_2 + y_1 - 1$ erweitert. Für $d = 2$ und die Terme $y_1^2, y_1 y_2, y_2^2$ erhalten wir nach Zeilenumformungen die Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 0 & 0 & -2 & -2 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Es sind also $y_1^2 - y_1$ und $y_1 y_2$ neue Elemente von Q bzw. $y_2^2 + y_1^2 - 1$ von G. Im Fall $d = 3$ müssen dann die Terme y_1^3 und $y_1^2 y_2$ untersucht werden. Dabei ergeben sich aber keine Nullzeilen. Erst für $d = 4$ und die Terme $y_1^4, y_1^3 y_2$ ist dies wieder der Fall und die zugehörige Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 0 & 0 & -2 & -2 & 1 & -1 & -1 & 1 \\ 0 & 0 & 0 & 2 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$$

führt zu den aktualisierten Mengen

$$G = \{y_1^{(1)} - y_2, y_2^{(1)} + y_1, y_2^2 + y_1^2 - 1, y_1^4 - y_1^2\}$$

bzw.

$$Q = \{y_1, y_2 + y_1 - 1, y_1^2 - y_1, y_1y_2, y_1^3 + y_1y_2 - y_1, \\ y_1^2y_2 - y_1^3 - y_1y_2 + y_1, y_1^3y_2 - y_1^2y_2\}.$$

Da keine Terme höheren Grades existieren, die nicht Vielfache von $y_1^{(1)}, y_2^{(1)}, y_2^2, y_1^4$ sind, endet der Algorithmus mit der Ausgabe von G. Wieder erhalten wir ein genaueres Ergebnis als der übliche Buchberger-Möller-Algorithmus, der die Menge

$$\{y_1^{(1)} - y_2, y_2^{(1)} + y_1, y_1y_2, y_2^2 + y_1^2 - 1, y_1^3 - y_1\}$$

berechnen würde.

3.5 Approximative Methoden

Zum Abschluss wollen wir noch einmal die Problematik am Ende des vorherigen Abschnitts aufgreifen, um einen kurzen Einblick in ein relativ neues Gebiet der Mathematik zu geben, der *Approximativen Algebra* oder *Numerischen Algebra*. Die Leitfrage dabei ist, inwieweit sich die Algorithmen aus der kommutativen Algebra auf reale Messdaten anwenden lassen, d.h. auf Daten, deren Genauigkeit im Allgemeinen nicht garantiert ist. Dies beinhaltet die Anpassung existierender und die Entwicklung neuer Algorithmen, um eine nötige numerische Stabilität zu gewährleisten. Ein aktuelles Forschungsthema ist z.B. die Entwicklung einer approximativen Version des Buchberger-Möller-Algorithmus zur Bestimmung des *approximativen Verschwindungsideals* einer Menge von Punkten, deren Koordinaten aus Messdaten bestehen. Gesucht sind hierbei Polynome, die an den exakten Punkten verschwinden. Da diese jedoch nur „ungefähr“ bekannt sind, ist es nahe liegend, unter diesen Voraussetzungen auch Polynome zu bestimmen, die nur „ungefähr“ an den Messpunkten verschwinden.

In [6] und [10] finden sich hierzu zwei Lösungsansätze. Beide formulieren einen *approximativen Buchberger-Möller-Algorithmus*, der jeweils wie der ursprüngliche Algorithmus vorgeht. Sie verwenden jedoch unterschiedliche numerische Methoden, um zu entscheiden, ob ein Term ein neues Element des gesuchten approximativen Verschwindungsideals liefert. In [6] wird dazu ein Least Squares Problem gelöst, in [10] die Singulärwertzerlegung einer geeigneten Matrix berechnet.

Auch in unserer Situation ist eine Approximation von Interesse. Liegen die Werte der Funktionen $\varphi_i^{(k)}$ an den Stellen $x_1, \ldots, x_s$ nur ungenau vor, so führt die Berechnung des Ideals I_m nicht zu dem gewünschten Ergebnis. Denn das Ideal beschreibt die Polynome, deren Derivationen bis zur Ordnung $N - m$ exakt an den gegebenen Punkten verschwinden, und enthält daher keine Informationen über die exakten Punkte. Wünschenswert wäre es, einfache Relationen zu finden, die die geforderten Bedingungen beinahe erfüllen, z.B. Polynome mit möglichst kleinem Grad.

Zur Bestimmung einer geeigneten Approximation der Ideale $I_0, \ldots, I_N$ werden wir sowohl den Ansatz in [6] als auch den in [10] verfolgen. Dazu betrachten wir im Folgenden den differentiellen Polynomring $D = \mathbb{R}\{y_1, \ldots, y_n\}$ in n differentiellen Unbestimmten über dem Körper der reellen Zahlen. Dabei bezeichne $\|f\|$ für jedes Polynom $f \in D$ die euklidische Norm des Koeffizientenvektors von f und $\|\mathcal{A}\|_F$ die Frobeniusnorm der Matrix $\mathcal{A} \in \mathrm{Mat}_{m,l}(\mathbb{R})$. Des Weiteren betrachten wir wieder Funktionen $\varphi_1, \ldots, \varphi_n$ mit $\varphi_i : \mathbb{R} \longrightarrow \mathbb{R}$, deren Funktionswerte in $x_1, \ldots, x_s \in \mathbb{R}$ bis zur Ordnung $N \in \mathbb{N}_0$ bekannt sind. Diese notieren wir erneut mit $p_1, \ldots, p_s$, wobei wir nach geeigneter Skalierung annehmen dürfen, dass $p_1, \ldots, p_s \in [-1, 1]^{(N+1)n}$ gilt. Analog verwenden wir die Algebrenhomomorphismen $\psi_1, \ldots, \psi_s$ bzw. ψ. Zusätzlich sei noch die Abbildung $\Psi_{N-m} : D \longrightarrow \mathbb{R}^{(N-m+1)s}, f \mapsto (\psi(f^{(k)}))_{k=0,\ldots,N-m}$ definiert.

