Albert–Ludwigs–Universität Freiburg i. Br.
Fakultät für Mathematik

Modelltheorie von Körpern mit paarweise kommutierenden Derivationen

Diplomarbeit
vorgelegt von
Jens Böger

bei Professor Dr. Martin Ziegler

Abteilung für Mathematische Logik
und Grundlagen der Mathematik

September 1996

Inhaltsverzeichnis

Einleitung **2**

1 Differential algebraische Grundlagen **5**

1.1 Derivationen 5
1.2 Radikale D-Ideale 9
1.3 Fortsetzung von Derivationen und von der D-Struktur 12
1.4 Derivationen und Polynomringe 16
1.5 Separable Körpererweiterungen 17

2 Der D-Polynomring **21**

2.1 Die Menge der Ableitungsoperatoren Θ 21
2.2 Die Definition des D-Polynomringes 22
2.3 X-Ableitungen und Höhe der D-Polynome 23
2.4 Selbstreduzierte Mengen 26
2.5 Die charakteristische Menge eines D-Ideals 31
2.6 Die D-Ideale im D-Polynomring 33

3 Modelltheorie der Differential-Körper **38**

3.1 Das Erzwingungsideal 40
3.2 Kohärente Mengen 41
3.3 Differentiell abgeschlossene Körper 45
3.4 Quantorenelimination für $\mathbf{pDCF}_0$ und Anwendungen 48
3.5 ω-Stabilität und das Primmodell 52

Abschließende Bemerkung **55**

Einleitung

Mit dieser Arbeit soll die grundlegende Modelltheorie von Körpern, auf denen endlich viele Derivationsabbildungen erklärt sind, die bezüglich der Hintereinanderausführung jeweils paarweise miteinander vertauscht werden können, untersucht werden. Das Interesse an Körpern mit Derivationen geht auf J. F. Ritt zurück. Dieser hat hauptsächlich den Fall mit einer einzelnen Derivation (*gewöhnliche* differentielle Algebra) betrachtet, aber auch schon Ergebnisse auf die Situation mit endlich vielen paarweise kommutierenden Derivationen übertragen, die er dann *partielle Derivationen* genannt hat. Wir wollen uns dem anschließen. Seine Arbeiten wurden fortgesetzt und verallgemeinert, was für uns hauptsächlich bedeutet, daß die Theorie als *differentielle Algebra* formuliert wurde. In dieser Hinsicht denken wir an erster Stelle an E. R. Kolchin, sein Buch *Differential Algebra and Algebraic Groups* steht für die gesamte Algebra als Referenz im Hintergrund. Kolchin hat auch konsequent die differentielle Algebra für partielle Derivationen entwickelt.

Die ersten modelltheoretischen Untersuchungen wurden von A. Robinson in *On the concept of a differentially closed field* durchgeführt, die sich aber auf den Fall einer Derivation bezogen. Er hat dabei von der Arbeit *An elimination theory for differential algebra* von A. Seidenberg Gebrauch gemacht. Diese nutzte er zur Axiomatisierung der von ihm untersuchten Körper. Damit konnte Robinson die von ihm entwickelten Begriffe des Modellbegleiters und der Modellvervollständigung auch an den gewöhnlichen D-Körper (mit nur einer Derivation) demonstrieren. Diese Arbeit wurde von L. Blum aufgegriffen, als Verweis sei hier der Aufsatz *Differentially closed fields: a model-theoretic tour* genannt. Sie hat sich von der Seidenberg-Arbeit gelöst und andere Axiome für die existentiell abgeschlossenen D-Körper angeben. Ihr Ziel war ein Axiomensystem, das mehr an den Axiomen für algebraisch abgeschlossene Körper orientiert war. Darunter verstand sie insbesondere, daß es möglich sein solle, sich auf Polynome mit nur einer differentiell Unbestimmten zu beschränken. Dieses gelang ihr durch die Untersuchung der einfachen D-Körpererweiterungen. Weiterhin wandte sie die Techniken von Morley und Shelah an, um die Existenz eines Primmodelles nachzuweisen, weswegen sie als erste überhaupt mit modelltheoretischen Mitteln ein Analogon zum algebraischen Abschluß eines Körpers angeben konnte.

Daß sich die modelltheoretischen Ergebnisse von Körpern mit einer Derivation auf die Situation mit mehreren kommutierenden verallgemeinern lassen, wird in der Literatur an verschiedenen Stellen behauptet, man vergleiche mit der oben bereits zitierten Arbeit von Blum, oder Wood, *The model theory of differential fields revisited*. Es gibt allerdings bislang keine explizite Ausarbeitung. In der vorliegenden Arbeit soll das geschehen. Das könnte in Anlehnung an Robinson wieder dadurch geschehen, daß man anstelle von Theorem 1. dessen Verallgemeinerung Theorem 9. aus [SEIDENBERG] benutzt. Wir wollen jedoch den Weg von Blum beschreiten.

Dadurch ergibt sich eine Dreiteilung dieser Arbeit. Im 1. Kapitel werden uns die grundlegenden Eigenschaften der „D-Objekte“ begegnen. Darunter verstehen wir allgemeine Tatsachen über Derivationen, die Übertragung entsprechender Ergebnisse auf Ideale, die unter den Derivationen abgeschlossen sind (D-Ideale), wie zum Beispiel die irreduzible Zerlegung von radikalen Idealen unter ACC. Weiterhin sollen hier auch Fragen, die die Möglichkeit betreffen, zu Erweiterungsstrukturen überzugehen, die dann die vorhandenen D-Struktur in geeigneter Weise fortsetzen, geklärt werden.

Das 2. Kapitel ist dem D-Polynomring gewidmet. Es muß in Hinblick auf die Anwendungen das Aussehen dieses Ringes, bzw. dessen D-Ideale geklärt werden. Dazu geben wir seine Definition explizit an und entwickeln grundlegende Techniken für das Rechnen mit D-Polynomen. Wir müssen ein auf Ritt zurückreichendes Reduzierungsverfahren bereitstellen. Wir lernen die selbstreduzierten Polynommengen kennen, denen für die Theorie eine besondere Bedeutung zukommt. Ferner werden wir feststellen, daß ein D-Ideal immer durch eine endliche Menge von Polynomen beschrieben werden kann. Am Ende wollen wir eine Übertragung des Hilbertschen Basissatzes angeben, der aber nur für radikale D-Ideale Gültigkeit besitzen wird.

Nach all diesen Vorarbeiten können wir im 3. Kapitel nun die Modelltheorie ausarbeiten. Dabei ist das Ziel, einen Modellbegleiter für die Klasse der Körper mit mehreren kommutierenden Derivationen zu finden. Das werden wir angehen, indem wir die einfach-existentiell abgeschlossenen Strukturen untersuchen und versuchen, für diese ein geeignetes Axiomensystem anzugeben. Dazu müssen wir feststellen, welche Gleichungssysteme aus D-Polynomen überhaupt lösbar sind, um sagen zu können, daß diese dann auch alle in der abgeschlossenen Struktur realisiert sind. Es folgt dann die Aufgabe nachzuweisen, daß sich diese Systeme in der Sprache der ersten Stufe charakterisieren lassen. Damit können wir dann Quantorenelimination folgern und erhalten insgesamt den Modellbegleiter (die existentiell abgeschlossenen D-Körper). Dazu geben wir einige der übliche Anwendungen an. Insbesondere werden wir mit Hife der Quantorenelimination die Entsprechung von Typen und Primidealen zeigen, was dann die ω-Stabilität ergibt. Dadurch gewinnen wir die Existenz eines Primmodelles.

Zu guter letzt sei hier Herrn Professor Dr. Ziegler für die Betreuung dieser

Arbeit gedankt. Mein besonderer Dank gilt aber auch Herrn Bernhard Herwig und Herrn Martin Erkens für ihre Unterstützung, von ihnen konnte ich während der Bearbeitung viel lernen.

Kapitel 1

Differential algebraische Grundlagen

In diesem Kapitel soll die grundlegende differentielle Algebra entwickelt werden, die später dann für die Formulierung der Modelltheorie der D-Körper mit partiellen Derivationen notwendig ist. Dabei versucht man möglichst bekannte Erbegnisse der „gewöhnlichen“ Algebra auf die Situation mit Ableitungen zu übertragen. Das schlägt sich darin nieder, daß man, ausgehend von den bekannten algebraischen Objekten, solche untersucht, die eine D-Struktur tragen, bzw. mit dieser verträglich sind. Für dieses Kapitel sei auf das Buch von [KOLCHIN 1] oder auch auf [KAPLANSKY] als Referenz verwiesen.

Viele Eigenschaften für Derivationen gelten in beliebigen Ringen, bei der Untersuchung der Ideale ergeben sich aber im Zusammenhang mit radikalen D-Idealen Probleme, die wir unterdrücken wollen, um eine möglichst starke Analogie zum derivationsfreien Fall zu erhalten. Deswegen schränken wir uns ein und betrachten im folgenden ausschließlich nullteilerfreie, kommutative Ringe R mit 1 (von der Null verschieden), die $\mathbb{Q}$ enthalten, bzw. Körper F von der Charakteristik 0.

1.1 Derivationen

Unter einem **D-Ring** verstehen wir einen Ring, auf dem m **partielle Derivationen** (oder auch **partielle Ableitungen**) $\partial_1, \ldots, \partial_m$ erklärt sind. Damit meinen wir Abbildungen $\partial_i : R \to R$, die den folgenden Regeln genügen:

$$\begin{aligned} \partial_i(x+y) &= \partial_i(x) + \partial_i(y), \\ \partial_i(xy) &= \partial_i(x)y + x\partial_i(y) \quad \text{(Produktregel)} \end{aligned}$$

f.a. $x, y \in R$. Eine Abbildung mit diesen Eigenschaften bezeichnen wir als **Derivation**. Weiter fordern wir die Vertauschungsregeln

$$\partial_i\partial_j(x) = \partial_j\partial_i(x)$$

f.a. $x \in R$ und $1 \leq i, j \leq m$.

Beispiele:

a) Sei G ein Gebiet des $\mathbb{C}^m$ und $\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_m}$ die partiellen Ableitungen in den komplexen Variablen $z_1, \ldots z_m$. Dann sind die in G analytischen komplexwertigen Funktionen ein D-Ring.

b) Sei G ein Gebiet des $\mathbb{C}^m$ und $\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_m}$ die komplexen partiellen Ableitungen. Dann bilden die in G meromorphen komplexwertigen Funktionen $\mathcal{M}(G)$ einen D-Körper.

Wir bezeichnen einen Unterring R' von R als **D-Unterring**, wenn die Derivationen eingeschränkt auf R' bereits Derivationen auf R' sind. Dann gelten die Vertauschungsregeln automatisch. R selbst heißt üblicherweise **D-Oberring** von R'. Ein **D-Körper** ist ein Körper, der ein D-Ring ist, die Begriffe D-Oberkörper und D-Unterkörper sind ebenso zu gebrauchen. Wenn wir mit $L \supset K$ solch eine D-Ringerweiterung, bzw. D-Körpererweiterung gegeben haben, dann definieren wir für eine Teilmenge A von L:

$$K\{A\} \stackrel{\text{def}}{=} \bigcap \{K' \subset L \mid K \cup A \subset K',\ K' \text{ D-Unterring von } L\}\ ,$$

den von A und K erzeugten D-Unterring in L, bzw.

$$K\langle A\rangle \stackrel{\text{def}}{=} \bigcap \{K' \subset L \mid K \cup A \subset K',\ K' \text{ D-Unterkörper von } L\}\ ,$$

den von A und K erzeugten D-Unterkörper in L.

Bemerkung 1.1.1 *Für eine Derivation ∂_i gilt:*

a) $\partial_i 0 = 0$ *und* $\partial_i 1 = 0$. *Damit für* $m \in \mathbb{N}$: $\partial_i(m \cdot 1) = \partial_i 1 + \ldots + \partial_i 1 = 0$. $\partial_i(-1) = 0$, *also* $\partial_i(m) = 0$ *für* $m \in \mathbb{Z}$.

b) Existiert a^{-1} *in* R *zu* $a \in R$, *dann gilt für beliebiges* $b \in R$:

$$\partial_i\left(\frac{b}{a}\right) = \frac{\partial_i b \cdot a - b \cdot \partial_i a}{a^2} \quad (\textit{Quotientenregel})\,.$$

c) Für $a \in \mathbb{Q}$ *gilt:* $\partial_i a = 0$.

d) Für $n \in \mathbb{N}$ *gilt:* $\partial_i(a^n) = na^{n-1}\partial_i a$ *f.a.* $a \in R$.

e) Es gilt die Leibniz-Regel: $\partial_i^n(ab) = \sum_{k=0}^{n} \binom{n}{k} \partial_i^{n-k} a \cdot \partial_i^k b$ *für* $n \in \mathbb{N}$.

f) Für zwei Derivationen ∂_i *und* ∂_j *sind* $\partial_i + \partial_j$ *und* $\partial_i - \partial_j$ *wieder Derivationen.*

Denn: Zu a) $\partial_i 0 = \partial_i(0+0) = \partial_i 0 + \partial_i 0 = 2\cdot\partial_i 0$, also $\partial_i 0 = 0$.
$\partial_i 1 = \partial_i(1\cdot 1) = (\partial_i 1)\cdot 1 + 1\cdot(\partial_i 1) = 2\cdot\partial_i 1$. Es folgt $\partial_i 1 = 0$.
$0 = \partial_i 0 = \partial_i(1+(-1)) = \partial_i 1 + \partial_i(-1) = \partial_i(-1)$.
Zu b) $0 = \partial_i 1 = \partial_i(aa^{-1}) = (\partial_i a)\cdot a^{-1} + a\cdot\partial_i(a^{-1}) \quad\Longrightarrow\quad \partial_i(a^{-1}) = -\frac{\partial_i a}{a^2}$. Also gilt $\partial_i(ba^{-1}) = (\partial_i b)\cdot a^{-1} + b\cdot(-\frac{\partial_i a}{a^2}) = \frac{\partial_i b\cdot a - b\cdot\partial_i a}{a^2}$.
Zu c) Folgt aus *a), und b)*.
Nun folgen jeweils Induktionsbeweise über n.
Zu d) Der Induktionsanfang $n=0$ ist mit a) klar.

$$\begin{aligned}\partial_i(a^n) &= \partial_i(a^{n-1}a) \;=\; \partial_i(a^{n-1})\cdot a + a^{n-1}\partial_i a\\ &\overset{\text{I.V.}}{=} ((n-1)a^{n-2}\partial_i a)a + a^{n-1}\partial_i a \;=\; (n-1)a^{n-1}\partial_i a + a^{n-1}\partial_i a\\ &= na^{n-1}\partial_i a\,.\end{aligned}$$

Zu e) $n=1$ ist gerade die Produktregel. Im Fall $n-1\to n$ berechnen wir

$$\begin{aligned}\partial_i^n(ab) &= \partial_i(\partial_i^{n-1}(ab)) \overset{\text{I.V.}}{=} \partial_i\left(\sum_{k=0}^{n-1}\binom{n-1}{k}\partial_i^{n-1-k}a\cdot\partial_i^k b\right)\\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}\partial_i\left(\partial_i^{n-1-k}a\cdot\partial_i^k b\right)\\ &= \sum_{k=0}^{n-1}\binom{n-1}{k}\left(\partial_i^{n-k}a\cdot\partial_i^k b + \partial_i^{n-(k+1)}a\cdot\partial_i^{k+1}b\right)\,.\end{aligned}$$

Wir zerlegen diese Summe in $\sum_{k=0}^{n-1}\binom{n-1}{k}\partial_i^{n-k}a\cdot\partial_i^k b$ und $\sum_{k=1}^{n}\binom{n-1}{k-1}\partial_i^{n-k}a\cdot\partial_i^k b$, wobei wir bei der zweiten Summe eine Indexverschiebung vorgenommen haben. Es gilt bekanntlich für die Binomialkoeffizienten $\binom{n-1}{k}+\binom{n-1}{k-1} = \binom{n}{k}$, $1 = \binom{n-1}{0} = \binom{n}{0}$, $1 = \binom{n-1}{n-1} = \binom{n}{n}$, und wir erhalten, nachdem wir die äußeren Terme nochmals abgespaltet haben:

$$\binom{n}{0}\partial_i^{n-k}a\cdot b + \sum_{k=1}^{n-1}\left(\binom{n-1}{k}+\binom{n-1}{k-1}\right)\partial_i^{n-k}a\cdot\partial_i^k b + \binom{n}{n}a\cdot\partial_i^n b\,,$$

was dann zusammengefaßt gerade $\sum_{k=0}^{n}\binom{n}{k}\partial_i^{n-k}a\cdot\partial_i^k b$ ergibt.
Zu f) Wir rechnen beide Fälle zusammen durch, indem wir $\pm$ verwenden. Für $a,b\in R$ gilt:

$$\begin{aligned}(\partial_i\pm\partial_j)(a+b) &= \partial_i(a+b)\pm\partial_j(a+b) \;=\; \partial_i a + \partial_i b \pm (\partial_j a + \partial_j b)\\ &= \partial_i a \pm \partial_j a + \partial_i b \pm \partial_j b \;=\; (\partial_i\pm\partial_j)a + (\partial_i\pm\partial_j)b\end{aligned}$$

$$\begin{aligned}(\partial_i\pm\partial_j)(ab) &= \partial_i(ab)\pm\partial_j(ab) \;=\; \partial_i a\cdot b + a\cdot\partial_i b \pm \partial_j a\cdot b \pm a\cdot\partial_j b\\ &= (\partial_i a\pm\partial_j a)b + a(\partial_i b\pm\partial_j b) \;=\; (\partial_i\pm\partial_j)a\cdot b + a\cdot(\partial_i\pm\partial_j)b\,.\end{aligned}$$

□

Ein Element $c\in R$, für das $\partial_i c = 0$ gilt, nennen wir eine Konstante bzgl. ∂_i.

Die Menge $C_{\partial_i} \stackrel{\text{def}}{=} \{c \in R \mid \partial_i c = 0\}$ ist ein Unterring von R, da $\partial_i 0 = 0$, $\partial_i 1 = 0$ und für $c_1, c_2 \in C_{\partial_i}$ mit den Ableitungsregeln $\partial_i(c_1 - c_2) = \partial_i c_1 - \partial_i c_2 = 0 - 0 = 0$, $\partial_i(c_1 c_2) = \partial_i c_1 \cdot c_2 + c_1 \cdot \partial_i c_2 = 0 \cdot c_2 + c_1 \cdot 0 = 0$ gilt. Die Menge $C = \bigcap_{i=1}^m C_{\partial_i}$ ist somit auch ein Unterring von R, für dessen Elemente c $\partial_i c = 0$ f.a. ∂_i erfüllt ist. Insbesondere sind alle Derivationen eingeschränkt auf C wieder Derivationen (m triviale Derivationen). C ist also ein D-Unterring von R, den wir als den **Ring der Konstanten** bezeichnen. Die letzte Bemerkung hat gezeigt, daß $\mathbb{Q}$ immer in der Menge der Konstanten eines Ringes enthalten ist.
Für den Fall von D-Körpern halten wir ausdrücklich nochmals fest, daß für zwei $c_1, c_2 \in C$ mit $c_2 \neq 0$ die Quotientenregel gerade $\partial_i(c_1 c_2^{-1}) = 0$ liefert, die Konstanten somit einen D-Unterkörper bilden, der natürlich immer $\mathbb{Q}$ enthalten muß. Für eine Konstante c und ein beliebiges $a \in R$ folgt weiterhin $\partial_i(c \cdot a) = 0 \cdot a + c \cdot \partial_i a = c \cdot \partial_i a$. Dies besagt also, daß die Derivationen C-linear sind.
Einen Homomorphismus ϕ zwischen zwei D-Ringen R und R' mit jeweils m Derivationen ∂_i^R, bzw. $\partial_i^{R'}$ nennen wir einen **D-Homomorphismus**, wenn er mit den Ableitungen verträglich ist, wenn also $\phi(\partial_i^R a) = \partial_i^{R'} \phi(a)$ f.a. i und $a \in R$. Jetzt ist klar, was D-Isomorphismen, D-Automorphismen usw. sind.
Weiter bezeichnen wir ein Ideal $\mathfrak{A}$ in R als **D-Ideal**, wenn es unter allen Derivationen abgeschlossen ist, d.h.: $x \in \mathfrak{A} \Longrightarrow \partial_i x \in \mathfrak{A}$ für $1 \leq i \leq m$.