Der zentrale Schritt beim Buchberger-Möller-Algorithmus ist die Überprüfung der linearen Abhängigkeit von Vektoren, die den Auswertungen von Termen in den gegebenen Punkten entspricht. In unserem Fall testen wir, ob der Vektor $v_{r+1} = (\psi(t_r^{(k)}))_{k=0,\ldots,N-m}$ aus Satz 3.4.5 ein Element des $\mathbb{R}$-Vektorraums $\langle v_1, \ldots, v_r \rangle_{\mathbb{R}}$ ist. Dies ist der Punkt, in dem nun numerische Methoden zum Einsatz kommen. In [6] findet sich dazu eine Definition der „numerischen" Vektorraumzugehörigkeit. Ein Vektor v_{r+1} liegt demnach numerisch in $V = \langle v_1, \ldots, v_r \rangle_{\mathbb{R}}$, wenn für die zu V orthogonale Komponente v von v_{r+1} die Bedingung $\| v \|_2 < \varepsilon \cdot \| v_{r+1} \|_2$ für ein festes $\varepsilon \in \mathbb{R}_+$ erfüllt ist. Wir müssen mit dieser Überlegung also überprüfen, ob $\| v_{r+1} - (v_1, \ldots, v_r)\, \overline{x} \|_2 < \varepsilon \cdot \| v_{r+1} \|_2$ für eine Lösung $\overline{x}$ des Least Squares Problems $(v_1, \ldots, v_r)x = v_{r+1}$ gilt. Für die Berechnung der Lösungen eines Least Squares Problems $\mathcal{A}x = b$ verweisen wir auf den folgenden Satz aus der Numerik.

Satz 3.5.1. *Sei $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{R})$ und $b \in \mathbb{R}^m$. Dann existiert eine Lösung $\overline{x} \in \mathbb{R}^n$ der Gleichung*

$$\|b - \mathcal{A}x\|_2 = \min\{\|b - \mathcal{A}y\|_2 \mid y \in \mathbb{R}^n\},$$

und für jede weitere Lösung $\tilde{x} \in \mathbb{R}^n$ gilt $\tilde{x} - \overline{x} \in \{x \in \mathbb{R}^n \mid \mathcal{A}x = 0\}$ und $\mathcal{A}^T\mathcal{A}\tilde{x} = \mathcal{A}^T b$.

Beweis. Siehe [9], Abschnitt 6.1. □

Die oben beschriebene Vorgehensweise im Buchberger-Möller-Algorithmus führt zu der Berechnung eines Ideals, das in [10] als ε-approximatives Verschwindungsideal bezeichnet wird.

Definition 3.5.2. Ein Ideal $I \subseteq D_N$ heißt ein *ε-approximatives Verschwindungsideal* von $\{p_1, \ldots, p_s\}$, falls es ein Erzeugendensystem $G \subseteq D_N$ von I gibt, so dass für jedes $g \in G$ gilt $\|\psi(g)\|_2 < \varepsilon \cdot \|g\|$.

Auf die gleiche Weise lassen sich auch die Ideale I_m mit $0 \leq m \leq N$ approximieren. Unter einer ε-Approximation von I_m verstehen wir dabei ein Ideal $I \subseteq D_m$, welches ein

Erzeugendensystem $G \subseteq D_m$ besitzt mit $\|\psi(g^{(k)})\|_2 < \varepsilon \cdot \|g^{(k)}\|$ für jedes $g \in G$ und jedes $k \in \{0, \dots, N-m\}$. Für die Berechnung eines solchen Ideals gehen wir nun wie oben beschrieben vor.

Satz 3.5.3. *Sei $m \in \mathbb{N}_0$ mit $m \leq N$, σ eine Termordnung auf $\mathbb{T}^n_m$ und $\varepsilon \in \mathbb{R}_+$. Wir betrachten die folgenden Instruktionen:*

1) *Setze $t_1 = 1$, $O = \{1\}$, $G = \emptyset$, $r = 1$ und $v_1 = (v_{11}, \dots, v_{1,(N-m+1)s}) \in \mathbb{R}^{(N-m+1)s}$ mit $v_{1i} = 1$ für $i = 1, \dots, s$ und $v_{1j} = 0$ für $j = s+1, \dots, (N-m+1)s$.*
2) *Bestimme den bzgl. σ kleinsten Term t_{r+1} in $\mathbb{T}^n_m \backslash \{t\,\mathrm{LT}_\sigma(g) \mid t \in \mathbb{T}^n_m, g \in G\}$. Existiert solch ein Term nicht, so gib G aus und stoppe.*
3) *Bestimme $v_{r+1} = (\psi(t^{(k)}_{r+1}))_{k=0,\dots,N-m} \in \mathbb{R}^{(N-m+1)s}$ und eine Lösung $c \in \mathbb{R}^r$ des Least Squares Problems $(v_1, \dots, v_r)\,x = v_{r+1}$. Gilt dabei*
$$\|v_{r+1} - (v_1, \dots, v_r)\,c\|_2 < \varepsilon \cdot \|v_{r+1}\|_2,$$
so füge $g = t_{r+1} - c_1 t_1 - \cdots - c_r t_r$ zu G hinzu und fahre mit 2) fort.
4) *Füge t_{r+1} zu O hinzu, ersetze r durch $r+1$ und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten eine Menge G ausgibt, so dass für jedes $g \in G$ gilt
$$\|\psi(g^{(k)})\|_2 < \varepsilon \sqrt{s \textstyle\sum_{k=0}^{N-m} \deg(\mathrm{LT}_\sigma(g))^k}$$
mit $0 \leq k \leq N-m$.

Beweis. Der Algorithmus terminiert, da zum einen die Anzahl r der Auswertungsvektoren nur endlich oft vergrößert werden kann und zum anderen nach Dicksons Lemma nur endlich viele Polynome zu G hinzugefügt werden können.

Ein Polynom $g \in D_m$ wird insbesondere nur dann in Schritt 3) zu G hinzugefügt, wenn die Bedingung $\|\psi(g^{(k)})\|_2 < \varepsilon \cdot \|\Psi_{N-m}(\mathrm{LT}_\sigma(g))\|_2$ für $k = 0, \dots, N-m$ erfüllt ist. Wegen $p_1, \dots, p_s \in [-1,1]^{(N+1)n}$ gilt dabei zunächst $\|\psi(\partial^k \mathrm{LT}_\sigma(g))\|_2 \leq \sqrt{\deg(\mathrm{LT}_\sigma(g))^k s}$ für $k = 0, \dots, N-m$, d.h. es ist $\|(\psi(\partial^k \mathrm{LT}_\sigma(g)))_{k=0,\dots,N-m}\|_2 \leq \sqrt{s \sum_{k=0}^{N-m} \deg(\mathrm{LT}_\sigma(g))^k}$. Insgesamt ergibt sich daraus die behauptete Abschätzung. □

Der Fehlerabschätzung lässt sich entnehmen, dass die Genauigkeit der Approximation für größere Ordnungen abnimmt und die gradkleinen Polynome die besten Approximationen liefern.