Definition 1 *$\mathfrak{A}$ sei ein D-Ideal in R.*

1. *$\mathfrak{A}$ heißt* **radikales D-Ideal**, *wenn aus $a^n \in \mathfrak{A}$ für ein $n \in \mathbb{N}$ auch $a \in \mathfrak{A}$ folgt.*

2. *$\mathfrak{A}$ heißt* **primes D-Ideal**, *wenn es als D-Ideal prim im gewöhnlichen Sinne ist, also $\mathfrak{A} \neq R$ und $ab \in \mathfrak{A} \Longrightarrow a \in \mathfrak{A}$ oder $b \in \mathfrak{A}$.*

Es ist klar, daß der Durchschnitt über eine beliebige Familie von D-Idealen wieder ein D-Ideal ist, denn liegt ein x im Durchschnitt, so liegen f.a. i $\partial_i x$ nach Definition in jedem der D-Ideale, somit auch im Durchschnitt. Deswegen ist es möglich, für eine Teilmenge $A \subset R$ das von A erzeugte D-Ideal als den Durchschnitt über alle D-Ideale, die A enthalten, zu bilden. Dadurch wird auch der Durchschnitt über eine Familie von radikalen D-Idealen wieder ein D-Ideal, und für a^n im Durchschnitt folgt, daß a in allen Idealen liegt. Deswegen liegt a selbst im Durchschnitt der radikalen D-Ideale, und somit ist der Durchschnitt ebenfalls radikales D-Ideal. Wir können daher folgende Definitionen treffen:

Definition 2 *Sei A eine Teilmenge von R.*

1. *$\langle A \rangle \stackrel{\text{def}}{=} \bigcap \{\mathfrak{A} \subset R \mid A \subset \mathfrak{A}\ ,\ \mathfrak{A}$ D-Ideal von $R\}$ heißt das von A* **erzeugte D-Ideal**.

2. *$\{A\}_{\mathfrak{r}} \stackrel{\text{def}}{=} \bigcap \{\mathfrak{A} \subset R \mid A \subset \mathfrak{A}\ ,\ \mathfrak{A}$ radikales D-Ideal von $R\}$ heißt das von A* **erzeugte radikale D-Ideal**.

Für die späteren Anwendungen wollen wir auch noch festhalten, daß bei einer aufsteigende Kette $\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \ldots$ von D-Idealen die Vereinigung $\mathfrak{M} = \bigcup_{n\in\mathbb{N}} \mathfrak{A}_n$ wieder ein D-Ideal ist. Die Idealeigenschaften gelten aus den üblichen Gründen, und für ein $a \in \mathfrak{M}$ muß bereits ein n existieren mit $a \in \mathfrak{A}_n$, damit auch $\partial_i a \in \mathfrak{A}_n \subset \mathfrak{M}$. Würden wir eine solche Kette aus radikalen D-Idealen betrachten, wäre $\mathfrak{M}$ ebenfalls radikales D-Ideal, weil wir uns wieder auf eines der radikalen D-Ideale $\mathfrak{A}_n$ zurückziehen können.

1.2 Radikale D-Ideale

Als nächstes wollen wir die radikalen D-Ideale etwas genauer untersuchen. Diese stehen im Sinne der algebraischen Geometrie ja in naher Verbindung zu Nullstellenmengen von Polynomen. Wir leiten mit Lemma 1.2.4 ein zentrales Ergebnis her, das wir auch später benutzen werden. Ferner erhalten wir die Gleichheit vom Radikal eines D-Ideals und dem vom D-Ideal erzeugten radikalen Ideal.

Lemma 1.2.1 *Sei $\mathfrak{A}$ ein radikales D-Ideal von R, und sei $ab \in \mathfrak{A}$. Dann sind $\partial_i a \cdot b$ und $a \cdot \partial_i b$ in $\mathfrak{A}$ enthalten für alle Derivationen ∂_i.*

Beweis: Aus $ab \in \mathfrak{A}$ und $\mathfrak{A}$ D-Ideal folgt $\partial_i(ab) \in \mathfrak{A}$ f.a. ∂_i.

$$\partial_i(ab) = \partial_i a \cdot b + a \cdot \partial_i b \in \mathfrak{A} \tag{1.1}$$

Wenn wir diese Gleichung mit $\partial_i a \cdot b$ multiplizieren, gelangen wir zu

$$(\partial_i a \cdot b)^2 + (\partial_i a \cdot b)(a \cdot \partial_i b) = (\partial_i a \cdot b)^2 + \partial_i a \cdot \partial_i b \cdot ab \in \mathfrak{A}\ .$$

Weil wir $ab \in \mathfrak{A}$ vorausgesetzt haben, liegt der zweite Summand in $\mathfrak{A}$, und wir können auch für den ersten, $(\partial_i a \cdot b)^2 \in \mathfrak{A}$ folgern. Da $\mathfrak{A}$ radikales D-Ideal ist, ergibt sich nach Definition, daß $\partial_i a \cdot b$ Element von $\mathfrak{A}$ ist, wie behauptet.
Wenn wir (1.1) mit $a \cdot \partial_i b$ multiplizieren, erhalten wir ebenso $a \cdot \partial_i b \in \mathfrak{A}$. □

In der gewöhnlichen Algebra betrachtet man das Radikal eines Ideals, was bekanntlich $\sqrt{\mathfrak{A}} \overset{\text{def}}{=} \{a \in R \mid \text{es ex. } n \in \mathbb{N} \text{ mit } a^n \in \mathfrak{A}\}$ ist. Man erhält den Sachverhalt, daß $\mathfrak{A}$ genau dann ein radikales Ideal ist, wenn $\sqrt{\mathfrak{A}} = \mathfrak{A}$ gilt. Die Menge $\{a \mid \text{es ex. } n \in \mathbb{N} \text{ mit } a^n \in \mathfrak{A}\}$ können wir natürlich auch für ein D-Ideal $\mathfrak{A}$ betrachten, stehen dann aber vor der Frage, ob diese wieder ein D-Ideal bildet. Unter der Voraussetzung $\mathbb{Q} \subset R$ gelingt jedenfalls der Nachweis.

Lemma 1.2.2 *Sei $\mathfrak{A}$ ein D-Ideal in $R \supset \mathbb{Q}$, und für $a \in R$ existiere ein $n \in \mathbb{N}$ mit $a^n \in \mathfrak{A}$. Dann gilt für jede der Derivationen: $(\partial_i a)^{2n-1} \in \mathfrak{A}$.*

Beweis: Wir zeigen für alle ∂_i: $a^{n-k}(\partial_i a)^{2k-1} \in \mathfrak{A}$. $k = n$ liefert dann das gewünschte Ergebnis.
<u>$k = 1$:</u> Es gilt ja $\partial_i(a^n) = na^{n-1}\partial_i a \in \mathfrak{A}$ nach Bemerkung 1.1.1, dadurch $a^{n-1}\partial_i a \in \mathfrak{A}$, da $n^{-1} \in \mathbb{Q} \subset R$ vorausgesetzt ist.
<u>$k \to k+1$:</u> Wir nehmen $a^{n-k}(\partial_i a)^{2k-1} \in \mathfrak{A}$ als I.V. an. Damit berechnen wir:

$$\begin{aligned} \partial_i(a^{n-k}(\partial_i a)^{2k-1}) &= \partial_i(a^{n-k}) \cdot (\partial_i a)^{2k-1} + a^{n-k} \cdot \partial_i\left((\partial_i a)^{2k-1}\right) \\ &= (n-k)a^{n-(k+1)} \cdot (\partial_i a)^{2k} + (2k-1)a^{n-k} \cdot (\partial_i a)^{2k-2} \cdot \partial_i^2 a \,. \end{aligned}$$

Da $\mathfrak{A}$ D-Ideal ist, liegt der Ausgangsterm und damit diese Summe in $\mathfrak{A}$, weswegen auch nach Multiplikation mit $\partial_i a$ gilt:

$$(n-k)a^{n-(k+1)} \cdot (\partial_i a)^{2k+1} + (2k-1)a^{n-k} \cdot (\partial_i a)^{2k-1} \cdot \partial_i^2 a \ \in \mathfrak{A} \,.$$

Nach unserer I.V. ist hiervon der rechte Summand bereits Element von $\mathfrak{A}$, weswegen wir das dann auch für den linken schließen können. Division durch $(n-k)$ liefert $a^{n-(k+1)}(\partial_i a)^{2(k+1)-1} \in \mathfrak{A}$. □

Jetzt wissen wir also, daß $\{a \in R \mid \text{es ex. } n \in \mathbb{N} \text{ mit } a^n \in \mathfrak{A}\}$ unter den Derivationen abgeschlossen, also ein D-Ideal ist. Wir können das gewünschte Ergebnis folgern.

<u>Korollar</u> 1.2.3

$$\begin{aligned} \{\mathfrak{A}\}_{\mathfrak{r}} &= \bigcap \{\mathfrak{B} \subset R \mid \mathfrak{B} \textit{ radikales D-Ideal in } R, \mathfrak{A} \subset \mathfrak{B}\} \\ &= \{a \in R \mid \textit{es ex. } n \in \mathbb{N} \textit{ mit } a^n \in \mathfrak{A}\} \end{aligned}$$

Nun sollen noch einige wichtige Eigenschaften von radikalen D-Idealen formuliert werden, die wir später ebenfalls benötigen werden.

<u>Lemma</u> 1.2.4 *Sei R ein D-Ring, und seien S und T Teilmengen von R. Für die von S und T erzeugten radikalen D-Ideale gilt:*

a) $\{S\}_{\mathfrak{r}} \cdot \{T\}_{\mathfrak{r}} \subset \{S \cdot T\}_{\mathfrak{r}}$.

b) $\{S \cdot T\}_{\mathfrak{r}} = \{S\}_{\mathfrak{r}} \cap \{T\}_{\mathfrak{r}}$.

Beweis: Zu a) Sei $\mathcal{M}$ eine Teilmenge und $\mathfrak{A}$ ein radikales D-Ideal von R. Die Menge $\mathfrak{B} \overset{\text{def}}{=} \{x \in R \mid \mathcal{M}x \subset \mathfrak{A}\}$ ist dann ein radikales D-Ideal, da aus $a, b \in \mathfrak{B}$ für ein beliebiges $s \in \mathcal{M}$ natürlich folgt, daß $s(a+b) = sa + sb$ und $s(ab) = (sa)b = a(sb)$ Elemente von $\mathfrak{A}$ sind. Weiter ist nun dieses Ideal $\mathfrak{B}$ auch D-Ideal, da ja für ein beliebiges ∂_i und $a \in \mathfrak{B}$ aus $sa \in \mathfrak{A}$ mit Lemma 1.2.1 $s \cdot \partial_i a \in \mathfrak{A}$ für beliebiges s aus $\mathcal{M}$ folgt. Und $a^n \in \mathfrak{B}$ heißt $sa^n \in \mathfrak{A}$ für ein beliebiges s aus $\mathcal{M}$. Jetzt ergibt die Multiplikation mit s^{n-1} sofort $s^n a^n \in \mathfrak{A}$, was wegen $\mathfrak{A}$ radikales

Ideal ja $sa \in \mathfrak{A}$ bedeutet. Das heißt aber genau $a \in \mathfrak{B}$. Insgesamt also ist $\mathfrak{B}$ radikales D-Ideal.

Nun wählen wir als Teilmenge $\mathcal{M}$ ein einzelnes Element $a \in R$ und als radikales D-Ideal $\mathfrak{A}$ das von a und T erzeugte radikale D-Ideal, d.h. $\mathfrak{B}_{a,T} \stackrel{\text{def}}{=} \{x \in R \mid ax \in \{a, T\}_\mathfrak{r}\}$. $\mathfrak{B}_{a,T}$ enthält die ganze Menge T, als radikales D-Ideal damit definitionsgemäß das von T erzeugte radikale D-Ideal $\{T\}_\mathfrak{r}$. Wir haben somit die Inklusion $a \cdot \{T\}_\mathfrak{r} \subset \{a, T\}_\mathfrak{r}$.

Zuletzt nehmen wir das Ideal $\{S\}_\mathfrak{r}$ als $\mathcal{M}$ und betrachten $\mathfrak{B} \stackrel{\text{def}}{=} \{x \in R \mid \{S\}_\mathfrak{r} \cdot x \subset \{S, T\}_\mathfrak{r}\}$. Wir sehen, daß wieder ganz T, somit $\{T\}_\mathfrak{r} \subset \mathfrak{B}$ geschlossen werden kann. Das liefert jetzt das Behauptete: $\{S\}_\mathfrak{r} \cdot \{T\}_\mathfrak{r} \subset \{S \cdot T\}_\mathfrak{r}$.

Zu b) „$\supset$“: Für das radikale D-Ideal $I \stackrel{\text{def}}{=} \{S\}_\mathfrak{r} \cap \{T\}_\mathfrak{r}$ gilt natürlich $I \subset \{S\}_\mathfrak{r}$ und $I \subset \{T\}_\mathfrak{r}$. Das ergibt mit *a)* $I \cdot I \subset \{S\}_\mathfrak{r} \cdot \{T\}_\mathfrak{r} \subset \{S \cdot T\}_\mathfrak{r}$. Für ein $a \in I$ folgt somit $a^2 \in \{S \cdot T\}_\mathfrak{r}$, wegen der Radikalität also $a \in \{S \cdot T\}_\mathfrak{r}$.
„$\subset$“: Für ein $a \in \{S \cdot T\}_\mathfrak{r}$ gilt unmittelbar aus der Definition für ein radikales Ideal, daß sowohl $a \in \{S\}_\mathfrak{r}$, als auch $a \in \{T\}_\mathfrak{r}$, und somit $a \in \{S\}_\mathfrak{r} \cap \{T\}_\mathfrak{r}$ erfüllt ist. $\square$

Dieses Lemma leitet uns auf einen Sachverhalt von großer Bedeutung für die radikalen D-Ideale hin. Wir werden als Folgerung aus dem nächsten Lemma die Zerlegung eines radikalen D-Ideals in D-Primideale zeigen können.

Lemma 1.2.5 *Sei R ein D-Ring und $T \subset R$ eine multiplikativ abgeschlossene Teilmenge. Wenn $\mathfrak{A}$ maximal ist unter den radikalen D-Idealen, die T nicht enthalten, dann ist $\mathfrak{A}$ prim.*

Beweis: Angenommen, die Aussage ist falsch. Wir geben uns dann Elemente $a \notin \mathfrak{A}$, $b \notin \mathfrak{A}$ mit $ab \in \mathfrak{A}$ vor. Die radikalen D-Ideale $\{\mathfrak{A}, a\}_\mathfrak{r}$ und $\{\mathfrak{A}, b\}_\mathfrak{r}$ umfassen demnach $\mathfrak{A}$ echt, enthalten also beide T wegen der Maximalität von $\mathfrak{A}$. Für ein beliebiges Element $t \in T$ können wir mit Lemma 1.2.4 folgern:

$$t^2 \in \{\mathfrak{A}, a\}_\mathfrak{r} \cdot \{\mathfrak{A}, b\}_\mathfrak{r} \subset \{\mathfrak{A}, ab\}_\mathfrak{r} = \mathfrak{A} \ ,$$

was dann $T \subset \mathfrak{A}$ bedeuten würde, also ein Widerspruch ist! $\square$

Mit ACC bezeichnen wir wie üblich die aufsteigende Kettenbedingung, d.h., daß eine aufsteigende Kette von Idealen bereits nach endlich vielen Schritten stationär wird. Durch die Forderung von ACC für radikale D-Ideale können wir nun auch den Zerlegungssatz für diese formulieren.

Lemma 1.2.6 *In einem D-Ring R mit ACC für die radikalen D-Ideale läßt sich jedes (echte) radikale D-Ideal als Durchschnitt von endlich vielen primen D-Idealen darstellen. Es existiert eine eindeutige irreduzible Darstellung.*

Beweis: Angenommen, die Menge M der radikalen D-Ideale, die sich nicht als solch ein Schnitt darstellen lassen, ist nicht leer. Dann können wir mit ACC ein maximales Element $\mathfrak{A}$ in M wählen. Selbstverständlich kann $\mathfrak{A}$ selbst nicht prim sein, so daß wir $a \notin \mathfrak{A}$ und $b \notin \mathfrak{A}$ mit $ab \in \mathfrak{A}$ wählen können. Die beiden radikalen D-Ideale $\{\mathfrak{A}, a\}_\mathfrak{r}$ und $\{\mathfrak{A}, b\}_\mathfrak{r}$ liegen echt über $\mathfrak{A}$, müssen also beide wegen der Maximaltät von $\mathfrak{A}$ Durchschnitt von jeweils endlich vielen D-Primidealen sein. Wir zeigen nun $\mathfrak{A} = \{\mathfrak{A}, a\}_\mathfrak{r} \cap \{\mathfrak{A}, b\}_\mathfrak{r}$, was dann ein Widerspruch wäre!
„$\subset$" ist klar, für „$\supset$" geben wir uns ein $r \in \{\mathfrak{A}, a\}_\mathfrak{r} \cap \{\mathfrak{A}, b\}_\mathfrak{r}$ vor. Wir schließen mit Lemma 1.2.4:

$$r^2 \in \{\mathfrak{A}, a\}_\mathfrak{r} \cdot \{\mathfrak{A}, b\}_\mathfrak{r} \subset \{\mathfrak{A}, ab\}_\mathfrak{r} = \mathfrak{A} ,$$

wegen der Radikalität von $\mathfrak{A}$ demnach $r \in \mathfrak{A}$.
Für zwei Darstellung $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n = \mathfrak{A} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$, in denen keines der Primideale $\mathfrak{p}_i$ bzw. $\mathfrak{q}_i$ weggelassen werden kann, wollen wir jetzt zeigen, daß diese dann übereinstimmen. Ohne Einschränkung nehmen wir $n \leq m$ an. Wegen der Gleichheit können wir einmal $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n \subset \mathfrak{q}_1$ schließen, was uns zu

$$\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n \subset \mathfrak{q}_1 \tag{1.2}$$

wegen der Idealeigenschaften der $\mathfrak{p}_i$ führt. Wäre keines der $\mathfrak{p}_i$ ganz in $\mathfrak{q}_1$ enthalten, gäbe es $a_1 \in \mathfrak{p}_1, \ldots, a_n \in \mathfrak{p}_n$, aber $a_1, \ldots, a_n \notin \mathfrak{q}_1$. Damit $a_1 \cdots a_n \notin \mathfrak{q}_1$, weil $\mathfrak{q}_1$ prim ist, was aber ein Widerspruch zu (1.2) wäre. Also gilt $\mathfrak{p}_i \subset \mathfrak{q}_1$ für ein i, nach eventueller Umnummerierung ist es $\mathfrak{p}_1$. Genauso können wir folgern, daß eines der $\mathfrak{q}_i$ in $\mathfrak{p}_1$ enthalten ist. Wäre dieses nicht $\mathfrak{q}_1$, hätten wir $\mathfrak{q}_i \subset \mathfrak{q}_1$, weswegen $\mathfrak{q}_1$ dann in der Schnittbildung weggelassen werden könnte, was aber für eine irreduzible Darstellung nicht gelten darf. Also $\mathfrak{p}_1 = \mathfrak{q}_1$. Auf diese Weise erhalten wir dann $\mathfrak{p}_i = \mathfrak{q}_i$ für $1 \leq i \leq n$. Wäre jetzt $m > n$, gäbe es $\mathfrak{q}_i$, die wieder bei der Schnittbildung überflüssig wären, was ja nicht sein kann. □

1.3 Fortsetzung von Derivationen und von der D-Struktur

Wir müssen uns nun dem Problem der Fortsetzbarkeit der D-Struktur zuwenden, denn in der Algebra ist der Übergang zu Faktorringen, Oberringen, Quotientenkörpern etc. allgegenwärtig, und es ist natürlich zu hoffen, daß wir für oben erwähnte Objekte auf „naheliegende Weise" eine D-Struktur erhalten können. Das bedeutet immer, auf diesen Objekten lassen sich ebenfalls Derivationen $\partial_1, \ldots, \partial_m$ erklären, die dann auch die Vertauschungsregeln erfüllen. Die beteiligten Homomorphismen sollen weiterhin D-Homomorphismen sein.
Für den Fall einer Erweiterungsstruktur, also solch einer Struktur, in die wir uns unseren D-Ring bzw. D-Körper eingebettet denken können, wünschen wir uns

ausdrücklich Derivationen, die die Derivationen der kleineren Struktur fortsetzen und den Vertauschungsregeln genügen. Die zugehörige Einbettung soll ein D-Monomorphismus sein. Erst dann können wir von einer Fortsetzung der D-Struktur und von einer D-Erweiterungsstruktur sprechen. Es ist in diesen Fällen im Hinblick auf die modelltheoretischen Untersuchungen zusätzlich noch wichtig, Ergebnisse zur Eindeutigkeit der Fortsetzung zu erhalten.
Dazu ein Lemma, welches diese Frage für die Faktorisierung klärt.

Lemma 1.3.1 *Sei R' ein beliebiger Ring, R ein D-Ring und $\phi : R \to R'$ ein surjektiver Ringhomomorphismus, bei dem $ker\phi$ ein D-Ideal in R ist.*
Dann lassen sich partielle Derivationen $\partial'_1, \ldots, \partial'_m$ auf R' erklären, und ϕ ist ein D-Homomorphismus.

Beweis: ϕ ist surjektiv, also existiert f.a. $s \in R'$ ein Urbild $r \in R$ mit $\phi(r) = s$. Definiere jetzt für $1 \leq i \leq m$ Abbildungen auf R' durch:

$$\partial'_i : R' \to R' \qquad \text{mit} \qquad \partial'_i(\phi(r)) = \partial'_i s \overset{\text{def}}{=} \phi(\partial_i r) \ . \tag{1.3}$$

Falls die ∂'_i Derivationen sind, ist mit der Definition klar, daß ϕ D-Homomorphismus ist. Zuerst zeige wir die Unabhängigkeit von der Wahl des Urbildes: Seien dazu r_1 bzw. r_2 Urbilder in R von $s \in R'$, also $\phi(r_1) = s = \phi(r_2)$; wir wollen $\partial'_i(\phi(r_1)) = \partial'_i(\phi(r_2))$ erhalten. Es gilt $0 = \phi(r_1) - \phi(r_2) = \phi(r_1 - r_2)$. Daraus folgt $r_1 - r_2 \in ker\phi$ und somit $\partial_i(r_2) - \partial_i(r_2) = \partial_i(r_1 - r_2) \in ker\,\phi$, da $ker\phi$ D-Ideal ist. Das ergiebt nun:

$$0 = \phi(\partial_i(r_1) - \partial_i(r_2)) = \phi(\partial_i(r_1)) - \phi(\partial_i(r_2)) \overset{(1.3)}{=} \partial'_i(\phi(r_1)) - \partial'_i(\phi(r_2)) \ ,$$

also $\partial'_i(\phi(r_1)) = \partial'_i(\phi(r_2))$.
Im Folgenden gelte nun $s_1 = \phi(r_1)$, $s_2 = \phi(r_2)$. Zur Additivität:

$$\begin{aligned} \partial'_i(s_1 + s_2) &= \partial'_i(\phi(r_1) + \phi(r_2)) = \partial'_i(\phi(r_1 + r_2)) \overset{(1.3)}{=} \phi(\partial_i(r_1 + r_2)) \\ &= \phi(\partial_i(r_1) + \partial_i(r_2)) = \phi(\partial_i(r_1)) + \phi(\partial_i(r_2)) \overset{(1.3)}{=} \partial'_i s_1 + \partial'_i s_2 \ . \end{aligned}$$

Und zur Produktregel erhalten wir:

$$\begin{aligned} \partial'_i(s_1 s_2) &= \partial'_i(\phi(r_1)\phi(r_2)) = \partial'_i(\phi(r_1 r_2)) \overset{(1.3)}{=} \phi(\partial_i(r_1 r_2)) \\ &= \phi((\partial_i r_1) \cdot r_2 + r_1 \cdot (\partial_i r_2)) = \phi(\partial_i r_1)\phi(r_2) + \phi(r_1)\phi(\partial_i r_2) \\ &\overset{(1.3)}{=} (\partial'_i s_1)s_2 + s_1(\partial'_i s_2) \ . \end{aligned}$$

Die Abbildungen in (1.3) sind demnach Derivationen, nun muß noch überprüft werden, ob die Vertauschungsrelationen gelten:

$$\partial'_i\partial'_j s = \partial'_i\partial'_j(\phi(r)) = \partial'_i(\phi(\partial_j r)) = \phi(\partial_i\partial_j r) = \phi(\partial_j\partial_i r) = \partial'_j\partial'_i(s)$$

□

Wir wenden dieses Lemma nun auf die Situation an, in der wir einen D-Ring nach einem von seinen D-Idealen faktorisieren.

Korollar 1.3.2 *Sei $\mathfrak{A}$ D-Ideal eines D-Ringes R, dann lassen sich auf dem Faktorring partielle Derivationen $\partial_1, \ldots, \partial_m$ definieren, und der kanonische Homomorphismus ist ein D-Homomorphismus.*

Eine weitere wichtige Konstruktion ist die Lokalisierung eines Ringes bezüglich eines multiplikativ abgeschlossenen Systems $S \subset R$ mit $1 \in S$. Der Ring, der durch die Nennerhinzunahme entsteht, wird wie üblich mit $S^{-1}R$ bezeichnet, falls wir $R \setminus \{0\}$ als S wählen sprechen wir natürlich von $Quot(R)$, dem Quotientenkörper von R. Zur Frage der Fortsetzung der Dervationen können wir das folgende Ergebnis festhalten.

Satz 1.3.3 *Sei R ein D-Ring, S ein multiplikativ abgeschlossenes System und $R' = S^{-1}R$ die Lokalisierung von R nach S.*
Dann läßt sich jede Derivation ∂_i auf R eindeutig zu einer Derivation ∂_i' auf R' fortsetzen. Weiterhin erfüllen die Derivationen ∂_i' die Vertauschungsregeln.

Beweis: Um die Eindeutigkeit zu erkennen, nehmen wir an, daß ∂_i' und ∂_i^* zwei Fortsetzungen von ∂_i sind. Wie wir bereits in der Bemerkung 1.1.1 gesehen haben, müssen sowohl ∂_i', als auch ∂_i^* die Quotientenregel erfüllen, was aber nichts anderes besagt, als daß beide bereits durch die Werte von ∂_i auf R bestimmt und somit identisch sind.

Zum Beweis der Existenz benutzt man die Quotientenregel als Definition für die gesuchte Derivation. Für jedes $x \in R'$ existieren $a \in R$ und $s \in S$, mit $x = \frac{a}{s}$. Definiere für $1 \leq i \leq m$:

$$\partial_i' : R' \to R' \quad \text{und} \quad \partial_i' x \overset{\text{def}}{=} \frac{\partial_i a \cdot s - a \cdot \partial_i s}{s^2} .$$

Als erstes müssen wir uns wieder die Wohldefiniertheit überlegen, gelte dazu $x = \frac{\hat{a}}{\hat{s}}$ für obiges x und zwei weitere $\hat{a} \in R$, $\hat{s} \in S$. Damit rechnen wir $a\hat{s} = \hat{a}s$ aus (wir setzen ja immer Nullteilerfreiheit voraus), was wiederum $\partial_i(a\hat{s} - \hat{a}s) = 0$ f.a. ∂_i zur Folge hat. Wir berechnen:

$$\begin{aligned} \partial_i'(\frac{a}{s}) - \partial_i'(\frac{\hat{a}}{\hat{s}}) &= \partial_i'\left(\frac{a}{s} - \frac{\hat{a}}{\hat{s}}\right) = \partial_i'\left(\frac{a\hat{s} - \hat{a}s}{s\hat{s}}\right) \\ &= \frac{\partial_i(a\hat{s} - \hat{a}s) \cdot s\hat{s} - (a\hat{s} - \hat{a}s) \cdot \partial_i(s\hat{s})}{(s\hat{s})^2} = 0 . \end{aligned}$$

Nun müssen wir wieder die Additivität der Fortsetzung für zwei Quotienten $\frac{a_1}{s_1}$, $\frac{a_2}{s_2} \in R'$ nachweisen:

$$\partial_i'\left(\frac{a_1}{s_1} + \frac{a_2}{s_2}\right) = \partial_i'\left(\frac{a_1 s_2 + a_2 s_1}{s_1 s_2}\right)$$

Der Zähler der rechten Seite berechnet sich mit der Qutientenregel zu

$$\partial_i(a_1 s_2 + a_2 s_1) \cdot s_1 s_2 - (a_1 s_2 + a_2 s_1) \cdot \partial_i(s_1 s_2) .$$

Wenn wir diesen Term auflösen, gelangen wir zu den vier Summanden $\partial_i(a_1 s_2) \cdot s_1 s_2$, $\partial_i(a_2 s_1)\cdot s_1 s_2$, $-a_1 s_2 \cdot \partial_i(s_1 s_2)$ und $-a_2 s_1 \cdot \partial_i(s_1 s_2)$, die wir mit der Produktregel für ∂_i zu $\partial_i a_1 \cdot s_1 s_2^2 - a_1 s_2^2 \cdot \partial_i s_1 + \partial_i a_2 \cdot s_2 s_1^2 - a_2 s_1^2 \cdot \partial_i s_2$ aufaddieren, wobei wir die Summanden, die sich gegenseitig aufheben, bereits gekürzt haben. Wenn wir nun wieder den Nenner hinzunehmen, erhalten wir:

$$\frac{\partial_i a_1 \cdot s_1 s_2^2 - a_1 s_2^2 \cdot \partial_i s_1}{(s_1 s_2)^2} + \frac{\partial_i a_2 \cdot s_2 s_1^2 - a_2 s_1^2 \cdot \partial_i s_2}{(s_1 s_2)^2} = \partial_i'(\frac{a_1}{s_1}) + \partial_i'(\frac{a_2}{s_2}) \, .$$

Und zur Produktregel halten wir fest:

$$\partial_i' \left(\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} \right) = \partial_i' \left(\frac{a_1 a_2}{s_1 s_2} \right) = \frac{\partial_i(a_1 a_2) \cdot s_1 s_2 - a_1 a_2 \cdot \partial_i(s_1 s_2)}{(s_1 s_2)^2} \, ,$$

für den Zähler des letzten Bruches ergibt die Produktregel für ∂_i wieder vier Summanden $\partial_i a_1 \cdot a_2 s_1 s_2$, $a_1 \cdot \partial_i a_2 \cdot s_1 s_2$, $-a_1 a_2 \cdot \partial_i s_1 \cdot s_2$ und $-a_1 a_2 s_1 \cdot \partial_i s_2$. Diese fassen wir zu den zwei Summanden $(\partial_i a_1 \cdot s_1 - a_1 \cdot \partial_i s_2) \cdot s_2 a_2$ und $a_1 s_1 \cdot (\partial_i a_2 \cdot s_2 - a_2 \cdot \partial_i s_2)$ zusammen, was mit dem Hauptnenner $(s_1 s_2)^2$ ergibt:

$$\frac{\partial_i a_1 \cdot s_1 - a_1 \cdot \partial_i s_2}{s_1^2} \cdot \frac{s_2 a_2}{s_2^2} + \frac{a_1 s_1}{s_1^2} \cdot \frac{\partial_i a_2 \cdot s_2 - a_2 \cdot \partial_i s_2}{s_2^2} = \partial_i'(\frac{a_1}{s_1}) \cdot \frac{a_2}{s_2} + \frac{a_1}{s_1} \cdot \partial_i'(\frac{a_2}{s_2}) \, .$$

Wir müssen uns noch um die Vertauschungsregeln kümmern, aber wir erkennen durch direktes Nachrechnen, daß sich auch diese vererben.

$$\begin{aligned} \partial_i' \partial_j'(\frac{a}{s}) &= \partial_i' \left(\frac{\partial_j a \cdot s - a \cdot \partial_j s}{s^2} \right) \\ &= \frac{\partial_i(\partial_j a \cdot s - a \cdot \partial_j s) \cdot s^2}{s^4} - \frac{(\partial_j a \cdot s - a \cdot \partial_j s) \cdot \partial_i(s^2)}{s^4} \end{aligned}$$

Wir berechnen die zwei Summanden wieder getrennt zu:

$$\frac{\partial_i \partial_j a \cdot s}{s^2} + \frac{\partial_j a \cdot \partial_i s}{s^2} - \frac{\partial_i a \cdot \partial_j s}{s^2} - \frac{a \cdot \partial_i \partial_j s}{s^2} - \frac{2 \partial_j a \cdot \partial_i s}{s^2} + \frac{2a \cdot \partial_j s \cdot \partial_i s}{s^3} \, ,$$

was sich mit den Vertauschungsregeln für ∂_i, ∂_j zu

$$\frac{\partial_j \partial_i a \cdot s}{s^2} + \frac{\partial_i a \cdot \partial_j s}{s^2} - \frac{\partial_j a \cdot \partial_i s}{s^2} - \frac{a \cdot \partial_j \partial_i s}{s^2} - \frac{2 \partial_i a \cdot \partial_j s}{s^2} + \frac{2a \cdot \partial_i s \cdot \partial_j s}{s^3}$$

umformen läßt. Das ist aber nach einer entsprechenden Rechnung wie oben gerade $\partial_j' \partial_i'(\frac{a}{s})$.

Als Letztes sei noch daran erinnert, daß wir unseren Integritätsbereich R injektiv in den Erweiterungsring $S^{-1}R$ durch $\phi_S(a) \stackrel{\text{def}}{=} \frac{a}{1}$ einbetten können, wobei ϕ_S sogar ein D-Monomorphismus ist, denn mit $\partial_i 1 = 0$ folgt

$$\partial_i'(\phi_S(a)) = \partial_i'(\frac{a}{1}) = \frac{\partial_i a \cdot 1 - a \cdot \partial_i 1}{1} = \frac{\partial_i a}{1} = \phi_S(\partial_i a) \, .$$

□

Für den wichtigen Fall, daß wir $S = R \setminus \{0\}$ wählen, und so zum Quotientenkörper von R übergehen, halten wir nochmals ausdrücklich fest, daß dieser eine eindeutige D-Struktur trägt, die die von R fortsetzt.

1.4 Derivationen und Polynomringe

Als nächstes wollen wir Derivationen im Zusammenhang mit Polynomringen untersuchen. Wir erinnern daran, daß man auf $R[X]$ die sogenannte formale Derivation $\frac{\partial f}{\partial X}$ kennt, worunter wir die Derivation $\sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=1}^{n} k a_k X^{k-1}$ für ein $f \in R[X]$ verstehen. Diese wird uns an verschiedenen Stellen wieder begegnen.

Lemma 1.4.1 *Sei R ein D-Ring, $R' = R[(Y_j)_{j\in J}]$ ein Polynomring über R in den Unbestimmten Y_j. Es gilt:*

a) Jede Derivation ∂' von R', die eine Derivation ∂ von R fortsetzt, ist bereits durch die Werte ∂Y_j auf dem Erzeugendensystem eindeutig bestimmt.

b) Die Abbildung $f \mapsto f^{\partial_i}$ ist eine Derivation auf R', wobei f^{∂_i} das Polynom ist, was man aus f erhält, wenn man alle Koeffizienten durch ihre ∂_i-Ableitungen in R ersetzt.

c) Für eine beliebige Familie $(u_j)_{j\in J}$ von Elementen aus R' ist die Abbildung $d : R\{X\} \to R'$, $f \mapsto \sum_{j\in J} \frac{\partial f}{\partial Y_j} \cdot u_j$ eine Derivation auf R'. (Man beachte, daß die Summe für jedes f endlich ist!)

Beweis: Zu a) Angenommen, ∂' und $\bar{\partial}'$ seien zwei Fortsetzungen von ∂ mit $\partial' Y_j = \bar{\partial}' Y_j$ f.a. $j \in J$. Es ist mit Bemerkung 1.1.1 klar, daß $\partial' - \bar{\partial}'$ wieder eine Derivation auf R' ist. Wir wissen, daß $C_{\partial' - \bar{\partial}'} = \{a \in R' \mid \partial' - \bar{\partial}' a = 0\}$ — die Konstanten von R' bzgl. $\partial' - \bar{\partial}'$ — ein Unterring von R' ist, der jetzt R und $\{Y_j \mid j \in J\}$ enthält. Der kleinste Unterring von R', der R und das Erzeugendensystem enthält, ist aber R' selbst, damit gilt $\partial' - \bar{\partial}' = 0$ auf ganz R', d.h. $\partial' = \bar{\partial}'$.
Zu b) Seien $f = \sum_{\bar{\nu}\in\mathbb{N}^n} \alpha_{\bar{\nu}} Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n}$ und $g = \sum_{\bar{\mu}\in\mathbb{N}^m} \beta_{\bar{\mu}} Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m}$ zwei Polynome aus R'. Wir rechnen exemplarisch die Produktregel nach.

$$
\begin{aligned}
(fg)^{\partial_i} &= \sum\sum \partial_i(\alpha_{\bar{\nu}}\beta_{\bar{\mu}}) \cdot Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n} \cdot Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m} \\
&= \sum\sum (\partial_i\alpha_{\bar{\nu}} \cdot \beta_{\bar{\mu}} + \alpha_{\bar{\nu}} \cdot \partial_i\beta_{\bar{\mu}}) \cdot Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n} \cdot Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m} \\
&= \sum\sum \partial_i\alpha_{\bar{\nu}} \cdot \beta_{\bar{\mu}} \cdot Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n} \cdot Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m} \\
&\quad + \sum\sum \alpha_{\bar{\nu}} \cdot \partial_i\beta_{\bar{\mu}} \cdot Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n} \cdot Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m} \\
&= \sum \partial_i\alpha_{\bar{\nu}} Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n} \cdot \sum \beta_{\bar{\mu}} Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m} \\
&\quad + \sum \alpha_{\bar{\nu}} Y_{k_1}^{\nu_1} \cdots Y_{k_n}^{\nu_n} \cdot \sum \partial_i\beta_{\bar{\mu}} Y_{j_1}^{\mu_1} \cdots Y_{j_m}^{\mu_m} \\
&= f^{\partial_i} \cdot g + f \cdot g^{\partial_i} .
\end{aligned}
$$

Zu c) Wir wissen ja bereits, daß für jedes j die Abbildung $f \mapsto \frac{\partial f}{\partial Y_j}$ eine Derivation ist. In einem $f \in R'$ kommen jeweils immer nur endlich viele Y_j vor, die Abbildung $f \mapsto \sum_{j\in J} \frac{\partial f}{\partial Y_j}$ ist demnach nur eine endliche Summe von Ableitungen, die somit nach Bemerkung 1.1.1 e) additiv ist und der Produktregel genügt. Die Multiplikation mit den u_j ändert nun nichts wesentliches mehr,

$$\begin{aligned}
d(fg) &= \sum_{j\in J} \frac{\partial(fg)}{\partial Y_j}\cdot u_j = \sum_{i_1,\ldots,i_n} \frac{\partial(fg)}{\partial Y_{i_k}}\cdot u_{i_k} \\
&= \left(\sum_{i_1,\ldots,i_n} \frac{\partial f}{\partial Y_{i_k}}\cdot g + f\cdot \sum_{i_1,\ldots,i_n} \frac{\partial g}{\partial Y_{i_k}}\right)\cdot u_{i_k} \\
&= \left(\sum_{j\in J} \frac{\partial f}{\partial Y_{i_j}}\cdot u_j\right)\cdot g + f\cdot \left(\sum_{j\in J} \frac{\partial f}{\partial Y_{i_j}}\cdot u_j\right) \\
&= d(f)g + fd(g)\ .
\end{aligned}$$

Die Additivität ist natürlich analog nachzuvollziehen. □

1.5 Separable Körpererweiterungen

Es wird später für uns von Bedeutung sein, die separablen Körpererweiterungen genauer zu kennen. Bekanntlich stehen ja die über einem Körper K separable Elemente in einem gewissen Zusammenhang mit der formalen Derivation $\frac{\partial f}{\partial X}$ des Polynomringes $K[X]$. Diese formale Derivation wird sich als bedeutsam für die Möglichkeit der Forsetzung einer beliebigen Derivationen auf einen separablen Erweiterungskörper erweisen. Weiterhin ist für uns noch wichtig daran zu erinnern, daß wir ausschließlich mit Körpern der Charakteristik 0 arbeiten, für die bekanntlich jede algebraische Erweiterung bereits separabel ist. Es klärt sich somit insbesondere auch die Fortsetzungsfrage auf den algebraischen Abschluß eines D-Körpers.