Die Ausgabe des obigen Algorithmus muss im Allgemeinen aber keine Gröbnerbasis sein. Es muss auch nicht jedes Polynom, welches auf den Punkten $p_1, \dots, p_s$ geeignet verschwindet, in $\langle G \rangle$ liegen. Daher stellt sich die Frage, ob es einen Zusammenhang zwischen G und dem Ideal $I_m = I_m(\mathbb{X})$ zu der Punktmenge $\mathbb{X} = \{p_1, \dots, p_s\}$ gibt.

Dazu betrachten wir eine Punktmenge $\widetilde{\mathbb{X}} = \{\tilde{p}_1, \dots, \tilde{p}_s\}$, die in der Nähe von $\mathbb{X}$ liegt, d.h. es gibt ein $\delta \in [0,1]$, so dass $|\tilde{p}_{ij} - p_{ij}| \leq \delta \cdot |\tilde{p}_{ij}|$ für $i = 1, \dots, s$ und $j = 1, \dots, (N+1)n$

gilt. Für das zugehörige Ideal $I_m(\widetilde{X}) \subseteq D_m$ sei dabei O identisch mit $\mathbb{T}^n_m \setminus \mathrm{LT}_\sigma\{I_m(\widetilde{\mathbb{X}})\}$. Zusätzlich nehmen wir an, dass die Dimension des $\mathbb{R}$-Vektorraums $D_m/I_m(\widetilde{X})$ gleich $(N-m+1)s$ ist. Diese Annahme führt nur zu einer unwesentlichen Einschränkung, da für empirische Daten üblicherweise das entsprechende Maximum angenommen wird.

Es lässt sich nun zeigen, dass die Elemente von G Approximationen der Elemente der reduzierten σ-Gröbnerbasis $\widetilde{G}$ von $I_m(\widetilde{X})$ sind, und zwar im folgenden Sinn.

Definition 3.5.4. Sei $T \subseteq \mathbb{T}^n$ eine Menge von Termen und seien $f, \tilde{f} \in D$ Polynome mit $f = \sum_{t\in T} c_t t$ bzw. $\tilde{f} = \sum_{t\in T} \tilde{c}_t t$ und $c_t, \tilde{c}_t \in \mathbb{R}$ für jedes $t \in T$. Für ein $\varepsilon \in \mathbb{R}_+$ heißt $\tilde{f}$ eine ε-Approximation von f, falls

$$\frac{\|f - \tilde{f}\|}{\|f\|} = \frac{\|(c_t - \tilde{c}_t)_{t\in T}\|_2}{\|(c_t)_{t\in T}\|_2} < \varepsilon$$

erfüllt ist.

Folgen wir den Ausführungen in [6], Abschnitt 4, so ergibt sich eine geeignete Zuordnung der Gröbnerbasiselemente. Wir verwenden dabei die den Abbildungen $\psi_1, \ldots, \psi_s, \psi$, und Ψ_{N-m} entsprechenden Abbildungen $\widetilde{\psi}_1, \ldots, \widetilde{\psi}_s, \widetilde{\psi}, \widetilde{\Psi}_{N-m}$ für die Punkte $\tilde{p}_1, \ldots, \tilde{p}_s$ sowie die Matrizen $\mathcal{A}, \widetilde{\mathcal{A}} \in \mathrm{Mat}_{(N-m+1)s}(\mathbb{R})$, deren Spalten gerade den Vektoren $\Psi_{N-m}(t)$ bzw. $\widetilde{\Psi}_{N-m}(t)$ für ein $t \in O$ entsprechen.

Satz 3.5.5. *Zu jedem $\tilde{g} \in \widetilde{G}$ existiert ein Polynom $g \in G$ mit $\mathrm{LT}_\sigma(\tilde{g}) = \mathrm{LT}_\sigma(g)$ und*

$$\frac{\|\tilde{g} - g\|}{\|\tilde{g}\|} < \frac{\kappa(\mathcal{A})}{1 - \varepsilon_2\, \kappa(\mathcal{A})}\,(\varepsilon_1 + \varepsilon_2)$$

mit $\varepsilon_1 = \delta(d_{\max}+1)^{N-m+1}$ und $\varepsilon_2 = \delta\, d_{\max}^{N-m+1}\sqrt{r}$, wobei $\kappa(\mathcal{A})$ die Konditionszahl von $\mathcal{A}$ und $d_{\max}$ der maximale Grad der Terme in $O = \{t_1, \ldots, t_r\}$ ist.

Beweis. Wegen $\mathbb{T}^n_m \setminus \{t\, \mathrm{LT}_\sigma(\tilde{g}) \mid t \in \mathbb{T}^n_m,\ \tilde{g} \in \widetilde{G}\} = \{t_1, \ldots, t_r\}$ gibt es zu jedem $\tilde{g} \in \widetilde{G}$ ein Polynom $g \in G$ mit demselben Leitterm bzgl. σ. Schreiben wir $\tilde{g} = \mathrm{LT}_\sigma(\tilde{g}) + \sum_{i=1}^r \tilde{c}_i t_i$ bzw. $g = \mathrm{LT}_\sigma(g) + \sum_{i=1}^r c_i t_i$ mit $\tilde{c}_1, \ldots, \tilde{c}_r, c_1, \ldots, c_r \in \mathbb{R}$, so gilt

$$\frac{\|\tilde{g} - g\|}{\|\tilde{g}\|} = \frac{\|(1,\tilde{c}) - (1,c)\|_2}{\|(1,\tilde{c})\|_2} < \frac{\|\tilde{c} - c\|_2}{\|\tilde{c}\|_2} \leq \frac{\kappa(\mathcal{A})}{1 - \varepsilon_2\, \kappa(\mathcal{A})}\,(\varepsilon_1 + \varepsilon_2)$$

nach dem allgemeinen Störungssatz für lineare Gleichungssysteme mit

$$\varepsilon_1 = \frac{\|\widetilde{\Psi}_{N-m}(\mathrm{LT}_\sigma(g)) - \Psi_{N-m}(\mathrm{LT}_\sigma(g))\|_2}{\|\widetilde{\Psi}_{N-m}(\mathrm{LT}_\sigma(g))\|_2}, \quad \varepsilon_2 = \frac{\|\widetilde{\mathcal{A}} - \mathcal{A}\|_2}{\|\widetilde{\mathcal{A}}\|_2}.$$

Für eine genauere Betrachtung der Werte ε_1 und ε_2 sei nun $t \in \mathbb{T}^n_N$ und $i \in \{1, \ldots, s\}$. Nach Voraussetzung haben p_{ij} und $\tilde{p}_{ij}$ für $j = 1, \ldots, (N+1)n$ das gleiche Vorzeichen und es gilt $|p_{ij}| \leq |\tilde{p}_{ij}| \cdot (1+\delta)$. Mit einer Fehleranalyse erster Ordnung ergibt sich daher

$$|\widetilde{\psi}_i(t) - \psi_i(t)| \leq |\widetilde{\psi}_i(t)|\, \delta \deg(t)$$

und daraus

$$\begin{aligned}|\widetilde{\psi}_i(\partial^k \operatorname{LT}_\sigma(g)) - \psi_i(\partial^k \operatorname{LT}_\sigma(g))| &\leq \delta \deg(\operatorname{LT}_\sigma(g))^{k+1} \cdot |\widetilde{\psi}_i(\partial^k \operatorname{LT}_\sigma(g))| \\ &\leq \delta\,(d_{\max}+1)^{k+1} \cdot |\widetilde{\psi}_i(\partial^k \operatorname{LT}_\sigma(g))|\end{aligned}$$

für $k = 0, \ldots, N-m$. Wegen

$$\begin{aligned}\|\widetilde{\Psi}_{N-m}(\operatorname{LT}_\sigma(g)) - \Psi_{N-m}(\operatorname{LT}_\sigma(g))\|_2^2 &= \sum_{i=1}^{s}\sum_{k=0}^{N-m} |\widetilde{\psi}_i(\partial^k \operatorname{LT}_\sigma(g)) - \psi_i(\partial^k \operatorname{LT}_\sigma(g))|^2 \\ &\leq \sum_{i=1}^{s}\sum_{k=0}^{N-m} \delta^2\,(d_{\max}+1)^{2(k+1)} \cdot |\widetilde{\psi}_i(\partial^k \operatorname{LT}_\sigma(g))|^2 \\ &\leq \delta^2\,(d_{\max}+1)^{2(N-m+1)} \cdot \|\widetilde{\Psi}_{N-m}(\operatorname{LT}_\sigma(g))\|_2^2\end{aligned}$$

erhalten wir also $\varepsilon_1 \leq \delta(d_{\max}+1)^{N-m+1}$. Ferner gilt für die Frobeniusnorm der Matrix $\widetilde{\mathcal{A}} - \mathcal{A}$ gerade

$$\begin{aligned}\|\widetilde{\mathcal{A}} - \mathcal{A}\|_F^2 &= \sum_{j=1}^{r} \|\widetilde{\Psi}_{N-m}(t_j) - \Psi_{N-m}(t_j)\|_2^2 \\ &\leq \delta^2 \sum_{j=1}^{r} d_{\max}^{2(N-m+1)}\ \|\widetilde{\Psi}_{N-m}(t_j)\|_2^2 \\ &= \delta^2 d_{\max}^{2(N-m+1)}\ \|\widetilde{\mathcal{A}}\|_F^2\ .\end{aligned}$$

Die Äquivalenz der Matrixnormen mit $\|\mathcal{A}\|_2 \leq \|\mathcal{A}\|_F \leq \sqrt{r}\,\|\mathcal{A}\|_2$ impliziert schließlich $\varepsilon_2 \leq \delta\, d_{\max}^{N-m+1}\sqrt{r}$. □

Eine andere numerische Methode zur Überprüfung der Vektorraumzugehörigkeit verwendet die Singulärwertzerlegung von Matrizen. Für genauere Betrachtungen verweisen wir dabei auf [9].

Satz 3.5.6. *Zu jeder Matrix $\mathcal{A} \in \operatorname{Mat}_{m,n}(\mathbb{R})$ gibt es orthogonale Matrizen $\mathcal{U} \in \operatorname{Mat}_m(\mathbb{R})$, $\mathcal{V} \in \operatorname{Mat}_n(\mathbb{R})$ und eine Diagonalmatrix $\mathcal{D} = \operatorname{diag}(s_1, \ldots, s_r, 0, \ldots, 0) \in \operatorname{Mat}_{m,n}(\mathbb{R})$ mit $s_1 \geq s_2 \geq \cdots \geq s_r > 0$, so dass gilt $\mathcal{A} = \mathcal{U}\mathcal{D}\mathcal{V}^T$.*

Beweis. Siehe [9], Theorem 2.3.1. □

Die Zahlen $s_1, \ldots, s_r$ heißen die *Singulärwerte* von $\mathcal{A}$. Sie hängen insbesondere nur von der Matrix $\mathcal{A}$ ab. Für die Singulärwertzerlegung $\mathcal{U}\mathcal{D}\mathcal{V}^T$ gilt insbesondere, dass die Matrizen $\mathcal{D}$ und $\mathcal{A}$ den gleichen Rang haben und die letzten $n - \operatorname{rank}(\mathcal{A})$ Spaltenvektoren von $\mathcal{V}$ eine Orthonormalbasis des Kerns von $\mathcal{A}$ bilden.

Definition 3.5.7. Sei $\mathcal{A} \in \operatorname{Mat}_{m,n}(\mathbb{R})$ eine Matrix mit Singulärwertzerlegung $\mathcal{U}\mathcal{D}\mathcal{V}^T$, $\varepsilon > 0$ und seien $s_1, \ldots, s_k$ diejenigen Singulärwerte von $\mathcal{A}$, die echt größer als ε sind. Ist $\mathcal{D}_\varepsilon = \operatorname{diag}(s_1, \ldots, s_k, 0, \ldots, 0) \in \operatorname{Mat}_{m,n}(\mathbb{R})$, so heißt der Kern der Matrix $\mathcal{A}_\varepsilon = \mathcal{U}\mathcal{D}_\varepsilon\mathcal{V}^T$ der *ε-approximative Kern* von $\mathcal{A}$ und wird mit $\operatorname{apker}(\mathcal{A}, \varepsilon)$ notiert.