Wir beginnen, die Situation für ein einzelnes separables Element zu untersuchen.

Lemma 1.5.1 *K sei ein D-Körper. Weiterhin sei $K(\alpha) \supset K$ eine algebraische Körpererweiterung mit α separabel über K.*
Dann existiert für jede der Derivationen ∂_i auf K eine eindeutige Fortsetzung ∂_i' auf $K(\alpha)$.

Beweis: Da α separabel ist, existiert das dazugehörige Minimalpolynom f mit $f(\alpha) = 0$. Dieses f ist irreduzibel, erfüllt deswegen bekanntlich $\frac{\partial f}{\partial X}(\alpha) \neq 0$. Eine beliebige Derivation d auf $K(\alpha)$ muß zwangsläufig folgende Gleichungen nach der erfüllen:

$$0 = d(f(\alpha)) = f^d(\alpha) + \frac{\partial f}{\partial X}(\alpha)\cdot d\alpha \qquad \text{gdw.} \qquad d\alpha = -\frac{f^d(\alpha)}{\frac{\partial f}{\partial X}(\alpha)} \tag{1.4}$$

Ist d eine Fortsetzung von ∂_i, dann ist der Wert von d an der Stelle α eindeutig durch f und die Koeffizienten von f^d bestimmt, diese Koeffizienten sind aber wiederum eindeutig durch $d\lceil_K = \partial_i$ gegeben. Demnach müssen zwei Fortsetzungen d und $\bar{d}$ von ∂_i auf K und an der Stelle α übereinstimmen. Wir können wieder $K(\alpha) \subset C_{d-\bar{d}}$, damit $d = \bar{d}$ schließen.

Natürlich benutzt man jetzt obige Gleichung 1.4 als Definition von $\partial_i'\alpha$, ebenso ist die Setzung $\partial_i' b \stackrel{\text{def}}{=} \partial_i b$ für $b \in K$ klar. Damit erklären wir die ganze Fortsetzung ∂_i'. Wir wissen, daß $K(\alpha) = Quot(K[\alpha])$ und $K[\alpha] = \{g(\alpha) \mid g(X) \in K[X]\}$ gilt, also setzen wir

$$\partial_i'(g(\alpha)) \stackrel{\text{def}}{=} g^{\partial_i'}(\alpha) + \frac{\partial g}{\partial X}(\alpha) \cdot \partial_i'\alpha, \quad \text{dann} \quad \partial_i'(\frac{g}{h}(\alpha)) \stackrel{\text{def}}{=} \frac{(\partial_i' g \cdot h)(\alpha) - (g \cdot \partial_i' h)(\alpha)}{h^2(\alpha)}$$

für $g(X), h(X) \in K[X]$ und $h(\alpha) \neq 0$. Es muß überprüft werden, ob wir nun eine Derivation auf $K[\alpha]$ vorliegen haben:

$$\partial_i'(h(\alpha) + g(\alpha)) = \partial_i'((h+g)(\alpha)) = (h+g)^{\partial_i'}(\alpha) + \frac{\partial(h+g)}{\partial X}(\alpha) \cdot \partial_i'\alpha \,.$$

Daß der zweite Summand zerlegt werden kann, ist klar, beim ersten beachte man, daß die Koeffizienten von $h+g$ aus K kommen, deren Werte unter der Ableitung ∂_i' mit ihren Ableitungen unter ∂_i übereinstimmen, wodurch wir die Additivität durch die von ∂_i erhalten. Wir können $(h+g)^{\partial_i'}(\alpha) = h^{\partial_i'}(\alpha) + g^{\partial_i'}(\alpha)$ folgern, damit:

$$\begin{aligned} \partial_i'(h(\alpha) + g(\alpha)) &= h^{\partial_i'}(\alpha) + \frac{\partial h}{\partial X}(\alpha) \cdot \partial_i'\alpha + g^{\partial_i'}(\alpha) + \frac{\partial g}{\partial X}(\alpha) \cdot \partial_i'\alpha \\ &= \partial_i'(h(\alpha)) + \partial_i'(g(\alpha)) \,. \end{aligned}$$

Die Produktregel rechnet man genauso nach.
Jetzt ist klar, daß zusammen mit dem zweiten Teil der Definition, die ja nichts anderes als die Quotientenregel beinhaltet, eine Derivation auf $K(\alpha)$ erklärt ist, da wir bereits wissen, wie wir Derivationen auf den Quotientenkörper fortsetzen müssen. □

Wir führen nun den Fall einer beliebigen separablen Körpererweiterung auf dieses Lemma zurück, indem wir ausnutzen, daß sich $L \supset K$ separabel als $L = K((\alpha_j)_{j \in J})$, mit α_j separabel über K f.a. j, schreiben läßt.

Es ist vorteilhaft, vorher noch den **Kommutator** zweier Derivationen ∂_i und ∂_j einzuführen. Darunter verstehen wir die Abbildung $[\partial_i, \partial_j] \stackrel{\text{def}}{=} \partial_i\partial_j - \partial_j\partial_i$. Für uns heißt das nun, daß wir äquivalent zur Aussage ∂_i, ∂_j erfüllen die Vertauschungsregeln, auch die Gleichung $[\partial_i, \partial_j] = 0$ prüfen können.

Lemma 1.5.2 *Für zwei beliebige Derivationen von R ist der Kommutator $[\partial_i, \partial_j]$ eine Derivation auf R.*

Beweis: Wir berechnen

$$\begin{aligned}(\partial_i\partial_j - \partial_j\partial_i)(a+b) &= \partial_i\partial_j(a+b) - \partial_j\partial_i(a+b)\\ &= \partial_i\partial_j a + \partial_i\partial_j b - \partial_j\partial_i a - \partial_j\partial_i b\\ &= \partial_i\partial_j a - \partial_j\partial_i a + \partial_i\partial_j b - \partial_j\partial_i b\\ &= (\partial_i\partial_j - \partial_j\partial_i)(a) + (\partial_i\partial_j - \partial_j\partial_i)(b)\,,\end{aligned}$$

die Additivität ist somit erfüllt. Die Produktregel überträgt sich ebenfalls:

$$\begin{aligned}(\partial_i\partial_j - \partial_j\partial_i)(ab) &= \partial_i\partial_j(ab) - \partial_j\partial_i(ab)\\ &= \partial_i(\partial_j a\cdot b + a\cdot\partial_j b) - (\partial_j(\partial_i a\cdot b + a\cdot\partial_i b))\\ &= \partial_i\partial_j a\cdot b + \partial_j a\cdot\partial_i b + \partial_i a\cdot\partial_j b + a\cdot\partial_i\partial_j b\\ &\quad -(\partial_j\partial_i a\cdot b + \partial_i a\cdot\partial_j b + \partial_j a\cdot\partial_i b + a\cdot\partial_j\partial_i b)\\ &= (\partial_i\partial_j a - \partial_j\partial_i a)\cdot b + a\cdot(\partial_i\partial_j b - \partial_j\partial_i b)\\ &= (\partial_i\partial_j - \partial_j\partial_i)(a)\cdot b + a\cdot(\partial_i\partial_j - \partial_j\partial_i)(b)\,.\end{aligned}$$

□

<u>**Lemma**</u> **1.5.3** *K sei ein D-Körper, $L \supset K$ eine separable algebraische Körpererweiterung.*
Dann existiert für jede der Derivationen ∂_i auf K eine eindeutige Fortsetzung ∂_i' auf L. Die Derivationen ∂_i^L erfüllen ebenfalls die Vertauschungsregeln.

Beweis: Wir betrachten eine feste Derivation ∂_i, mit ∂_i^F meinen wir immer eine Fortsetzung auf ein $F \supset K$.
Seien ∂_i^L, $\bar{\partial}_i^L$ zwei Fortsetzungen von ∂_i auf L. Wir schließen wieder für den Konstantenkörper $C_{\partial_i^L - \bar{\partial}_i^L}$, daß dieser K und auch $(\alpha_j)_{j\in J}$ umfaßt. Denn die Werte der Fortsetzungen für jedes α_j sind, wie bereits im Lemma 1.5.1 überlegt, eindeutig durch ∂_i und das Minimalpolynom von α_j bestimmt. Damit erhalten wir wieder $C_{\partial_i^L - \bar{\partial}_i^L} = K((\alpha_j)_{j\in J})$, d.h. $\partial_i^L = \bar{\partial}_i^L$.
Sei nun $\{\alpha_{i_1}, \ldots, \alpha_{i_n}\}$ eine endliche Teilmenge von $\{\alpha_j \mid j \in J\}$. Für die Körpererweiterung $K' = K(\alpha_{i_1}, \ldots, \alpha_{i_n}) \supset K$ wissen wir, daß sie endlich und separabel ist. Nach dem Satz vom primitiven Element existiert ein über K separables β, mit $K' = K(\beta)$. Mit Lemma 1.5.1 existiert für jede Derivation ∂_i von K demnach eine eindeutige Fortsetzung auf jeden Erweiterungskörper der Art K'.
Seien zwei endliche Teilmengen mit $A_1 \subset A_2$ aus $\{\alpha_j \mid j \in J\}$ gegeben, dann gilt für die Fortsetzungen $\partial_i^{K_2}$ auf $K_2 = K(A_2)$ und $\partial_i^{K_1}$ auf $K_1 = K(A_1)$ sogar $\partial_i^{K_2}\restriction_{K_1} = \partial_i^{K_1}$. Denn angenommen, es würde $\partial_i^{K_2}\restriction_{K_1} \neq \partial_i^{K_1}$ gelten, dann könnte man $\partial_i^{K_1}$ auf K_2 fortsetzen, da K_2 eine endliche separable Erweiterung von K_1 ist, die aber nicht mit $\partial_i^{K_2}$ übereinstimmen würde. Es gäbe zwei verschiedene Fortsetzungen von ∂_i auf K_2, ein Widerspruch!

Wenn ein Element $b \in L$ in zwei Körpern der Gestalt $K_1 = K(A_1)$ und $K_2 = K(A_2)$ enthalten ist, wobei A_1, A_2 jetzt zwei beliebige endliche Teilmengen von $\{\alpha_j \mid j \in J\}$ sein sollen, dann stimmt $\partial_i^{K_1}(b)$ mit $\partial_i^{K_2}(b)$ überein, da wir ja $K_3 = K(A_1 \cup A_2)$ betrachten können und mit dem Obigen wissen, daß einerseits $\partial_i^{K_1}(b) = \partial_i^{K_3}(b)$, und andererseits $\partial_i^{K_2}(b) = \partial_i^{K_3}(b)$ gelten muß, und $\partial_i^{K_3}$ wiederum eindeutig ist.
Da ein Element $b \in L$ immer in einem Körper $K' = K(\alpha_{i_1}, \ldots, \alpha_{i_n})$ enthalten ist, können wir eine Abbildung ∂_i^L auf L definieren, indem wir $\partial_i^L(b) \stackrel{\text{def}}{=} \partial_i^{K'}(b)$ setzen. Das ist wohldefiniert, da es, wie wir festgestellt haben, unabhängig von der endlichen Menge $\{\alpha_{i_1}, \ldots, \alpha_{i_n}\}$ ist. Die Regeln für eine Derivation übertragen sich unmittelbar: Für $a, b \in L$ können wir ein $K' = K(\alpha_{i_1}, \ldots, \alpha_{i_n})$ mit $a, b \in K'$ finden, $\partial_i^L(a+b) = \partial_i^{K'}(a+b)$, $\partial_i^L(ab) = \partial_i^{K'}(ab)$, weil $\partial_i^{K'}$ bereits eine Derivation ist.
Es bleibt, die Vertauschungsregel für zwei beliebige Fortsetzungen $\partial_i^L, \partial_j^L$ nachzuweisen. Dafür benutzen wir den Kommutator $[\partial_i, \partial_j]$, der nach 1.5.2 eine Derviation auf K und nach Voraussetzung auf K die triviale Derivation ist. Diese wird aber einerseits von der trivialen Derivation auf L fortgesetzt, also gilt $[\partial_i, \partial_j]^L = 0$. Andererseits setzt natürlich auch die Derivation $[\partial_i^L, \partial_j^L]$ auf L $[\partial_i, \partial_j]$ fort, wir haben damit wegen der Eindeutigkeit der Fortsetzung:

$$[\partial_i^L, \partial_j^L] = \partial_i^L \partial_j^L - \partial_j^L \partial_i^L = [\partial_i, \partial_j]^L = 0 ,$$

d.h. die Vertauschungsregeln. $\square$

Bemerkung 1.5.4 *Für eine D-Körpererweiterung $L \supset K$ und $\alpha \in L$ separabel über K gilt: $K\langle\alpha\rangle = K(\alpha)$.*

Kapitel 2

Der D-Polynomring

In diesem Kapitel wollen wir den D-Polynomring erklären und danach die zentralen technischen Hilfsmittel bereitstellen, die nötig sein werden, um die radikalen bzw. primen D-Ideale zu untersuchen. Wir gehen wieder aus von einem Ring R und Derivationen $\partial_1, \ldots, \partial_m$, bezüglich derer R ein D-Ring ist. Als Referenz sei wieder auf [KOLCHIN 1] verwiesen.

2.1 Die Menge der Ableitungsoperatoren Θ

Wir führen nun die Ableitungsoperatoren ein, die für uns ein bequemes Hilfsmittel sein werden, Eigenschaften von Polynomen zu beschreiben. Die Elemente der Menge $\Theta \stackrel{\text{def}}{=} \{\partial_1^{\nu_1} \cdots \partial_m^{\nu_m} \mid \nu_1, \ldots, \nu_m \in \mathbb{N}\}$ heißen **Ableitungsoperatoren** des D-Ringes R. Die Vertauschungsrelationen der ∂_i setzen wir nun auf diese Menge fort, indem wir eine *kommutative* Multiplikation durch $(\partial_1^{\nu_1} \cdots \partial_m^{\nu_m}) \cdot (\partial_1^{\mu_1} \cdots \partial_m^{\mu_m}) \stackrel{\text{def}}{=} \partial_1^{(\nu_1+\mu_1)} \cdots \partial_m^{(\nu_m+\mu_m)}$ erklären. Es ist zu beachten, daß wir für die Exponenten auch die Werte 0 zulassen, wir bezeichnen dann $1_\Theta \stackrel{\text{def}}{=} \partial_1^0 \cdots \partial_m^0$ als das Eins-Element von Θ bezüglich obiger Multiplikation. Man erkennt also in Θ das von $\partial_1, \ldots, \partial_m$ erzeugte freie kommutative Monoid mit 1.

Weiter definieren wir ein Maß für die Elemente von Θ, das angibt, „wie oft ein Operator insgesamt ableitet".

Definition 3 *Sei $\theta = \partial_1^{\nu_1} \cdots \partial_m^{\nu_m}$ ein Element aus Θ.*
Dann heißt die natürliche Zahl $ord(\theta) \stackrel{\text{def}}{=} \sum_{i=1}^{m} \nu_i$ die **Ordnung** *von θ.*

Nun ist bekannt, daß wir eine assoziative Operation $*$ des ganzen Monoids Θ auf dem Ring R erhalten, wenn wir diese für das Erzeugendensystem erklären. Dafür übernehmen wir aber gerade die Wirkungsweise der ∂_i als Abbildungen von R nach R. Die 1 muß natürlich als Identität operieren.

Definition 4 *Die Abbildung* $*: \Theta \times R \to R$ *ist gegeben durch:*

$$1_\Theta * a \stackrel{\text{def}}{=} a \quad \text{f.a. } a \in R$$
$$\partial_j * a \stackrel{\text{def}}{=} \partial_j(a) \quad \text{f.a. } a \in R\,.$$

Durch die assoziative Eigenschaft von $*$, d.h. $(\theta_1 \cdot \theta_2) * a = \theta_1 * (\theta_2 * a)$ für beliebeiges $a \in R$ und $\theta_1, \theta_2 \in \Theta$, ist es gerechtfertigt, im weiteren immer nur $\theta_1\theta_2 a$ anstatt $(\theta_1 \cdot \theta_2) * a = \theta_1 * (\theta_2 * a)$ zu schreiben. Zur Sprachkonvention sei gesagt, daß wir ein Element θa aus R eine **echte Ableitung** von a aus R nennen, falls $ord(\theta) > 0$ gilt.
Mit Hilfe von Θ lassen sich bereits bekannte Objekte auch so ausdrücken:

Bemerkung 2.1.1 *a) Sei* $A \subset R$*, dann gilt:* $\langle A \rangle = (\Theta A)$*, das von* A *erzeugte D-Ideal stimmt mit dem von* ΘA *erzeugten (algebraischen) Ideal überein.*

b) Sei $L \supset K$ *eine D-Körpererweiterung,* $\alpha \in L$*. Dann gilt:* $K\{\alpha\} = K[\Theta\alpha]$ *und* $K\langle\alpha\rangle = K(\Theta\alpha)$*.*

2.2 Die Definition des D-Polynomringes

Wir wollen jetzt den Polynomring in einer *differentiell Unbestimmten* über R einführen.