Unser ursprüngliches Problem war es zu entscheiden, ob der Vektor v_{r+1} ein Element des $\mathbb{R}$-Vektorraums $\langle v_1, \dots, v_r \rangle_{\mathbb{R}}$ ist. Für jeden Vektor $x \in \mathbb{R}^{r+1}$ im ε-approximativen Kern der Matrix $\mathcal{A} = (v_{r+1}, v_1, \dots, v_r)$ mit $\|x\|_2 \leq 1$ gilt nun

$$\|\mathcal{A}x\|_2 = \|(\mathcal{A} - \mathcal{A}_\varepsilon)x\|_2 \leq \|\mathcal{A} - \mathcal{A}_\varepsilon\|_2 \leq \|\mathcal{D} - \mathcal{D}_\varepsilon\|_2 \leq \varepsilon.$$

Ist die erste Komponente x_1 von x dabei von Null verschieden, so ergibt sich

$$\|v_{r+1} - (v_1, \dots, v_r)\,(-\tfrac{x_2}{x_1}, \dots, -\tfrac{x_{r+1}}{x_1})^T\|_2 \leq \tfrac{1}{|x_1|} \cdot \|\mathcal{A}x\|_2 \leq \tfrac{\varepsilon}{|x_1|}.$$

Genauer gilt das Folgende.

Satz 3.5.8. *Sei $\mathcal{A} \in \mathrm{Mat}_{m,n}(\mathbb{R})$ mit Singulärwertzerlegung $\mathcal{A} = \mathcal{U}\mathcal{D}\mathcal{V}^T$, $\varepsilon > 0$ und seien $s_1, \dots, s_k$ diejenigen Singulärwerte von $\mathcal{A}$, die echt größer als ε sind.*

a) Es gilt $\min\{\|\mathcal{A} - \mathcal{B}\|_2 \mid \mathcal{B} \in \mathrm{Mat}_{m,n}(\mathbb{R}), \mathrm{rank}(\mathcal{B}) \leq k\} = \|\mathcal{A} - \mathcal{U}\mathcal{D}_\varepsilon\mathcal{V}^T\|_2 = s_{k+1}$.

b) Für jede Matrix $\mathcal{B} \in \mathrm{Mat}_{m,n}(\mathbb{R})$ mit $\|\mathcal{A} - \mathcal{B}\|_2 \leq \varepsilon$ ist die Dimension des Kerns von $\mathcal{B}$ kleiner oder gleich $\dim_{\mathbb{R}}(\mathrm{apker}(\mathcal{A}, \varepsilon))$.

c) Die letzten $n-k$ Spaltenvektoren $v_{k+1}, \dots, v_n$ von $\mathcal{V}$ bilden eine Orthonormalbasis von $\mathrm{apker}(\mathcal{A}, \varepsilon)$*, und es gilt $\|\mathcal{A}v_i\|_2 \leq \varepsilon$ für $i = k+1, \dots, n$.*

Beweis. Siehe [10], Korollar 2.2. □

Mit den obigen Überlegungen lässt sich nun eine approximative Version des Algorithmus aus Korollar 3.4.6 angeben. Dabei betrachten wir wieder alle Terme eines Grades simultan und berechnen die Zeilenstufenform der Matrix, deren Zeilenvektoren eine Orthonormalbasis des approximativen Kerns der zugehörigen Auswertungsmatrix bilden. Hierzu verwenden wir eine numerisch stabile Version des Gauss-Algorithmus mit Pivotsuche, wie sie auch in [10], Theorem 3.1 zu finden ist. So kommen u.a. nur diejenigen Einträge als Pivotelemente in Frage, deren Betrag größer als ε' ist, wobei ε' ein zusätzlicher, frei wählbarer Parameter ist. Zudem werden für jedes neu bestimmte Polynom von G nur diejenigen Terme des Trägers berücksichtigt, deren Koeffizient im Betrag größer als ε' ist.

Satz 3.5.9. *Sei $m \in \mathbb{N}_0$ mit $m \leq N$, σ eine gradkompatible Termordnung auf $\mathbb{T}^n_m$ und seien $\varepsilon, \varepsilon' \in \mathbb{R}_+$. Wir betrachten die folgenden Instruktionen:*

1) Setze $g_1 = 1$, $G = \emptyset$, $r = d = 1$ und $\mathcal{M} = (1, \dots, 1) \in \mathrm{Mat}_{(N-m+1)s,1}(\mathbb{R})$.

2) Sei $\mathcal{T} = \{t_1, \dots, t_l\} \subseteq \mathbb{T}^n_m$ die Menge aller Terme vom Grad d, die nicht in $\{t\,\mathrm{LT}_\sigma(g) \mid t \in \mathbb{T}^n_m,\ g \in G\}$ enthalten sind. Gilt $\mathcal{T} = \emptyset$, so gib G aus und stoppe.

3) Forme die Matrix

$$\mathcal{A} = \big((\Psi_{N-m}(t_j))_{j=1,\dots,l} \quad \mathcal{M}\big)$$

mit $t_1 >_\sigma t_2 >_\sigma \cdots >_\sigma t_l$ und bestimme eine Orthonormalbasis $v_1, \dots, v_p$ von $\mathrm{apker}(\mathcal{A}, \varepsilon)$*. Setze $i = j_1 = 1$ und $j_2 = \cdots = j_p = 0$.*

4) Ist $i > p$, so fahre mit 5) fort. Ansonsten fahre wie folgt fort:

i) *Bestimme den Index* $j \in \{i, \dots, p\}$ *mit* $|v_{jj_i}| = \max\{|v_{kj_i}| \mid k = i, \dots, p\}$. *Gilt* $|v_{jj_i}| < \varepsilon'$, *so ersetze* $v_{ij_i}, \dots, v_{pj_i}$ *durch Null, erhöhe* j_i *um Eins und fahre mit 4) fort.*
ii) *Ersetze* v_k *für* $k \in \{1, \dots, p\} \setminus \{j\}$ *durch* $v_k - \frac{v_{kj_i}}{v_{jj_i}} v_j$.
iii) *Ersetze* v_k *durch* $\frac{v_k}{\|v_k\|_2}$ *für jedes* $k \in \{1, \dots, p\}$ *mit* $\|v_k\|_2 > 1$.
iv) *Vertausche* v_i *und* v_j, *setze* $j_{i+1} = j_i + 1$, *ersetze* i *durch* $i+1$ *und fahre mit 4) fort.*