Dazu betrachten wir die Familie $(\theta X)_{\theta\in\Theta}$, von der wir annehmen, daß keines ihrer Elemente bereits in R vorkommt. Damit sind die θX algebraisch Unbestimmte über R. Nun betrachten wir den algebraischen Polynomring über R in diesen Unbestimmten und definieren $R\{X\} \stackrel{\text{def}}{=} R[(\theta X)_{\theta\in\Theta}]$. Wir können jetzt auf $R\{X\}$ partielle Derivationen $\bar\partial_1, \ldots, \bar\partial_m$ erklären, die die auf R gegebenen fortsetzen. Dazu also für $1 \le j \le m$:

$$\bar\partial_j(f) \stackrel{\text{def}}{=} \partial_j f \quad \text{für} \quad f \in R \qquad \text{und} \qquad \bar\partial_j(\theta X) \stackrel{\text{def}}{=} \partial_j\theta X \quad \text{für} \quad \theta \in \Theta\,.$$

Wenn wir nun das Lemma 1.4.1 anwenden, wobei in unserem Fall die Familie der Unbestimmten ja $(\theta X)_{\theta\in\Theta}$ ist, und wir für die Familie der Elemente $(u_j)_{j\in J}$ die Familie $(\partial_j\theta X)_{\theta\in\Theta}$ nehmen, wissen wir, daß wir durch $f \mapsto f^{\partial_j} + \sum_{\theta\in\Theta} \frac{\partial f}{\partial\theta X} \cdot \partial_j\theta X$ eine Summe zweier Ableitungen auf $R\{X\}$ erklärt haben. Nach Bemerkung 1.1.1 ist die Summe selbst wieder Ableitung, sie setzt ∂_j von R fort, und ist gemäß der Definition auf dem Erzeugendensystem $(\theta X)_{\theta\in\Theta}$ als Fortsetzung eindeutig bestimmt (Lemma 1.4.1).

Weiterhin wissen wir wieder, daß $\bar\partial_i\bar\partial_j - \bar\partial_j\bar\partial_i$ natürlich $[\partial_i, \partial_j] = 0$ fortsetzt, damit wegen der Eindeutigkeit $[\bar\partial_i, \bar\partial_j] = \bar\partial_i\bar\partial_j - \bar\partial_j\bar\partial_i = 0$ gelten muß, also die Ableitungen $\bar\partial_j$ die Vertauschungsregeln erfüllen.

Somit haben wir auf kanonische Weise eine Fortsetzung der D-Struktur auf $R\{X\}$ gewonnen. Um aber eine vollständige Analogie zum algebraischen Polynomring zu erhalten, müssen wir noch klären, was es heißt, ein Element für die D-Unbestimmte X im „D-Sinne“ einzusetzen.

Satz 2.2.1 (Universelle Eigenschaft des D-Polynomringes)
Sei R D-Ring und $R\{X\}$ der D-Polynomring in einer differentiell Unbestimmten über R, S sei ein weiterer D-Ring und $\phi : R \to S$ ein D-Homomorphismus. Weiter sei α ein Element aus S.
Dann gibt es genau einen D-Homomorphismus $\Phi : R\{X\} \to S$ mit $\Phi(X) = \alpha$ und $\phi = \Phi \circ \iota$, wobei ι die Inklusion $R \overset{\iota}{\hookrightarrow} R\{X\}$ bezeichnen soll.

Beweis: Die Aussage des Satzes erhält man dadurch, daß sich die universelle Eigenschaft des algebraischen Polynomringes in den unendlich vielen Unbestimmten $(\theta X)_{\theta\in\Theta}$ überträgt. Für die Familie $(\theta\alpha)_{\theta\in\Theta}$ von Elementen aus S gibt es genau einen Homomorphismus $\Phi : R[(\theta X)_{\theta\in\Theta}] \to S$ mit $\Phi(\theta X) = \theta\alpha$ (insbesondere $\Phi(X) = \alpha$). Jeder weitere D-Homomorphismus Ψ mit $\Psi(X) = \alpha$ muß natürlich auch $\Psi(\theta X) = \theta\Psi(X) = \theta\alpha$ erfüllen, also mit Φ übereinstimmen.
Weil für das Erzeugendensystem ja $\Phi(\partial_i\theta X) = \partial_i\Phi(\theta X)$ und $\Phi(\partial_i a) = \phi(\partial_i a) = \partial_i\phi(a) = \partial_i\Phi(a)$ für $a \in R$ gilt, da ϕ mit den ∂_i verträglich ist, folgt wegen der Homomorphismuseigenschaften von Φ für alle $f \in R\{X\}$: $\Phi(\partial_i f) = \partial_i\Phi(f)$. $\square$

Es sei sofort darauf hingewiesen, daß wir für ein D-Polynom f immer zwei mögliche Auffassungen haben. Erstens die „rein Algebraische“, nach der ein Polynom f endlich viele algebraische Unbestimmte enthält, die unabhängig voneinander sind und mit θX bezeichnet werden. Zweitens die eigentlich „D-Algebraische“, nach der die Unbestimmten nicht unabhängig voneinander sind, sondern als Ableitungen von X gekoppelt sind. Wir können dann ein Ringelement nur für X frei einsetzen, für die restlichen algebraischen Unbestimmten müssen wir die passenden Ableitungen wählen.

Wir werden von nun an die algebraischen Unbestimmten $(\theta X)_{\theta\in\Theta}$, die wir in obiger Definition als Ableitungen der D-Unbestimmten X festgelegt haben, naheliegender Weise auch mit **X-Ableitung** bezeichnen. Für X-Ableitungen wählen wir in der Regel die kleinen Buchstaben u, v, w.

2.3 X-Ableitungen und Höhe der D-Polynome

Nun müssen wir einige technische Hilfsmittel zur Untersuchung des Polynomringes bereitstellen. Unser Ziel ist es, den Polynomring in einer „geeigneten Weise“ zu ordnen. Wir beginnen mit den X-Ableitungen.

Definition 5 *Seien $\theta_1, \theta_2 \in \Theta$ mit $\theta_1 = \partial_1^{\nu_1} \cdots \partial_j^{\nu_m}$ und $\theta_2 = \partial_1^{\mu_1} \cdots \partial_j^{\mu_m}$ gegeben. Wir ordnen den X-Ableitungen $\theta_1 X$ und $\theta_2 X$ jeweils Tupel natürlicher Zahlen zu, $\theta_1 X \leftrightsquigarrow (\sum_{j=1}^m \nu_j, \nu_1, \ldots, \nu_m)$ und $\theta_2 X \leftrightsquigarrow (\sum_{j=1}^m \mu_j, \mu_1, \ldots, \mu_m)$.*
Wir sagen, die X-Ableitung $\theta_1 X$ hat **kleinere Höhe** *als $\theta_2 X$* (kurz $\theta_1 X \ll \theta_2 X$), *falls*
$(\sum_{j=1}^m \nu_j, \nu_1, \ldots, \nu_m) < (\sum_{j=1}^m \mu_j, \mu_1, \ldots, \mu_m)$ gilt in der lexikographischen Ordnung von $\mathbb{N}^{m+1}$.

Für $\theta_1 X \ll \theta_2 X$ schreiben wir auch $\theta_2 X$ ist **höher** als $\theta_1 X$. Man beachte an der Definition, daß wir in der ersten Komponente der Tupel eine Summe, genauer die Ordnung von θ geschrieben haben. Dadurch erreichen wir, daß ein θX nur endlich viele Vorgänger bzgl. $\ll$ haben kann. Denn es kann nur endlich viele Elemente geben, die unter θX liegen und die gleiche Ordnung wie θ haben, da sich nur endlich viele natürliche Zahlen zu $ord(\theta)$ aufaddieren lassen. Weiterhin gibt es nur endlich viele $n \in \mathbb{N}$, mit $n < ord(\theta)$, wozu es wieder nur endlich viele X-Ableitungen $\theta' X$ geben kann, mit $ord(\theta') = n$.
Es ist außerdem klar, daß sich die Eigenschaften einer Wohlordnung vererben.

Bemerkung 2.3.1 *Die Relation $\ll$ ist eine Wohlordnung auf der Menge der X-Ableitungen $\{\theta X \mid \theta \in \Theta\}$, die isomorph ist zur Ordnung von $\mathbb{N}$.*

Wenn wir jetzt den D-Polynomring betrachten, können wir ohne Einschränkung annehmen, daß $R\{X\} = R[(\theta_i X)_{i \in \mathbb{N}}]$ mit $\theta_i X \ll \theta_j X$ für $i < j$ gilt. Da in endlich vielen D-Polynomen nur endlich viele X-Ableitungen echt auftreten (mit Koeffizienten ungleich Null), können wir uns für Rechnungen mit endlich vielen Polynomen auf einen Polynomring $R[X, \ldots, \theta X]$ zurückziehen, wobei θX die höchste in den Polynomen auftretende X-Ableitung ist. Diese Vorstellung wird an verschiedenen Stellen für uns von Bedeutung sein.

Nun nutzen wir die $\ll$-Ordnung der X-Ableitungen aus, um die D-Polynome genauer zu untersuchen. Dazu betrachten wir die endlich vielen in einem D-Polynom auftretenden X-Ableitungen. Unter diesen existiert genau eine, die höher ist als alle übrigen. Wir bezeichnen sie mit u_f und können jetzt das D-Polynom f als Polynom in u_f auffassen, d.h. $f = \sum_{k=0}^{n} I_k u_f^k$, wobei $I_n \neq 0$ gelten soll. Die I_k sind ebenfalls D-Polynome, die aber nur noch X-Ableitungen kleinerer Höhe als u_f enthalten. Falls g ein weiteres Polynom ist, soll $grad_{u_f}(g)$ die höchste Potenz angeben, in der u_f in g echt auftritt. Wir führen jetzt folgende Begriffe ein.

Definition 6 *Sei $f \in R\{X\} \setminus R$, also ein nicht-konstantes D-Polynom.*

1. *Die höchste in f echt auftretende X-Ableitung heißt* **Leitableitung** *von f, sie wird mit u_f bezeichnet.*

2. *Der zur höchsten Potenz von u_f gehörende (Polynom-) Koeffizient I_n heißt* **Leitterm** *von f.*

3. *Das Polynom $S_f \stackrel{\text{def}}{=} \frac{\partial f}{\partial u_f} = \sum_{k=1}^{n} k I_k u_f^{k-1}$ heißt der* **Separant** *von f.*

Diese Begriffe sind für den weiteren Text von zentraler Bedeutung. Mit Hilfe der Leitableitung eines Polynomes läßt sich nun die Ordnung der X-Ableitungen auf den Polynomring erweitern.

Definition 7 (Höhe der Polynome) *Gegeben seien zwei D-Polynome g und f.*

1. *Wir sagen, daß g* **kleinere Höhe** *als f hat, falls gilt:*
   a) *$g \in R$ und $f \in R\{X\} \setminus R$, dann hat g kleinere Höhe als f.*
   b) *$g, f \in R\{X\} \setminus R$ und für die Leitableitungen gilt $u_g \ll u_f$ (in der Ordnung der X-Ableitungen), dann hat g kleinere Höhe als f.*
   c) *$g, f \in R\{X\} \setminus R$ und für die Leitableitungen gilt $u_g = u_f$ und $grad_{u_f}(g) < grad_{u_f}(f)$, dann hat g kleinere Höhe als f.*
2. *f und g haben* **dieselbe Höhe**, *falls gilt, daß g nicht kleinere Höhe als f und f nicht kleinere Höhe als g hat.*

Notation: Für g kleinere Höhe als f benutzen wir wieder die Kurzform $g \ll f$ und sagen ebenfalls f ist **höher** als g, was gerechtfertigt ist, da im Falle von $g = \theta X$ und $f = \theta' X$ natürlich f höher ist als g (aufgefaßt als D-Polynome), wenn f höher ist als g im Sinne der X-Ableitungen. Für die Relation „g hat kleinere oder gleiche Höhe wie f“ benutzen wir die Schreibweise $g \leqslant\!\!\!\leqslant f$.

Aus den Definitionen folgt natürlich die Reflexivität und die Transitivität von $\leqslant\!\!\!\leqslant$, man beachte aber, daß ein D-Polynom unendlich viele $\leqslant\!\!\!\leqslant$-Vorgänger besitzen kann, und daß aus $f \leqslant\!\!\!\leqslant g$ und $g \leqslant\!\!\!\leqslant f$ *nicht* $f = g$ folgt. Wenn wir eine nichtleere Menge von D-Polynomem haben, enthält diese (mindestens) ein $\leqslant\!\!\!\leqslant$-minimales Element. Das ist ein konstantes Polynom, falls solche enthalten sind. Gibt es keine konstanten, betrachten wir die Menge der Leitableitungen der D-Polynome dieser Menge, unter denen es eine eindeutige $\ll$-minimale, etwa v geben muß. Von den D-Polynomen, die dieses v als Leitableitung besitzen, gibt es dann welche, in denen v im kleinsten Grad auftritt, diese sind dann $\leqslant\!\!\!\leqslant$-minimal.

Bemerkung 2.3.2 *a) Die Relation $\leqslant\!\!\!\leqslant$ ist eine reflexive, transitive Relation auf der Menge der D-Polynome. Jede nichtleere Menge von D-Polynomen enthält mindestens ein bzgl. $\leqslant\!\!\!\leqslant$ minimales Element.*

b) Für $f \in R\{X\} \setminus R$ gilt $S_f \ll f$ und $I_f \ll f$.

Der Einfachheit halber sprechen wir von den D-Polynomen nur als Polynomen, wenn keine Zweideutigkeiten zu befürchten sind. An den Stellen, an denen wir die Vorstellung benutzen, daß ein Polynom $f = f(X, \ldots, \theta X)$ ein Polynom in mehreren algebraischen Unbestimmten ist, werden wir das ausdrücklich bemerken. Genauso sprechen wir einfach von Nullstellen, wenn wir meinen, daß ein α mit seinen entsprechenden Ableitungen eingesetzt für die jeweilige X-Ableitungen ein Polynom zu Null macht.

Wir wollen jetzt ein Lemma angeben, was uns anzeigt, wie sich eine Ableitung eines Polynoms $f \in R\{X\} \setminus R$ darstellen läßt, insbesondere werden wir sehen, daß die Leitableitung von θf gerade θu_f ist.

Lemma 2.3.3 *Sei $f \in R\{X\} \setminus R$, $f = \sum_{j=0}^{d} I_j u_f^j$, und $\theta \in \Theta$ mit $ord(\theta) > 0$. Dann existiert ein $T \in R\{X\}$ mit $\theta f = S_f \theta u_f + T$ und $T \ll \theta u_f$.*

Beweis: Der Beweis erfolgt durch Induktion über $k = ord(\theta)$.
$\underline{k = ord(\theta) = 1}$, d.h. $\theta = \partial_i$ für ein i mit $1 \leq i \leq m$. Wir berechnen:

$$\begin{aligned} \partial_i f &= \partial_i(\sum_{j=0}^{d} I_j \cdot u_f^j) = \sum_{j=0}^{d} j I_j \cdot u_f^{j-1} \cdot \partial_i u_f + \sum_{j=0}^{d} \partial_i I_j \cdot u_f^j \\ &= S_f \cdot \partial_i u_f + \sum_{j=0}^{d} \partial_i I_j \cdot u_f^j \end{aligned}$$

Wir setzen nun $T \overset{\text{def}}{=} \sum_{j=0}^{d} \partial_i I_j \cdot u_f^j$. Da jede X-Ableitung, die in den I_j auftritt, kleinere Höhe als u_f hat, insbesondere auch die Leitableitungen u_{I_j}, folgt $\partial_i I_j \ll \partial_i u_f$ f.a. j. Natürlich gilt $u_f \ll \partial_i u_f \Longrightarrow T \ll \partial_i u_f$.
$\underline{k-1 \to k}$, d.h. $\theta = \partial_i \theta'$ für geeigntes ∂_i und $\theta' \in \Theta$, wobei $ord(\theta') = k-1$, θ' also die Induktionsvoraussetzung erfüllt.
$\theta f = \partial_i(\theta' f) \overset{\text{I.V.}}{=} \partial_i(S_f \cdot \theta' u_f + T')$ mit $T' \ll \theta' u_f$, insbesondere $u_{T'} \ll \theta' u_f$. Mit $T \overset{\text{def}}{=} \partial_i T' + \partial_i S_f \cdot \theta' u_f$ folgt die Behauptung, da $\partial_i u_{T'} \ll \partial_i \theta' u_f = \theta u_f$. □

2.4 Selbstreduzierte Mengen

Wir müssen jetzt ein Reduzierungsverfahren für X-Ableitungen einführen, das den Prozeß des Euklidischen Algorithmus verallgemeinert. Im Hinterkopf haben wir die Absicht, ausgehend von einem beliebigen D-Polynom g in Abhängigkeit von einem nicht-konstantem Polynom f zu einem Polynom g' überzugehen, das keine Ableitungen von u_f mehr und u_f selbst nur noch in kleinerem Grad als f enthält.

Definition 8 *Sei $f \in R\{X\} \setminus R$ gegeben. Ein Polynom $g \in R\{X\}$ heißt*

1. **partiell reduziert bezüglich** *f, falls g keine echten Ableitungen von u_f enthält (d.h. keine X-Ableitung θu_f mit $ord(\theta) > 0$).*

2. **reduziert bezüglich** *f, falls g partiell reduziert bzgl. f ist, und $grad_{u_f}(g) < grad_{u_f}(f)$ gilt.*

Diese Begriffe übertragen sich jetzt auf beliebige Mengen von nicht-konstanten Polynomen $\mathcal{A} \subset R\{X\} \setminus R$. Denn g heißt

3. **partiell reduziert bezüglich** $\mathcal{A}$, *falls* g *partiell reduziert bzgl. jedem* $f \in \mathcal{A}$ *ist.*

4. **reduziert bezüglich** $\mathcal{A}$, *falls* g *reduziert bzgl. jedem* $f \in \mathcal{A}$ *ist.*

5. *Eine Menge* $\mathcal{A} \subset R\{X\} \setminus R$ *heißt* **selbstreduziert**, *wenn für jedes* $f \in \mathcal{A}$ *gilt:* f *ist reduziert bzgl.* $\mathcal{A}\setminus\{f\}$, *d.h., jedes* f *ist reduziert bzgl. aller übrigen Polynome.*

Der Begriff der selbstreduzierten Menge wird uns von nun an immer wieder begegnen. Um die Ideale des D-Polynomringes zu untersuchen und zu beschreiben, sind spezielle selbstreduzierte Mengen die entscheidenden Merkmale, wie wir noch sehen werden. Jetzt aber die ersten wichtigen Eigenschaften von selbstreduzierten Mengen.

Lemma 2.4.1 *Sei* $\mathcal{A} \subset R\{X\} \setminus R$ *eine selbstreduzierte Menge von Polynomen. Dann gilt:*

a) Die Leitableitungen der Polynome aus $\mathcal{A}$ *sind paarweise verschieden.*

b) $\mathcal{A}$ *ist eine endliche Menge.*

Beweis: Zu a) Angenommen, es gäbe f_1 und f_2 in $\mathcal{A}$ mit $u_1 = u_2$, wobei wir $u_i = u_{f_i}$ abgekürzt haben. Dann muß $grad_{u_1}(f_2) < grad_{u_1}(f_1)$ gelten, da ja f_2 reduziert bzgl. der übrigen Polynomen sein muß. Andererseits muß aus dem gleichen Grund $grad_{u_1}(f_1) = grad_{u_2}(f_1) < grad_{u_2}(f_2)$ gelten. Diese beiden Ungleichungen ergeben aber einen Widerspruch!