5) *Ersetze* v_{jk} *für* $j = 1, \dots, p$ *und* $k = 1, \dots, l+r$ *durch Null, falls* $|v_{jk}| < \varepsilon'$ *gilt. Für jedes* $j \in \{1, \dots, p\}$ *mit* $v_j \neq (0, \dots, 0)$ *füge das Polynom* $\sum_{k=1}^{l+r} v_{jk} t_k$ *zu* G *hinzu. Ersetze* $\mathcal{M}$ *durch* $\big((\Psi_{N-m}(t_j))_{j \in \mathcal{J}} \;\; \mathcal{M}\big)$ *mit* $\mathcal{J} = \{1, \dots, l\} \setminus \{j_1, \dots, j_p\}$. *Ersetze* r *durch* $r + |\mathcal{J}|$ *und fahre mit 2) fort.*

Dies ist ein Algorithmus, der nach endlich vielen Schritten eine Menge G *ausgibt, so dass für jedes* $g \in G$ *gilt*

$$\|\psi(g^{(k)})\|_2 \leq (\varepsilon + \varepsilon' \deg(g)^k \sqrt{s}\, \dim_{\mathbb{R}}(D_m/I_m)) \cdot \#G$$

mit $0 \leq k \leq N - m$.

Beweis. Für jede Spalte $\Psi_{N-m}(t)$ der Matrix $\mathcal{M}$ gilt $t \in \mathbb{T}^n_m \setminus \mathrm{LT}_\sigma\{I_m\}$. Also sind die Spalten von $\mathcal{M}$ stets linear unabhängig, und es kann $\mathcal{M}$ nur endlich oft vergrößert werden. Nach Dicksons Lemma kann auch G nur endlich oft erweitert werden. Also terminiert der Algorithmus.

Sei nun $g \in G$ und $v_1, \dots, v_p$ die Orthonormalbasis in Schritt 3) für $d = \deg(g)$. Mit Schritt 4) erhalten wir eine Matrix $\mathcal{V} \in \mathrm{Mat}_{p,l+r}(\mathbb{R})$ in Zeilenstufenform, in der der Koeffizientenvektor c von g als Zeilenvektor vorkommt. Ist dabei das Pivotelement in i) im Betrag stets größer oder gleich ε', so ist c ein Element von $\mathrm{apker}(\mathcal{A}, \varepsilon)$, d.h. $c = a_1 v_1 + \cdots + a_p v_p$ für gewisse $a_1, \dots, a_p \in [-1, 1]$ und

$$\|\psi(g^{(k)})\|_2 \leq \|\Psi_{N-m}(g)\|_2 = \|\mathcal{A}c\|_2 \leq \sum_{i=1}^{p} |a_i| \cdot \|\mathcal{A}v_i\|_2 \leq \varepsilon p$$

für $k = 0, \dots, N-m$. Andernfalls weicht der Wert $\|\psi(g^{(k)})\|_2$ für jedes Pivotelement v_{jj_i} mit Betrag kleiner als ε' davon um höchstens $\varepsilon' p \,\|\psi(t_{j_i}^{(k)})\|_2 \leq \varepsilon' p \deg(g)^k \sqrt{s}$ ab. Da Einträge in höchstens so vielen Spalten auf Null gesetzt werden können, wie die Menge $\mathbb{T}^n_m \setminus \mathrm{LT}_\sigma\{I_m\}$ Elemente hat, ergibt sich insgesamt

$$\|\psi(g^{(k)})\|_2 \leq \varepsilon p + \varepsilon' p \deg(g)^k \sqrt{s}\, \dim_{\mathbb{R}}(D_m/I_m).$$

Wegen $p \leq \#G$ folgt daraus die Behauptung. □

Die Güte der Approximation hängt neben den Parametern $\varepsilon, \varepsilon'$ wieder vom Grad der Polynome in G und von der Anzahl der gegebenen Punkte ab. Zudem spielt hier die

Anzahl $\#G$ der gefundenen Polynome eine Rolle, die wiederum von ε und ε' abhängt. Die richtige Wahl der Parameter ist also von entscheidender Bedeutung. Sie sollten insbesondere nicht zu klein gewählt werden, damit sich das Resultat noch vom exakten Ideal I_m der Punkte unterscheidet.

Schließlich erfüllt auch die Ausgabe G des Algorithmus die Bedingung in Satz 3.5.5. D.h. die Polynome in G approximieren die Elemente der reduzierten σ-Gröbnerbasis $\widetilde{G}$ eines Ideals I_m für Punkte, die in der Nähe der gegebenen liegen, wenn die Vektorräume $D_m/\langle G\rangle$ und $D_m/\langle\widetilde{G}\rangle$ übereinstimmen.

Beispiel 3.5.10.

a) Wir betrachten wieder die Funktionen $\varphi_1 : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ und $\varphi_2 : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^3$ aus Beispiel 3.4.7 a). An den Stellen $x_1 = 0$, $x_2 = 1$ und $x_2 = -1$ seien nun die folgenden gestörten Daten gegeben:

	$\varphi_1(x_i)$	$\varphi_2(x_i)$	$\varphi_1^{(1)}(x_i)$	$\varphi_2^{(1)}(x_i)$	$\varphi_1^{(2)}(x_i)$	$\varphi_2^{(2)}(x_i)$
$x_1 = 0$	0,02	0,03	0,03	–0,04	1,95	0,06
$x_2 = 1$	0,97	0,98	1,96	2,94	1,93	5,92
$x_3 = -1$	0,98	–0,96	–2,05	2,93	2,08	5,91

Wir folgen dem Algorithmus aus Satz 3.5.3 mit $\varepsilon = 0,01$. Dabei ergibt sich erst für y_2^5 eine Lösung des zugehörigen Least Squares Problems, die die Bedingung in Schritt 3) erfüllt. Wir erhalten dadurch das Polynom

$$g_1 = y_2^5 - 0,07y_2^4 - 1,879y_2^3 + 0,094y_2^2 + 0,882y_2 - 0,026,$$

dessen Koeffizienten wir hier gerundet angeben. Trotz der Störung der Funktionswerte liegen wir damit nahe der Relation $\tilde{g}_2 = y_2^5 - 2y_2^3 + y_2$ der exakten Punkte, denn es ist $\|g_1 - \tilde{g}_1\| < 0,08 \cdot \|\tilde{g}_1\|$. Für g_1 gilt zudem die in Satz 3.5.3 angegebene Fehlerabschätzung mit

$$\|\psi(g_1)\|_2 < 0,0016 \quad \text{bzw.} \quad \|\psi(g_1^{(1)})\|_2 < 0,035.$$

Als Nächstes ergibt sich

$$g_2 = y_1 + 0,705y^4 - 0,023y_2^3 - 1,679y_2^2 + 0,035y_2 - 0,02$$

als Approximation des Polynoms $\tilde{g}_2 = y_1 + \frac{2}{3}y_2^4 - \frac{5}{3}y_2^2$. Dabei ist $\|\psi(g_2)\|_2 < 0,035$ und $\|\psi(g_2^{(1)})\|_2 < 0,033$. Die Berechnung liefert schließlich noch die Polynome

$$g_3 = y_2^{(1)} + 2,258y_2^4 - 0,088y_2^3 - 5,288y_2^2 + 0,1y_2 + 0,042$$
$$g_4 = y_1^{(1)}y_2 - 0,03y_1^{(1)} + 0,735y_2^4 - 0,03y_2^3 - 2,759y_2^2 + 0,142y_2 - 0,002$$
$$g_5 = (y_1^{(1)})^2 - 0,059y_1^{(1)} + 3,039y_2^4 - 0,174y_2^3 - 7,13y_2^2 + 0,499y_2 - 0,008.$$

Diese approximieren die Polynome $\tilde{g}_3 = y_2^{(1)} + 2y_2^4 - 5y_2^2$, $\tilde{g}_4 = y_1^{(1)} y_2 + \frac{2}{3} y_2^4 - \frac{8}{3} y_2^2$ und $\tilde{g}_5 = (y_1^{(1)})^2 + \frac{8}{3} y_2^4 - \frac{20}{3} y_2^2$.

b) Für die Funktionen $\varphi_1 = \sin$ und $\varphi_2 = \cos$ seien an den Stellen $x_1 = 0$, $x_2 = \frac{\pi}{2}$, $x_3 = \pi$ und $x_4 = \frac{3\pi}{2}$ die folgenden Daten bekannt:

	$\varphi_1(x_i)$	$\varphi_2(x_i)$	$\varphi_1^{(1)}(x_i)$	$\varphi_2^{(1)}(x_i)$	$\varphi_1^{(2)}(x_i)$	$\varphi_2^{(2)}(x_i)$
$x_1 = 0$	0,02	1,03	0,97	0,01	0,03	–0,95
$x_2 = \frac{\pi}{2}$	0,98	0,02	–0,01	–1,04	–1,02	–0,03
$x_3 = \pi$	–0,02	–0,97	–1,05	–0,01	–0,03	0,98
$x_4 = \frac{3\pi}{2}$	–0,97	–0,03	–0,05	1,03	1,02	0,01

Im Vergleich zu Beispiel 3.4.7 b) ergibt sich mit dem Algorithmus aus Satz 3.5.9 mit $\varepsilon = \varepsilon' = 0,1$ das folgende Ergebnis. Für $d = 1$ erhalten wir als Singulärwerte der Matrix

$$\mathcal{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0,02 & 0,98 & -0,02 & -0,97 & 0,97 & -0,01 & -1,05 & -0,05 \\ 1,03 & 0,02 & -0,97 & -0,03 & 0,01 & -1,04 & -0,01 & 1,03 \\ 0,97 & -0,01 & -1,05 & -0,05 & 0,03 & -1,02 & -0,03 & 1,02 \\ 0,01 & -1,04 & -0,01 & 1,03 & -0,95 & -0,03 & 0,98 & 0,01 \end{pmatrix}^T$$

gerade $s_1 = 2,88$, $s_2 = 2,81$, $s_3 = 2$, $s_4 = 0,09$ und $s_5 = 0$, wobei wir wieder gerundete Werte angeben. Für den ε-approximativen Kern von $\mathcal{A}$ ergibt sich dann $\operatorname{apker}(\mathcal{A}, \varepsilon) = \langle v_1, v_2 \rangle_{\mathbb{R}}$ mit

$$v_1 = \begin{pmatrix} 0,69 \\ 0,15 \\ -0,16 \\ 0,69 \\ 0,01 \end{pmatrix} \quad \text{bzw.} \quad v_2 = \begin{pmatrix} -0,15 \\ 0,69 \\ -0,69 \\ -0,15 \\ 0,03 \end{pmatrix}.$$

Dies liefert die beiden Polynome

$$g_1 = 0,69 y_2^{(1)} + 0,15 y_1^{1)} - 0,15 y_2 + 0,69 y_1$$
$$g_2 = 0,7 y_1^{(1)} - 0,7 y_2.$$

Im Schritt $d = 2$ wird analog das Polynom

$$g_3 = 0,57 y_2^2 + 0,6 y_1^2 - 0,57$$

und

$$g_4 = 0,72 y_1^4 - 0,69 y_1^2$$

im Schritt $d = 4$ berechnet. Nach Normierung erhalten wir also geeignete Approximationen der Polynome $\tilde{g}_1 = y_2^{(1)} + y_1$, $\tilde{g}_2 = y_1^{(1)} - y_2$, $\tilde{g}_3 = y_2^2 + y_1^2 - 1$, $\tilde{g}_4 = y_1^4 - y_1^2$.