Zu b) Um uns *b)* zu überlegen, ordnen wir den X-Ableitungen $\partial_1^{\nu_1} \cdots \partial_m^{\nu_m} X$ speziell das Tupel $(\nu_1, \ldots, \nu_m)$ natürlicher Zahlen zu, die wir uns diesmal durch die Produktordnung auf $\mathbb{N}^m$ geordnet denken. Darunter verstehen wir

$$(n_1, \ldots, n_m) \leq (n'_1, \ldots, n'_m) \quad \text{gdw.} \quad n_i \leq n'_i \quad \text{f.a. } i \text{ mit} \quad 1 \leq i \leq m.$$

Wir halten fest, daß jede Folge von m-Tupeln eine monoton wachsende (in der Produktordnung) Teilfolge hat.
Wir nehmen jetzt an, daß es eine selbstreduzierte Menge von Polynomen gibt, die unendlich ist. Dann erhalten wir eine unendliche Familie verschiedener Leitableitungen $(u_f)_{f\in\mathcal{A}}$ nach a), die uns wiederum mittels obiger Zuordnung eine unendliche Folge von m-Tupeln $((\nu_1^f, \ldots, \nu_m^f))_{f\in\mathcal{A}}$ liefert. Diese muß jetzt aber eine monoton wachsende Teilfolge enthalten, etwa $((\nu_1^{f_i}, \ldots, \nu_m^{f_i}))_{i\in\mathbb{N}}$ mit $(\nu_1^{f_i}, \ldots, \nu_m^{f_i}) \leq (\nu_1^{f_j}, \ldots, \nu_m^{f_j})$ für $i < j$.
Würde für zwei Polynome f_i, f_j nun $(\nu_1^{f_i}, \ldots, \nu_m^{f_i}) < (\nu_1^{f_j}, \ldots, \nu_m^{f_j})$ gelten, hieße das, daß u_{f_j} eine echte Ableitung von u_{f_i} wäre, was wegen der Reduziertheit von f_j bzgl. f_i ein Widerspruch wäre!

Es kann aber andererseits nicht $(\nu_1^{f_i}, \ldots, \nu_m^{f_i}) = (\nu_1^{f_j}, \ldots, \nu_m^{f_j})$ f.a. i, j gelten, was ja $u_{f_i} = u_{f_j}$ bedeuten würde, im Widerspruch zu a)!
Also ist die Annahme, daß $\mathcal{A}$ unendlich ist, falsch. □

Jetzt wollen wir das bereits angekündigte Reduktionsverfahren angeben. Dazu sei immer eine selbstreduzierte (und wie wir ja wissen damit endliche) Menge $\mathcal{A}$ gegeben. Wir werden der Fragen nachgehen, ob man zu einem beliebigen Polynom g ein Polynom g' finden kann, das reduziert bzgl. $\mathcal{A}$ ist, aber dennoch in gewissem Sinne mit g übereinstimmt. Darunter verstehen wir in erster Linie, daß g an einer gemeinsamen Nullstelle aller $f \in \mathcal{A}$ genau dann von Null verschieden ist, wenn g' dort von Null verschieden ist. Die nächsten Lemmata werden das präzisieren.

<u>Lemma</u> 2.4.2 *Sei $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine selbstreduzierte Menge von Polynomen und $g \in R\{X\}$.*
Dann existieren $n_i \in \mathbb{N}$, $1 \leq i \leq t$, und ein $\hat{g} \in R\{X\}$, mit $\hat{g}$ partiell reduziert bzgl. $\mathcal{A}$, $\hat{g} \underline{\ll} g$ und

$$\prod_{i=1}^{t} S_{f_i}^{n_i} g \equiv \hat{g} \pmod{\langle \mathcal{A} \rangle} .$$

Weiterhin gilt sogar: Es gibt $C_j \in R\{X\}$, $f_{i_j} \in \mathcal{A}$ und $\theta_j \in \Theta$ mit $\prod_{i=1}^{t} S_{f_i}^{n_i} g - \hat{g} = \sum_{j=1}^{r} C_j \cdot \theta_j f_{i_j}$, wobei die $\theta_j u_{f_{i_j}}$ kleinere oder gleiche Höhe wie u_g haben.

Beweis: Seien in $\mathcal{M} = \{u_1, \ldots, u_t\}$ die Leitableitungen der Polynome aus $\mathcal{A}$. Falls g bereits partiell reduziert bzgl. A ist, setzen wir $\hat{g} \stackrel{\text{def}}{=} g$ und $n_j \stackrel{\text{def}}{=} 0$ für $1 \leq i \leq t$. Es ist klar, daß mit dieser Wahl die Behauptung des Satzes gilt.
Sei also g nicht partiell reduziert bzgl. $\mathcal{A}$, d.h., g enthält mindestens eine echte Ableitung eines dieser u_i, etwa $v_1, \ldots, v_n$, wobei wir uns diese so nummerieren, daß $v_k \ll v_j$ für $j < k$ gilt. Es ist möglich, daß ein v_k die Ableitung von verschiedenen Leitableitungen aus $\mathcal{M}$ ist, dann wählen wir für die Darstellung $v_k = \theta_k u_{i_k}$ mit $ord(\theta_k) > 0$ immer das jeweils höchste dieser $u_{i_k} \in \mathcal{M}$ aus. Wir schreiben somit $\theta_n u_{i_n} \ll \ldots \ll \theta_1 u_{i_1}$ mit $ord(\theta_k) > 0$ für die in g auftretenden Ableitungen der $u_i \in \mathcal{M}$.
Nun definieren wir induktiv Polynome G_k und natürliche Zahlen $n_{k,i}$ für $1 \leq i \leq t$, wobei dann $v_1, \ldots, v_k$ in G_k nicht mehr auftritt, $G_k \underline{\ll} g$, und es glit:

$$\prod_{i=1}^{t} S_{f_i}^{n_{k,i}} g \equiv G_k \pmod{(\theta_1 f_{i_1}, \ldots, \theta_k f_{i_k})} .$$

Wir beginnen mit $G_0 \stackrel{\text{def}}{=} g$ und $n_{0,i} \stackrel{\text{def}}{=} 0$ f.a. i. Es ist klar, daß diese Wahl allen Forderungen genügt. Wir konstruieren nun G_k und die $n_{k,i}$ aus ihren Vorgängern. Für $v_k = \theta_k u_{i_k}$ bezeichne h_k das zu u_{i_k} gehörige Polynom aus $\mathcal{A}$ und S_k dessen Separanten. Nach Lemma 2.3.3 hat $T_k \stackrel{\text{def}}{=} S_k v_k - \theta_k h_k$ kleinere Höhe als v_k. Sei

$e_k \overset{\text{def}}{=} grad_{v_k}(G_{k-1})$. Dann schreiben wir $G_{k-1} = \sum_{i=0}^{e_k} J_i v_k^i$ als Polynom in v_k, wobei die J_i Polynome sind, die Ableitungen von u_{i_k} nur in kleinerer Höhe als v_k enthalten können, da $v_1, \ldots, v_{k-1}$ in G_{k-1} nicht mehr auftreten.

$$\begin{aligned}
S_k^{e_k} G_{k-1} &= \sum_{i=0}^{e_k} S_k^{e_k-i} J_i (S_k v_k)^i = \sum_{i=0}^{e_k} S_k^{e_k-i} J_i (T_k + \theta_k h_k)^i \\
&= \sum_{i=0}^{e_k} S_k^{e_k-i} J_i \left(\sum_{l=0}^{i} \binom{i}{l} T_k^{i-l} (\theta_k h_k)^l \right) \\
&= \sum_{i=0}^{e_k} S_k^{e_k-i} J_i \left(T_k^i + \sum_{l=1}^{i} \binom{i}{l} T_k^{i-l} (\theta_k h_k)^l \right) \\
&= \sum_{i=0}^{e_k} S_k^{e_k-i} J_i T_k^i + \underbrace{\sum_{i=0}^{e_k} S_k^{e_k-i} J_i \left(\sum_{l=1}^{i} \binom{i}{l} T_k^{i-l} (\theta_k h_k)^l \right)}_{\in (\theta_k h_k)}
\end{aligned}$$

Das können wir nun so formulieren: $S_k^{e_k} G_{k-1} - G_k \in (\theta_k h_k)$, wobei wir $G_k \overset{\text{def}}{=} \sum_{i=0}^{e_k} S_k^{e_k-i} J_i T_k^i$ gewählt haben. Weiter setzen wir $n_{k,i} \overset{\text{def}}{=} n_{k-1,i}$ falls $h_k \neq f_i$ und $n_{k,i} \overset{\text{def}}{=} n_{k-1,i} + e_k$ falls $h_k = f_i$. T_k und S_k haben kleinere Höhe als u_k, und für die J_i wissen wir: $J_i \lll G_{k-1}$. Daraus folgt $G_k \lll G_{k-1}$, was mit der Induktionsvoraussetzung $G_k \lll g$ ergibt. Ferner erhalten wir für eine geeignetes $P \in (\theta_k u_{i_k})$ ($\theta_k h_k = \theta_k f_{i_k}$!):

$$\begin{aligned}
G_k &= S_{i_k}^{e_k} G_{k-1} + P \overset{\text{I.V.}}{=} S_{i_k}^{e_k} \left(\prod_{i=1}^{t} S_{f_i}^{n_{k-1,i}} \cdot g + Q \right) + P \\
&= \prod_{i=1}^{t} S_{f_i}^{n_{k,i}} g + \underbrace{S_{i_k}^{e_k} Q + P}_{\in (\theta_1 f_{i_1}, \ldots, \theta_k f_{i_k})} ,
\end{aligned}$$

wobei wir wieder die Induktionsvoraussetzung für G_{k-1} mit einem passenden Q aus dem Ideal $(\theta_1 f_{i_1}, \ldots, \theta_k f_{i_{k-1}})$ in $R\{X\}$ benutzt haben.

Nach n Schritten haben wir alle $v_1, \ldots, v_n$ eliminiert, und wir definieren $\hat{g} \overset{\text{def}}{=} G_n$ und $n_i \overset{\text{def}}{=} n_{n,i}$ für $1 \leq i \leq t$. Es ist nach Konstruktion klar, daß mit dieser Wahl der erste Teil der Behauptung erfüllt ist. Weil die $\theta_k u_{i_k}$ aber in g auftreten, können wir $\theta_k u_{i_k} \lll u_g$ f.a. k schließen. Es ist aber $\theta_k u_{i_k} = \theta_k u_{f_{i_k}}$, weswegen mit $\prod_{i=1}^{t} S_{f_i}^{n_{k,i}} g - G_n \in (\theta_1 f_{i_1}, \ldots, \theta_n f_{i_n})$ auch der zweite Teil folgt. □

Wir wollen in einer Definition den konstruktiven Teil des Lemmas festhalten.

Definition 9 *Sei $\mathcal{A}$ eine selbstreduzierte Menge von Polynomen und $g \in R\{X\}$. Dann heißt das in dem induktiven Verfahren des Beweises von 2.4.2 konstruierte Polynom $\hat{g}$* **der partielle Rest** *von g bezüglich $\mathcal{A}$.*

Wenn wir anschließend an dieses Reduktionsverfahren noch Division mit Rest bezüglich der Leitableitungen von $\mathcal{A}$ durchführen, gelangen wir zu einem Polynom $\bar{g}$, das diese Leitableitungen nur in kleinerem Grad enthält, als die entsprechenden f aus $\mathcal{A}$, das also reduziert bzgl. $\mathcal{A}$ ist.

Lemma 2.4.3 *Sei $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine selbstreduzierte Menge von Polynomen und $g \in R\{X\}$.*
Dann existieren $n_i, m_i \in \mathbb{N}$, $1 \leq i \leq t$, und ein $\bar{g} \in R\{X\}$, mit $\bar{g}$ reduziert bzgl. $\mathcal{A}$, $\bar{g} \underline{\ll} g$ und

$$\prod_{i=1}^{t} I_{f_i}^{m_i} S_{f_i}^{n_i} g \equiv \bar{g} \pmod{\langle \mathcal{A} \rangle} .$$

Weiterhin gilt sogar: Es gibt $C_j \in R\{X\}$, $f_{i_j} \in \mathcal{A}$ und $\theta_j \in \Theta$ mit $\prod_{i=1}^{t} I_{f_i}^{m_i} S_{f_i}^{n_i} g - \bar{g} = \sum_{k=1}^{r'} D_k \cdot \theta_j f_{i_j}$, wobei $D_j \in R\{X\}$ und $\theta_j u_{f_{i_j}} \underline{\ll} u_g$.

Beweis: Seien wieder $\{u_1, \ldots, u_t\}$ die Leitableitungen, und wir können ohne Einschränkung für die Indizierung annehmen, daß $u_i \ll u_j$ für $1 \leq i < j \leq t$ gilt. I_j sei die Kurzform von I_{f_j}. Wir definieren induktiv Polynome r_k, mit $r_k \underline{\ll} g$, $d_k \stackrel{\text{def}}{=} grad_{u_k}(r_k) < grad_{u_k}(f_k) \stackrel{\text{def}}{=} e_k$, und r_k ist partiell reduziert bzgl. $\mathcal{A}$.
Wir bilden gemäß Lemma 2.4.2 den partiellen Rest $\hat{g}$ von g bzgl. $\mathcal{A}$, dann setzen wir $r_0 \stackrel{\text{def}}{=} \hat{g}$, was den Anforderungen genügt. Sei jetzt r_{k-1} bereits konstruiert, dann betrachten wir $m_k \stackrel{\text{def}}{=} max\{0, grad_{u_k} r_{k-1} - e_k + 1\}$. Die Division mit Rest liefert $r_k, q_k \in R\{X\}$, so daß für $f_k = \sum_{j=0}^{e_k} I_j u_k^j$ und r_{k-1} als Polynom in u_k gilt: $I_k^{m_k} r_{k-1} = q_k f_k + r_k$. Außerdem erhalten wir $grad_{u_k}(r_k) < grad_{u_k}(f_k)$. Bei diesen Rechenoperationen treten keine neuen Ableitungen auf, weswegen $r_k \underline{\ll} r_{k-1} \underline{\ll} g$ nach I.V. folgt.
Nach t Schritten brechen wir die Konstruktion ab und setzen $\bar{g} \stackrel{\text{def}}{=} r_t$. Wir rechnen aus:

$$\begin{aligned}
\bar{g} &= I_t^{m_t} r_{t-2} - q_t f_t \;=\; I_t^t (I_{t-1}^{m_{t-1}} r_{t-3} - q_{t-1} f_{t-1}) - q_t f_t \\
&= I_t^t (\cdots (I_2^{m_2} (I_1^{m_1} r_0 - q_1 f_1) - q_2 f_2) \ldots - q_{t-1} f_{t-1}) - q_t f_t \\
&= \prod_{k=1}^{t} I_k^{m_k} \hat{g} - \sum_{k=1}^{t} \left(\prod_{j=k+1}^{t} I_j^{m_j} \right) q_k f_k .
\end{aligned}$$

Mit Lemma 2.4.2 ersetzen wir nun noch $\hat{g} = \prod_{i=1}^{t} S_{f_i}^{n_i} g - \sum_{j=1}^{r} C_j \cdot \theta_j f_{i_j}$ und erhalten nach Umformung obiger Gleichung:

$$\prod_{i=1}^{t} I_{f_i}^{m_i} \left(S_{f_i}^{n_i} g - \sum_{j=1}^{r} C_j \cdot \theta_j f_{i_j} \right) - \bar{g} = \sum_{k=1}^{t} \left(\prod_{j=k+1}^{t} I_j^{m_j} \right) q_k f_k ,$$

was wir dann noch umschreiben zu

$$\prod_{i=1}^{t} I_{f_i}^{m_i} S_{f_i}^{n_i} g - \bar{g} = \sum_{j=1}^{r} C'_j \cdot \theta_j f_j + \sum_{k=1}^{t} Q_k f_k = \sum_{k=1}^{r'} D_k \cdot \theta_k f_{i_k} ,$$

wobei die $\theta_k u_{f_{i_k}}$ natürlich die behauptete Eigenschaft haben. □

Wieder halten wir das so konstruierte Polynom mit einer eigenen Definition fest.

Definition 10 *Sei $\mathcal{A}$ eine selbstreduzierte Menge von Polynomen und $g \in R\{X\}$. Dann heißt das in dem Verfahren des Beweises von 2.4.3 konstruierte Polynom $\bar{g}$* **der Rest** *von g bezüglich $\mathcal{A}$.*

2.5 Die charakteristische Menge eines D-Ideals

Die selbstreduzierten Mengen sind, wie bereits gesagt, quasi das Fundament für die Untersuchung der Ideale des Polynomrings. Wir wissen, daß jedes Ideal $\mathfrak{A}$ mindestens eine selbstreduzierte Menge enhält, als einfachstes Beispiel sei die leere Menge genannt, die ja in jedem Ideal enthalten ist. Aber auch für $f \in R\{X\} \setminus R$ und $f \in \mathfrak{A}$ ist klar, das $\{f\}$ eine selbstreduzierte Menge in $\mathfrak{A}$ ist. Wir wollen uns in diesem Abschnitt damit beschäftigen, ob es unter den selbstreduzierten Mengen eines Ideals welche gibt, die in einem entscheidenden Zusammenhang mit den restlichen Elementen des Ideals stehen, in einem gewissen Sinne das Ideal *charakterisieren*. Wir werden sehen, das es solche Mengen gibt. Wir stellen zur systematischen Darstellung noch den Begriff des Ranges selbstreduzierter Mengen bereit.

Notation: Von nun an nehmen wir immer an, daß die die Indizierung der selbstreduzierten Mengen $\mathcal{A} = \{f_1, \ldots, f_t\}$ so gewählt ist, daß die Polynome aufsteigend geordnet sind im Sinne von $\ll$. (Die Leitableitungen sind alle verschieden!)

Definition 11 *Seien $\mathcal{A} = \{f_1, \ldots, f_t\}$ und $\mathcal{B} = \{g_1, \ldots, g_l\}$ zwei selbstreduzierte Mengen.*

1. *Wir sagen $\mathcal{A}$ hat* **kleineren Rang** *als $\mathcal{B}$, falls*

   a) $\mathcal{B} = \emptyset$ und $\mathcal{A} \neq \emptyset$ gilt,

   oder b) es existiert ein n, $n \leq t$ und $n \leq l$, so daß f_j und g_j dieselbe Höhe für $1 \leq j < n$ haben, und $f_n \ll g_n$,

   oder c) es gilt $t < l$ und für $1 \leq j \leq t$ haben f_j, g_j dieselbe Höhe.

2. *Falls $t = l$ und f_j, g_j dieselbe Höhe haben für $1 \leq j \leq t$, dann sagen wir, daß $\mathcal{A}$ und $\mathcal{B}$* **denselben Rang** *haben.*

Anstelle von der Anzahl der Elemente aus $\mathcal{A}$ sprechen wir manchmal von der Länge von $\mathcal{A}$. Wir wollen festhalten, daß wir von einer selbstreduzierten Menge $\mathcal{A}$ zu einer kleineren Ranges gelangen, wenn wir $\mathcal{A}$ geeignet „verlängern“ können.