Notationen

$K[x_1,\dots,x_n]$	Polynomring in den Unbestimmten $x_1,\dots,x_n$ über K
$K\{y_1,\dots,y_n\}$	differentieller Polynomring in den differentiellen Unbestimmten $y_1,\dots,y_n$ über K
$\mathbb{D}^n$	Menge der Derivate der differentiellen Unbestimmten $y_1,\dots,y_n$
$\mathbb{T}^n$	Menge der Terme in den differentiellen Unbestimmten $y_1,\dots,y_n$
$\mathbb{D}(f)$	differentieller Träger des differentiellen Polynoms f
$\mathrm{Supp}(f)$	Träger des Polynoms f
$\mathrm{ord}(f)$	Ordnung des differentiellen Polynoms f
$w(f)$	Gewicht des differentiellen Polynoms f
G_k	Menge aller Elemente in G der Ordnung kleiner oder gleich k
$\langle G\rangle$	das von G erzeugte Ideal
$\langle G\rangle_\partial$	das von G differentiell erzeugte Ideal
$\sqrt{I}$	das Radikal von I
$\deg(f)$	Grad des differentiellen Polynoms f
$\mathrm{LD}_\tau(f)$	Leitderivat des differentiellen Polynoms f
$\mathrm{LV}_\tau(f)$	Leitvariable des differentiellen Polynoms f
$\mathrm{in}_\tau(f)$	Initial des differentiellen Polynoms f
$\mathrm{sep}_\tau(f)$	Separand des differentiellen Polynoms f
$\mathcal{Z}(f)$	Menge aller Nullstellen des differentiellen Polynoms f
$\mathcal{I}(\mathbb{X})$	Verschwindungsideal der Punktmenge $\mathbb{X}$
$\dim(D/I)$	Dimension von D/I
$\mathrm{ord}(I)$	Ordnung des differentiellen Ideals I
$\mathrm{HF}_{D/I}$	differentielle Hilbertfunktion von D/I
$\mathrm{HP}_{D/I}$	differentielles Hilbertpolynom von D/I
$\tau\mathtt{Lex}$	differentiell lexikographische Termordnung bzgl. τ
$\mathrm{LT}_\sigma(f)$	Leitterm des differentiellen Polynoms f
$\mathrm{LC}_\sigma(f)$	Leitkoeffizient des differentiellen Polynoms f
$\mathrm{LM}_\sigma(f)$	Leitmonom des differentiellen Polynoms f
$\mathrm{LT}_\sigma(I)$	Leittermideal des differentiellen Ideals I
$F_\gamma R$	γ-te Komponente einer Filtrierung von R
$\mathrm{gr}_\Phi(R)$	assoziiert graduierter Ring von R bzgl. der Filtrierung Φ
$\mathrm{LF}_\Phi(f)$	Leitform des differentiellen Polynoms f
$\mathrm{LF}_\Phi(I)$	Leittformenideal des differentiellen Ideals I
$\mathrm{pw}(f)$	Phantomgewicht des differentiellen Polynoms f

Literaturverzeichnis

[1] F. Boulier, D. Lazard, F. Ollivier, M. Petitot, *Representation for the radical of a finitely generated differential ideal*, Proc. ISSAC (1995), ACM Press, S. 158–166.

[2] F. Boulier, D. Lazard, F. Ollivier, M. Petitot, *Computing representations for radicals of finitely generated differential ideals*, Technical Report IT-306, LIFL.

[3] D. Bouziane, A. Kandri Rody, H. Maârouf, *Unmixed-dimensional decomposition of a finitely generated perfect differential ideal*, J. Symb. Comp. **31** (2001), S. 631–649.

[4] B. Buchberger, H.M. Möller, *The construction of multivariate polynomials with preassigned zeros*, Proc. EUROCAM'82, Lect. Notes in Comp. Sci. **144** (1982), Springer, Heidelberg, S. 24–31.

[5] G. Carrà-Ferro, *Gröbner bases and differential ideals*, Notes de AAECC **5**, Springer, Menorca, 1987, S. 129–140.

[6] C. Fassino, *An approximation to the Gröbner basis of ideals of perturbed points: Part I*, Preprint, 2006.

[7] R. Gebauer, H.M. Möller, *On an installation of Buchberger's algorithm*, J. Symb. Comp. **6** (1988), S. 275–286.

[8] A. Giovini, T. Mora, G. Niesi, L. Robbiano, C. Traverso, *"One sugar cube, please" or Selection strategies in Buchberger algorithm*, Proc. ISSAC (1991), ACM Press, New York, S. 49–54.

[9] G.H. Golub, C.F. van Loan, *Matrix computations*, The Johns Hopkins University Press, Baltimore, 1985.

[10] D. Heldt, M. Kreuzer, S. Pokutta, H. Poulisse, *Approximate computation of zero-dimensional polynomial ideals*, eingereicht (2006).

[11] E. Hubert, *Factorization-free decomposition algorithms in differential algebra*, J. Symb. Comp. **29** (2000), S. 641–662.

[12] I. Kaplansky, *An introduction to differential algebra*, Hermann, 1970.

[13] E. R. Kolchin, *Differential algebra and algebraic groups*, Academic Press, New York, 1973.

[14] M. Kreuzer, L. Robbiano, *Computational commutative algebra 1*, Springer, Heidelberg, 2000.

[15] M. Kreuzer, L. Robbiano, *Computational commutative algebra 2*, Springer, Heidelberg, 2005.

[16] E. Mansfield, *Differential Gröbner bases*, PhD thesis, Univ. of Sydney, 1991.

[17] M.G. Marinari, H.M. Möller, T. Mora, *Gröbner basis of ideals defined by functionals with an application to ideals of projective points*, Appl. Algebra Eng. Comm. Comp. **4** (1993), S. 103–145.

[18] F. Ollivier, *Standard bases of differential ideals*, Proc. AAECC **8** (1990), Tokio, S. 304-321.

[19] A. Ovchinnikov, A. Zobnin, *Classification and applications of monomial orderings and the properties of differential orderings*, Proc. of CASC 2002, S. 237–252.

[20] C. Riquier, *Les systèmes d'équations aux dérivées partielles*, Gauthier-Villars, Paris, 1910.

[21] J. F. Ritt, *Differential algebra*, Amer. Math. Soc., New York, 1950.

[22] A. Rosenfeld, *Specialization in differential algebra*, Trans. Amer. Math. Soc. **90** (1959), S. 394–407.

[23] C. Rust, G.J. Reid, *Rankings of partial derivatives*, Proc. ISSAC (1997), ACM Press, New York, S. 9–16.

[24] B. Sadik, *Computing characteristic sets of radical differential ideals*, Georg. Math. J. **13** (2006), S. 515–527.

[25] W.Y. Sit, *The Ritt-Kolchin theory for differential polynomials*, In: Differential Algebra and Related Topics, 2002, S. 1–70.

[26] H. Stetter, *Numerical polynomial algebra*, SIAM, Philadelphia, 2004.

[27] J.M. Thomas, *Matrices of integers ordering derivatives*, Trans. Amer. Math. Soc. **33** (1931), S. 389–410.

[28] V. Weispfenning, *Differential term-orders*, Proc. ISSAC (1993), ACM Press, New York, S. 245–253.

[29] A. Zobnin, *Admissible orderings and finiteness criteria for differential Standard bases*, Proc. ISSAC (2005), Beijing, S. 365–372.