Lemma 2.5.1 *Sei $R\{X\}$ ein D-Polynomring. Dann besitzt jede nicht leere Menge von selbstreduzierten Mengen aus $R\{X\}$ Elemente von minimalem Rang.*

Beweis: Sei $M \neq \emptyset$ diese Menge von selbstreduzierten Mengen aus $R\{X\}$. Wir definieren induktiv eine bzgl. Inklusion absteigende Folge M_n von Teilmengen aus M:
$\underline{n = 0:}$ $M_0 \stackrel{\text{def}}{=} M$.
$\underline{n - 1 \to n:}$ Sei M_{n-1} bereits konstruiert, wir betrachten $N_n \stackrel{\text{def}}{=} \{\mathcal{A} \in M_{n-1} \mid |\mathcal{A}| \geq n\}$, jede selbstreduzierte Mengen aus N_n besitzt also ein n-tes Polynom. In der Menge dieser n-ten Polynome gibt es jetzt wieder welche mit minimaler Höhe (in der Ordnung der Polynome). Definiere nun M_n als diejenigen selbstreduzierten Mengen aus N_n, deren n-tes Polynom eben von minimaler Höhe ist.
Diese Konstruktion stellt sicher, daß für $n \geq 1$ alle n-ten Polynome der selbstreduzierten Mengen aus M_n dieselbe Leitableitung haben müssen, da die n-ten Polynome immer dieselbe Höhe haben.
Angenommen, es existiert kein $n \in \mathbb{N}$ mit $M_n = \emptyset$, dann erhalten wir eine echt aufsteigende Folge von X-Ableitungen, nämlich die Leitableitungen der n-ten Polynome. Diese Leitableitungen dürfen keine Ableitungen voneinander sein, was an $M_{n-1} \supset M_n$ und der Selbstreduziertheit der Elemente von M_n liegt. Dies ist aber ein Widerspruch, denn wie wir im Beweis zu 2.4.1 gesehen haben, können solche Folgen von X-Ableitungen nicht existieren!
Es muß also insbesondere ein kleinstes n mit $M_n = \emptyset$ und $n > 0$ geben, da wir $M_0 = M \neq \emptyset$ vorausgesetzt haben. Natürlich sind jetzt die Elemente aus M_{n-1} die gesuchten selbstreduzierten Mengen von minimalen Rang. Aus $M_n = \emptyset$ folgt, daß alle selbstreduzierten Mengen aus M_{n-1} die gleiche Länge haben. Daß die i-ten Polynome der Elemente von M_{n-1} jeweils dieselbe Höhe haben, wird aber gerade durch unsere Konstruktion erzwungen (siehe oben). Also haben alle selbstreduzierten Mengen aus M_{n-1} denselben Rang, der nach Konstruktion auch minimal ist. □

Wenn wir jetzt zu einem D-Ideal $\mathfrak{A}$ die Menge $M_{\mathfrak{A}}$ aller selbstreduzierten Teilmengen $\mathcal{A}$ von $\mathfrak{A}$, für die $S_f \notin \mathfrak{A}$ f.a. $f \in \mathcal{A}$ gilt, betrachten, stellen wir fest, daß $M_{\mathfrak{A}}$ nicht leer ist, da $\emptyset \in M_{\mathfrak{A}}$. Das rechtfertigt die folgende Definition:

Definition 12 *Eine selbstreduzierte Mengen $\mathcal{A}$ von minimalem Rang in $M_{\mathfrak{A}}$ heißt* **charakteristische Menge** *von $\mathfrak{A}$.*

Man beachte, daß eine charakteristische Menge eines Ideals im allgemeinen nicht eindeutig bestimmt ist, eindeutig bestimmt ist jedoch ihr Rang, und damit ihre Länge und die Höhe der Polynome, die sie enthält, falls sie nicht die leere Menge (Länge Null) ist.

2.6 Die D-Ideale im D-Polynomring

Wir wollen jetzt darangehen zu untersuchen, welches Verhältins zwischen den Elementen eines Ideals und einer charakteristischen Menge besteht. Wir werden dann sehen, daß prime D-Ideale immer eine enge Beziehung zu ihren charakteristischen Mengen haben, welche das Ideal eben wirklich beschreiben. Damit sind wir dann in der Lage, den Basissatz für radikale D-Ideale anzugeben, der hier einen ersten Abschluß bilden soll.

Lemma 2.6.1 *Sei $R\{X\}$ ein D-Polynomring und $\mathfrak{A} \subset R\{X\}$ ein D-Ideal. $\mathcal{A} = \{f_1, \ldots, f_t\}$ sei eine charakteristische Menge von $\mathfrak{A}$. Dann gilt:*

a) Ist g ein nicht-konstantes Polynom aus $\mathfrak{A}$ und reduziert bzgl. $\mathcal{A}$, dann folgt $S_g \in \mathcal{A}$.

b) Für alle f_j aus $\mathcal{A}$ ist $I_{f_j} \notin \mathfrak{A}$.

c) Sei g ein beliebiges Polynom aus $\mathfrak{A}$, das reduziert bzgl. $\mathcal{A}$ ist. Dann folgt $g \in (\mathfrak{A} \cap R)$, wobei $(\mathfrak{A} \cap R)$ als Ideal in $R\{X\}$ zu verstehen ist.

Beweis: Zu a) Angenommen S_g ist kein Element von $\mathcal{A}$. Wir definieren dann die Menge $\mathcal{B} \stackrel{\text{def}}{=} \{f \in \mathcal{A} \mid u_f \ll u_g\} \cup \{g\}$. Diese Menge ist selbstreduziert, $S_{f'} \notin \mathfrak{A}$ f.a. $f' \in \mathcal{B}$. Außerdem hat $\mathcal{B}$ kleineren Rang als $\mathcal{A}$, denn entweder gilt $\mathcal{B} = \{f_1, \ldots, f_t, g\}$, dann können wir mit Definition 11 c) schließen, daß $\mathcal{B}$ kleinere Rang als $\mathcal{A}$ hat. Oder aber es gibt ein $f_n \in \mathcal{A}$ mit $u_g \underline{\ll} u_{f_n}$. Falls $u_g = u_{f_n}$ gilt, dann muß wegen der Reduziertheit von g bzgl. f_n $grad_{u_{f_n}}(g) < grad_{u_{f_n}}(f_n)$, und damit $g \ll f_n$ sein. Falls $u_g \ll u_{f_n}$ gilt, ist natürlich ebenso $g \ll f_n$.
Beide Fälle führen zu einem Widerspruch zur Minimalität von $\mathcal{A}$!

Zu b) Angenommen, es existiert ein $f \in \mathcal{A}$ mit $I_f \in \mathfrak{A}$. Sei $e \stackrel{\text{def}}{=} grad_{u_f}(f)$, betrachte dann das Polynom $g \stackrel{\text{def}}{=} f - I_f u_f^e$. g ist ein Element von $\mathfrak{A}$, da $f \in \mathfrak{A}$ und nach Annahme $I_f \in \mathfrak{A}$ gilt. g ist reduziert bzgl. $\mathcal{A}$, die Reduziertheit bzgl. $\mathcal{A} \setminus \{f\}$ erbt g von f, und da g u_f nur in kleinerer Potenz als f enthält, ist die Reduziertheit bzgl. f ebenfalls klar.
Falls g nicht-konstant ist, folgt mit *a)* $S_g \in \mathfrak{A}$. Für S_g können wir schreiben

$$S_g = \frac{\partial(f - I_f u_f^e)}{\partial u_f} = S_f - eI_f u_f^{e-1} ,$$

was mit $I_f, S_g \in \mathfrak{A}$ aber auch $S_f \in \mathfrak{A}$ bedeuten würde, ein Widerspruch
Falls g konstant ist, erhalten wir $S_g = 0$, und $I_f \in \mathfrak{A}$ ergibt wieder $S_f \in fA$.

Zu c) Ohne Einschränkung können wir g als nicht-konstant voraussetzen, für konstantes g ist die Behauptung klar.
Angenommen, es existieren nicht-konstante $g \in \mathfrak{A}$, reduziert bzgl. $\mathcal{A}$ und $g \notin (\mathfrak{A} \cap$

R). Wir wählen dann aus der Menge der Polynome mit dieser Eigenschaft ein g von mimimaler Höhe. Dann gilt: $S_g \in (\mathfrak{A} \cap R)$, da S_g auch reduziert bzgl. $\mathcal{A}$ ist und immer kleinere Höhe als g hat, g aber von minimaler Höhe gewählt war. Beachte $\mathbb{Q} \subset R$ und $grad_{u_g} g = e \neq 0$, da g nicht-konstant, somit $g' \stackrel{\text{def}}{=} g - \frac{1}{e} u_g S_g \in \mathfrak{A}$. Für g' können wir schließen, daß g' kleinere Höhe als g hat, da $u_g \ll u_{g'}$ oder $u_g = u_{g'}$ und $grad_{u_g}(g') < grad_{u_g}(g)$ gilt. Wegen der Minimalität von g muß wieder $g' \in (\mathfrak{A} \cap R)$ gelten, was dann aber wegen $S_g \in (\mathfrak{A} \cap R)$ auch $g \in (\mathfrak{A} \cap R)$ zur Folge hätte. Das ist ein Widerspruch, da ja $g \notin (\mathfrak{A} \cap R)$ gewählt war! $\square$

<u>Notation:</u> Sei $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine selbstreduzierte Menge, dann legen wir zur Abkürzung $H_{\mathcal{A}} \stackrel{\text{def}}{=} \prod_{i=1}^t S_{f_i} I_{f_i}$ fest. Falls $\mathcal{A} = \emptyset$, dann $H_{\mathcal{A}} \stackrel{\text{def}}{=} 1$.

Nachdem wir jetzt etwas darüber wissen, wie sich Polynome in einem Ideal verhalten, die bezüglich einer charakteristischen Menge des Ideals reduziert sind, und daß sowohl die Separanten als auch die Leitkoeffizienten von den Polynomen der charakteristischen Menge nicht im Ideal liegen, untersuchen wir nun spezieller die primen D-Ideale. Hier stellt sich heraus, daß prime D-Ideale besonders weitgehend durch eine charakteristische Menge bestimmt sind. Man beachte für prime D-Ideale immer, daß für jede charakteristische Menge $\mathcal{A}$ des Ideals $H_{\mathcal{A}}$ kein Element des Ideals ist, da ja alle Faktoren von $H_{\mathcal{A}}$ nicht im Ideal liegen (siehe oben).

<u>Lemma</u> 2.6.2 *R sei ein D-Ring, $\mathfrak{p}$ ein primes D-Ideal von $R\{X\}$. Sei $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine charakteristische Menge von $\mathfrak{p}$ mit dem dazugehörigen $H_{\mathcal{A}}$.*
Dann läßt sich $\mathfrak{p}$ schreiben als:

$$\mathfrak{p} = \bigcup_{n \in \mathbb{N}} \left\{ x \in R\{X\} \mid x \cdot H_{\mathcal{A}}^n \in \Big(\langle \mathcal{A} \rangle + (\mathfrak{p} \cap R) \Big) \right\} .$$

Beweis: Zuerst zeigen wir die Inklusion „$\subset$“: Sei dazu ein $g \in \mathfrak{p}$ gegeben. Bilde dann $\bar{g}$, den Rest von g bzgl. $\mathcal{A}$ gemäß Lemma 2.4.3, mit der Darstellung

$$\prod_{j=1}^t I_{f_j}^{m_j} S_{f_j}^{n_j} g \equiv \bar{g} \pmod{\langle \mathcal{A} \rangle} . \tag{2.1}$$

Weil $\bar{g}$ reduziert bzgl. $\mathcal{A}$ ist, liegt $\bar{g}$ in $(\mathfrak{p} \cap R)$ nach Lemma 2.6.1. Außerdem behaupten wir, daß

$$g \in \bigcup_{n \in \mathbb{N}} \left\{ x \in R\{X\} \mid x \cdot H_{\mathcal{A}}^n \in \Big(\langle \mathcal{A} \rangle + (\bar{g}) \Big) \right\} \tag{2.2}$$

gilt. Denn wenn wir mit (2.1) $n \stackrel{\text{def}}{=} kgV\{n_j, m_j \mid 1 \leq j \leq t\}$ wählen, dann erhalten wir nach geeigneter Multiplikation $\prod_{j=1}^t I_{f_j}^n S_{f_j}^n g - D \cdot \bar{g} \in \langle \mathcal{A} \rangle$, wobei D

ein Vielfaches der I_{f_j} und S_{f_j} ist. Wir sehen $g \cdot H_{\mathcal{A}}^n = H_{\mathcal{A}}^n \cdot g \in \Big(\langle\mathcal{A}\rangle + (\bar{g})\Big)$. Aus $\bar{g} \in (\mathfrak{p} \cap R)$ folgt natürlich $(\bar{g}) \subset (\mathfrak{p} \cap R)$. Wir können somit $\Big(\langle\mathcal{A}\rangle + (\bar{g})\Big) \subset \Big(\langle\mathcal{A}\rangle + (\mathfrak{p} \cap R)\Big)$ schließen, was dann mit (2.2) ergibt:

$$g \in \bigcup_{n\in\mathbb{N}} \Big\{x \in R\{X\} \mid x \cdot H_{\mathcal{A}}^n \in \Big(\langle\mathcal{A}\rangle + (\mathfrak{p} \cap R)\Big)\Big\} \ .$$

Jetzt zur Inklusion „$\supset$“: Sei dazu ein g gegeben mit $g \cdot H_{\mathcal{A}}^n \in \Big(\langle\mathcal{A}\rangle + (\mathfrak{p} \cap R)\Big)$ für ein geeignetes $n \in \mathbb{N}$. Da $\mathcal{A} \subset \mathfrak{p}$, $\mathfrak{p} \cap R \subset \mathfrak{p}$ gilt, und $\mathfrak{p}$ D-Ideal ist, erhalten wir $\Big(\langle\mathcal{A}\rangle + (\mathfrak{p} \cap R)\Big) \subset \mathfrak{p}$, also $g \cdot H_{\mathcal{A}}^n \in \mathfrak{p}$. Wir wissen, daß $H_{\mathcal{A}}$ nicht in $\mathfrak{p}$ liegt, also können wir $g \in \mathfrak{p}$ schließen, da $\mathfrak{p}$ primes Ideal ist. □

Für den Fall, daß wir D-Körper F und ein primes Ideal $\mathfrak{p}$, das echt in $F\{X\}$ enthalten ist, betrachten, stellen wir noch ausdrücklich Folgendes fest: es gilt $\mathfrak{p} \cap R = \{0\}$. Sonst gäbe es ein $0 \neq a \in \mathfrak{p} \cap F$, damit dann auch $1 = a^{-1}a \in \mathfrak{p}$, was dann ja $\mathfrak{p} = F\{X\}$ zur Konsequenz hätte. Das vereinfacht obige Darstellung von $\mathfrak{p}$ nochmals.

<u>**Korollar**</u> **2.6.3** *Sei F ein D-Körper und $\mathfrak{p}$ ein primes D-Ideal, das echt in $F\{X\}$ enthalten ist. Dann gilt für eine charakteristische Menge $\mathcal{A} = \{f_1, \ldots, f_t\}$ von $\mathfrak{p}$:*

$$\mathfrak{p} = \{x \in F\{X\} \mid x \cdot H_{\mathcal{A}}^n \in \langle\mathcal{A}\rangle\} \ .$$

Zum Abschluß dieses Kapitels wollen wir der Vollständigkeit halber noch den Basissatz für radikale D-Ideale angeben. Er zeigt, daß sich die Ergebnisse der Algebra nicht völlig analog auf unsere D-Ringe bzw. D-Körper übertragen lassen, aber doch in einem ausreichenden Maß. Denn der Basissatz gewinnt ja seine Bedeutung dadurch, daß man sich bei der Untersuchung von Nullstellenmengen von Idealen des Polynomringes auf die Nullstellen von endlich vielen Polynomen, der Idealbasis, beschränken kann. Da wir in unserem Falle der Charakteristik Null aber ebenfalls die Gleichheit $\{a \in R \mid \text{es ex. } n \in \mathbb{N} \text{ mit } a^n \in \mathfrak{A}\} = \{\mathfrak{A}\}_{\mathfrak{r}}$ für das von dem Ideal $\mathfrak{A}$ erzeugte radikale D-Ideal haben, erkennt man, daß die Nullstellenmenge von $\mathfrak{A}$ mit der des von $\mathfrak{A}$ erzeugten radikalen D-Ideals übereinstimmt. Ein Basissatz für radikale D-Ideale reicht also „für vieles“ aus.

<u>**Satz**</u> **2.6.4 (Basissatz für radikale D-Ideale)** *R sei ein D-Ring mit $R \supset \mathbb{Q}$. Sind die radikalen D-Ideale von R endlich erzeugt, dann sind auch die radikalen D-Ideale des D-Polynomringes $R\{X\}$ endlich erzeugt.*

Beweis: Annahme: Es existiert ein radikales D-Ideal $\mathfrak{A}$, das nicht endlich erzeugt ist. Selbstverständlich $\mathfrak{A} \neq R\{X\}$, sonst würde $\mathfrak{A}$ von der 1 erzeugt.
Wir können dann mit dem Zornschen Lemma ein maximales unter den Idealen

mit dieser Eigenschaft auswählen. Denn die Vereinigung einer aufsteigenden Kette von nicht endlich erzeugten radikalen D-Idealen, die $\mathfrak{A}$ enthalten, ist naürlich wieder ein radikales D-Ideal. Es kann nicht endlich erzeugt sein, sonst erhielte man bereits nach endlich vielen Schritten ein Ideal dieser Kette, das schon die ganze Idealbasis enthalten würde, also auch endlich erzeugt wäre, was aber nach Voraussetzung nicht der Fall ist. Selbstverständlich ist die Vereinigung nicht ganz $R\{X\}$ selbst, sonst wäre die 1 ebenso bereits in einem Ideal der Kette, was auch zu einem Widerspruch führen würde. Bezeichnen wir das so gewählte maximale Element mit $\mathfrak{M}$.

Als erstes stellen wir fest, daß $\mathfrak{M}$ prim ist. Nehmen wir dazu das Gegenteil an und geben uns zwei Polynome h_1 und h_2 vor, die nicht in $\mathfrak{M}$ enthalten sein sollen, deren Produkt h_1h_2 aber trotzdem Element von $\mathfrak{M}$ ist. Wir erhalten erst einmal zwei radikale D-Ideale mit $\mathfrak{M} \subsetneqq \{h_1, \mathfrak{M}\}_\mathfrak{r}$ und $\mathfrak{M} \subsetneqq \{h_2, \mathfrak{M}\}_\mathfrak{r}$. Wegen der Maximalität von $\mathfrak{M}$ liefert uns das zwei endliche Idealbasen $\mathcal{B}_1$ und $\mathcal{B}_2$ mit $\{h_1, \mathfrak{M}\}_\mathfrak{r} = \{\mathcal{B}_1\}_\mathfrak{r}$ und $\{h_2, \mathfrak{M}\}_\mathfrak{r} = \{\mathcal{B}_2\}_\mathfrak{r}$. Unsere Annahme $h_1h_2 \in \mathfrak{M}$ ergibt zusammen mit mehrmaliger Anwendung von Lemma 1.2.4:

$$\begin{aligned} \mathfrak{M} &= \{h_1h_2, \mathfrak{M}\}_\mathfrak{r} = \{h_1\mathfrak{M} \cdot h_2\mathfrak{M}\}_\mathfrak{r} = \{h_1, \mathfrak{M}\}_\mathfrak{r} \cap \{h_2, \mathfrak{M}\}_\mathfrak{r} \\ &= \{\mathcal{B}_1\}_\mathfrak{r} \cap \{\mathcal{B}_2\}_\mathfrak{r} = \{\mathcal{B}_1 \cdot \mathcal{B}_2\}_\mathfrak{r} \ . \end{aligned}$$

Da natürlich auch $\mathcal{B}_1 \cdot \mathcal{B}_2$ eine endliche Menge ist, haben wir also erhalten, daß $\mathfrak{M}$ endlich erzeugt ist, ein Widerspruch!

Sei nun $\mathcal{A}$ eine charakteristische Menge von $\mathfrak{M}$, und wir erinnern an $H_\mathcal{A} \notin \mathfrak{M}$ für $H_\mathcal{A} = \prod_{f \in \mathcal{A}} I_f S_f$. Weiterhin haben wir mit Lemma 2.6.2 die Darstellung

$$\mathfrak{M} = \bigcup_{n \in \mathbb{N}} \left\{ x \in R\{X\} \mid x \cdot H_\mathcal{A}^n \in \Big(\langle \mathcal{A} \rangle + (\mathfrak{M} \cap R) \Big) \right\} \ . \tag{2.3}$$

Es gilt: $H_\mathcal{A} \cdot \mathfrak{M} \subset \Big\{ \{ \langle \mathcal{A} \rangle + (\mathfrak{M} \cap R) \Big\}$, denn ein Element a aus $H_\mathcal{A} \cdot \mathfrak{M}$ können wir schreiben als $a = H_\mathcal{A} \cdot x$ für ein geeignetes $x \in \mathfrak{M}$. Zu einem x aus $\mathfrak{M}$ muß wiederum ein passendes $n \in \mathbb{N}$ existieren, so daß $x \cdot H_\mathcal{A}^n \in \Big(\langle \mathcal{A} \rangle + (\mathfrak{M} \cap R) \Big)$ nach (2.3) gilt, somit auch $(x \cdot H_\mathcal{A})^n \in \Big(\langle \mathcal{A} \rangle + (\mathfrak{M} \cap R) \Big)$. Daraus ergibt sich wieder mit Korollar 1.2.3: $a = x \cdot H_\mathcal{A} \in \{ \langle \mathcal{A} \rangle + (\mathfrak{M} \cap R) \}_\mathfrak{r}$.
Da $\mathfrak{M} \cap R$ ein radikales D-Ideal in R ist, existiert nach Voraussetzung eine endliche Idealbasis $\Delta \subset \mathfrak{M} \cap R$, so daß $\mathfrak{M} \cap R = \{\Delta\}_\mathfrak{r}$ in R erfüllt ist. Wir folgern jetzt für die jeweiligen Ideale in $R\{X\}$: $(\mathfrak{M} \cap R) \subset \{\Delta\}_\mathfrak{r} \subset \{\mathcal{A} \cup \Delta\}_\mathfrak{r}$, was dann zu $\{ \langle \mathcal{A} \rangle + (\mathfrak{M} \cap R) \}_\mathfrak{r} \subset \{\mathcal{A} \cup \Delta\}_\mathfrak{r}$ führt. Somit gelangen wir zu $H_\mathcal{A} \cdot \mathfrak{M} \subset \{\mathcal{A} \cup \Delta\}_\mathfrak{r}$.
Das radikale D-Ideal $\{H_\mathcal{A}, \mathfrak{M}\}_\mathfrak{r}$ enthält das radikale D-Ideal $\mathfrak{M}$ echt, da $H_\mathcal{A}$ nicht in $\mathfrak{M}$ liegt. Damit ist $\{\Psi'\}_\mathfrak{r} = \{H_\mathcal{A}, \mathfrak{M}\}_\mathfrak{r}$ für eine endliche Menge Ψ' von Polynomen, wieder wegen der Maximalität von $\mathfrak{M}$ unter den nicht endlich erzeugten radikalen D-Idealen. In Ψ' kann eventuell $H_\mathcal{A}$ enthalten sein, wir gehen deshalb über zu

$\Psi \overset{\text{def}}{=} \Psi' \setminus \{H_A\}$, Ψ ist jetzt sogar Teilmenge von $\mathfrak{M}$. Jedenfalls läßt sich dann auch $\{H_A, \Psi\}_\mathfrak{r} = \{H_A, \mathfrak{M}\}_\mathfrak{r}$ schreiben. Wir erhalten:

$$\begin{aligned} \mathfrak{M} &= \mathfrak{M} \cap \{H_A, \mathfrak{M}\}_\mathfrak{r} = \mathfrak{M} \cap \{H_A, \Psi\}_\mathfrak{r} = \{H_A \mathfrak{M}, \Psi\}_\mathfrak{r} \\ &\subset \{\{\mathcal{A} \cup \Delta\}_\mathfrak{r}, \Psi\}_\mathfrak{r} = \{\mathcal{A} \cup \Delta \cup \Psi\}_\mathfrak{r} \\ &\subset \mathfrak{M}\,, \end{aligned}$$

da $\mathcal{A}$, Δ und Ψ alles Teilmengen von $\mathfrak{M}$ sind.
Die letzte Inklusion bedeutet selbstverständlich die Gleichheit für alle auftretenden Ideale, insbesondere $\mathfrak{M} = \{\mathcal{A} \cup \Delta \cup \Psi\}_\mathfrak{r}$, was dann aber besagen würde, daß $\mathfrak{M}$ endlich erzeugt wäre, da die Mengen $\mathcal{A}$, Δ und Ψ alle endlich sind. Ein Widerspruch ! □

Wenn jedes radikale D-Ideale eine endliche Basis besitzt, muß jede aufsteigende Kette von radikalen D-Idealen bereits nach endlich vielen Schritten konstant werden. Wir können also wie gewohnt sagen, daß sich ACC auf den Polynomring vererbt. Wir halten fest, daß sich somit auch die Zerlegung eines radikalen D-Ideals in D-Primideale (Lemma 1.2.6) überträgt. Für den D-Polynoming über einem D-Körper K (der ja ACC hat) halten wir dies ausdrücklich in einem Korollar fest.

Korollar 2.6.5 *Jedes radikale D-Ideal aus $K\{X\}$ hat eine eindeutige irreduzible Darstellung als endlicher Schnitt von D-Primidealen.*

Kapitel 3

Modelltheorie der Differential-Körper

Dieses Kapitel soll nun dazu dienen, die grundlegenden modelltheoretischen Resultate zu entwickeln. Im wesentlichen handelt es sich um die Verallgemeinerung der Ergebnisse, die wir aus der gewöhnlichen Algebra kennen. Wir werden die Untersuchungen im Rahmen der Sprache der ersten Stufe durchführen, wobei wir als Symbolmenge die Symbolmenge der gewöhnlichen Körper zusammen mit m neuen einstelligen Funktionssymbolen $\partial_1, \ldots, \partial_m$, die als Derivationen interpretiert werden sollen, wählen.

$$\mathrm{S} \overset{\text{def}}{=} \{+, -, \cdot, 0, 1\} \dot{\cup} \{\partial_1, \ldots, \partial_m\}$$

Mit dieser Symbolmenge lassen sich jetzt die Körper der Charakteristik 0 mit m paarweise kommutierenden Derivationen in der ersten Stufe axiomatisieren, man vergleiche dazu mit dem ersten Kapitel.

<u>**Definition**</u> **13** *Mit* $\mathbf{pDF}_0$ *sei der Zusammenschluß der folgenden Mengen von Sätzen der erste Stufe gemeint:*

1. *Die üblichen Axiome für die Körper der Charakteristik* 0.
2. $\{\forall x \forall y\, \partial_i(x+y) = \partial_i(x) + \partial_i(y) \mid 1 \leq i \leq m\}$
3. $\{\forall x \forall y\, \partial_i(x \cdot y) = \partial_i(x) \cdot y + x \cdot \partial_i(y) \mid 1 \leq i \leq m\}$
4. $\{\forall x\, \partial_i \partial_j(x) = \partial_j \partial_i(x) \mid 1 \leq i, j \leq m\}$

Die Modelle von $\mathbf{pDF}_0$ sind gerade die D-Körper der Charakteristik 0. Man beachte ferner, daß $\mathbf{pDF}_0$ eine Menge von $\forall\exists$-Sätzen, ihre Modellklasse daher induktiv ist.

Unser Interesse gilt naturgemäß der Untersuchung der Teilklasse der existentiell abgeschlossenen Strukturen in der Klasse der D-Körper. Wir wissen bereits wegen der Induktivität, daß jedes Modell von $\mathbf{pDF}_0$ eine existentiell abgeschlossene Erweiterung besitzt. Doch wie sehen diese Strukturen überhaupt aus? Unser wichtigstes Anliegen ist demnach, ein geeignetes Axiomensystem für die existentiell abgeschlossenen D-Körper anzugeben. Dieses Axiomensystem werden wir in Anlehnung an die übliche Algebra mit $\mathbf{pDCF}_0$, die Modelle von $\mathbf{pDCF}_0$ als differentiell abgeschlossene D-Körper bezeichnen.

Wir wollen uns jetzt der Untersuchung der existentiell abgeschlossenen Strukturen von $\mathbf{pDF}_0$ zuwenden. Eine Struktur M aus dieser Klasse muß ja folgendes leisten: Jede Existensaussage $\exists \bar{x}\ \phi(\bar{x}; \bar{a})$ mit Parametern $\bar{a} \in M^n$, die in einer Erweiterungsstruktur von M gilt, muß auch in M gelten. Die Gestalt des quantorenfreien S-Ausdruckes $\phi(\bar{x}; \bar{a})$ wollen wir jetzt modulo $\mathbf{pDF}_0$ vereinfachen. Dieses geschieht in völliger Analogie zum Vorgehen bei gewöhnlichen Körpern.

Wir machen zuerst eine augenscheinlich starke Einschränkung, weil wir nur einfache Existenzaussagen betrachten. Diese Vereinfachung wollen wir mit den schon erwähnten Analogiebetrachtungen begründen, später werden wir tatsächlich sehen, daß sie gerechtfertigt ist. Weiter nehmen wir ϕ in disjunktiver Normalform an und überlegen uns, daß wir modulo $\mathbf{pDF}_0$ nach Umordnen die atomaren und negiert atomaren Bestandteile von ϕ als D-Polynomgleichung $f(X) = 0$ bzw. Ungleichung $g(X) \neq 0$ auffassen können, wobei die Parameter den Koeffizienten der Polynome entsprechen. Wie üblich fassen wir die Ungleichungen eines Disjunktionsglieds zu einer einzigen zusammen, indem wir zu deren Produkt übergehen. Da die Gültigkeit von $\exists x\ (\chi(x) \vee \psi(x))$ äquivalent zu $\exists x\ \chi(x) \vee \exists x\ \psi(x)$ ist, ist es möglich, sich auf ein Disjunktionsglied zu beschränken. Modulo $\mathbf{pDF}_0$ nehmen wir also

$$\phi(x; \bar{a}) = f_1(x) \doteq 0 \wedge \ldots \wedge f_n(x) \doteq 0 \wedge g(x) \neq 0 \tag{3.1}$$

an, wobei die f_i und g D-Polynome mit den Koeffizienten $\bar{a}$ entsprechen.

Wenn wir das Gesagte jetzt von der Seite der Algebra aus betrachten, müssen wir uns um die Lösung von Gleichungssystemen, die die Gestalt aus (3.1) haben, kümmern. Unser Axiomensystem $\mathbf{pDCF}_0$ muß inhaltlich von einer Struktur M fordern, daß jedes solche System mit Koeffizienten aus M, welches überhaupt eine Lösung besitzt, bereits eine Lösung in M hat.

Die Lösbarkeit eines Systemes, wie es in (3.1) auftritt, ist aber genau dann gegeben, wenn ein primes Ideal, genauer ein primes D-Ideal existiert, das die Polynome $f_1, \ldots, f_n$ enthält, aber g nicht umfaßt. Unser Ziel muß es demnach also sein, solche Gleichungssysteme durch elementare Eigenschaften zu beschreiben, zu denen man ein entsprechendes Primideal finden kann. Wir werden das Problem in den nächsten Abschnitten schrittweise lösen.

3.1 Das Erzwingungsideal

In diesem ersten Schritt werden wir beginnen, das anfangs beschriebene Problem, ein D-Primideal zu finden, das die Ungleichung nicht, aber die Gleichungen eines Gleichungssystems enthält, zurückzuführen auf das Problem, ein radikales D-Ideal mit den beschriebenen Eigenschaften zu finden.

Definition 14 *Sei R ein D-Ring und $h \in R\{X\}$ ein D-Polynom. Ein radikales D-Ideal $\mathfrak{A}$ aus $R\{X\}$ heißt* **D-Erzwingungsideal** *bezüglich h, wenn gilt:*

1. *h ist kein Element von $\mathfrak{A}$.*
2. *$\mathfrak{A}$ ist maximal unter den radikalen D-Idealen, die h nicht enthalten.*

Für ein Erzwingungsideal gilt nämlich das Folgende.

Korollar 3.1.1 *Sei $h \in R\{X\}$ und $\mathfrak{A}$ ein D-Erzwingungsideal bzgl. h. Dann ist $\mathfrak{A}$ prim.*

Denn: Dieses ist ein Spezialfall des Lemmas 1.2.5. Betrachte $T \stackrel{\text{def}}{=} \{h^n \mid n \in \mathbb{N}\}$, wegen der Radikalität von $\mathfrak{A}$ kann kein h^n in $\mathfrak{A}$ liegen. Dadurch ist $\mathfrak{A}$ auch maximal unter den radikalen D-Idealen bzgl. des Ausschlusses von T. Also liefert 1.2.5, daß $\mathfrak{A}$ prim ist.

Nach diesem Korollar können wir uns auf die Fragestellung beschränken, welche $f_1, \ldots, f_n$ ein Erzwingungsideal bzgl. g besitzen, wenn wir feststellen wollen, ob $f_1(X) = 0, \ldots, f_n(X) = 0, g(X) \neq 0$ lösbar ist. Diese Frage kann jetzt weiter vereinfacht werden.

Lemma 3.1.2 *Sei $\mathfrak{A}$ ein radikales D-Ideal, das die Polynome $f_1, \ldots, f_n$ enthält, aber $g \notin \mathfrak{A}$ erfüllt.*
Dann existiert ein D-Erzwingungsideal $\mathfrak{M}$ bezüglich g, das $\mathfrak{A}$ umfaßt. (Insbesondere gilt $f_1, \ldots, f_n \in \mathfrak{M}$ und $g \notin \mathfrak{M}$.)

Beweis: Diese Existenz folgt mit Hilfe des Zornschen Lemmas. Wir betrachten die Menge M aller radikalen D-Ideale, die $\mathfrak{A}$ umfassen, aber g nicht enthalten. Diese Menge ist selbstverständlich partiell geordnet (bzgl. „$\subset$"). Eine total geordnete Teilmenge N von M besitzt eine obere Schranke in M, da $\mathfrak{M} \stackrel{\text{def}}{=} \bigcup_{\mathfrak{B} \in N} \mathfrak{B}$ ein radikales D-Ideal ist, was wir im 1. Kapitel bemerkt haben, und $\mathfrak{A}$ umfaßt. g kann nicht in $\mathfrak{M}$ liegen, sonst müßte es bereits in einem der $\mathfrak{B} \in N$ liegen! Also besitzt M maximale Elemente, insbesondere ist $\mathfrak{A}$ selbst in einem maximalen Element $\mathfrak{M}$ enthalten.
Dieses $\mathfrak{M}$ muß jetzt aber schon maximal in der Menge aller radikalen D-Ideale, die g nicht enthalten, d.h. ein D-Erzwingungsideal bzgl. g sein. Denn ein $\mathfrak{M}' \supsetneq \mathfrak{M}$ enthielte ja auch $\mathfrak{A}$, wäre also sogar schon Element von M, was ein Widerspruch zur Maximalität von $\mathfrak{M}$ in M wäre. □

Damit haben wir das Ziel dieses Abschnittes ereicht.

3.2 Kohärente Mengen

Jetzt werden wir noch eine weitere Art von selbstreduzierten Mengen von Polynomen kennenlernen, von denen wir uns dann überlegen, daß es diese sind, um deren Lösbarkeit wir uns kümmeren müssen. Als Referenz sei hierzu wiederum auf [KOLCHIN 1] verwiesen.

Wir wollen für eine selbstreduzierte Menge $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine weitere Konvention treffen.

Notation: Sei v eine X-Ableitung, dann setzen wir fest: $\mathcal{A}_v \overset{\text{def}}{=} \{\theta f \mid f \in \mathcal{A},\ \theta \in \Theta \text{ und } \theta u_f \ll v\}$.

Da eine X-Ableitung nur endlich viele $\ll$-Vorgänger haben kann, und eine selbstreduzierte Menge immer endlich ist, kann $\mathcal{A}_v$ auch nur endlich sein. Weiterhin ist festzustellen, daß es für zwei Polynome $f_i, f_j \in \mathcal{A}$ immer genau eine gemeinsame Ableitung von $u_{f_i} = \partial_1^{\nu_1} \cdots \partial_m^{\nu_m} X$, bzw. $u_{f_j} = \partial_1^{\mu_1} \cdots \partial_m^{\mu_m} X$ gibt, die unter den gemeinsamen Ableitungen kleinste Höhe hat (als Potenz der ∂_i wähle jeweils das kgV von ν_i und μ_i). Wir schreiben für diese $v_{ij} \overset{\text{def}}{=} \theta_{ij} u_{f_i} = \theta_{ji} u_{f_j}$, wobei θ_{ij} und θ_{ji} aus Θ eindeutig bestimmt sind.

Definition 15 *Sei $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine selbstreduzierte Menge von D-Polynomen. $\mathcal{A}$ heißt* **kohärent**, *falls gilt:*
Für je zwei $f_i, f_j \in \mathcal{A}$, mit $v_{ij} = \theta_{ij} u_{f_i} = \theta_{ji} u_{f_j}$ der kleinsten gemeinsamen X-Ableitung von u_{f_i} und u_{f_j}, existiert ein $n_{ij} \in \mathbb{N}$ mit

$$H_{\mathcal{A}}^{n_{ij}} (S_{f_j} \cdot \theta_{ij} f_i - S_{f_i} \cdot \theta_{ji} f_j) \in (\mathcal{A}_{v_{ij}}) \,.$$

Bemerkung 3.2.1 *Sei F ein D-Körper, $\mathfrak{p}$ ein primes D-Ideal von $F\{X\}$ und $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine charakteristische Menge von $\mathfrak{p}$.*
Dann ist $\mathcal{A}$ auch eine kohärente Menge von Polynomen.

Denn: Seien f und f' aus $\mathcal{A}$ gegeben mit kleinster gemeinsamer Ableitung der Leitableitungen $v = \theta u_f = \theta' u_{f'}$. Wir setzen $g \overset{\text{def}}{=} S_{f'} \cdot \theta f - S_f \cdot \theta' f'$. Da $\mathfrak{p} = \{x \in R\{X\} \mid \text{es ex. } n \in \mathbb{N} \text{ mit } H_{\mathcal{A}}^n x \in \langle \mathcal{A} \rangle\}$ nach Korollar 2.6.3 gilt, muß $g \in \mathfrak{p}$ sein, da $g \in \langle \mathcal{A} \rangle$ ist.
Weiter muß dieses g frei von v sein, da dieses heraussubtrahiert wird. Also $g \ll v$. Nun wählen wir mit Lemma 2.4.3 die n_i, m_i und $\bar{g}$ den Rest von g bzgl. $\mathcal{A}$ und wissen, daß sich $\prod_{i=1}^t I_{f_i}^{m_i} S_{f_i}^{n_i} g - \bar{g}$ als Linearkombination von Ableitungen $\theta_k f_k$ mit $\theta_k u_{f_k} \underline{\ll} u_g \ll v$, also Elementen aus $\mathcal{A}_v$ schreiben läßt. Da $\bar{g}$ reduziert bzgl. $\mathcal{A}$ ist, folgt mit Lemma 2.6.1, daß $\bar{g} \in (\mathfrak{p} \cap F) = (0)$, somit $\bar{g} = 0$ ist. Wenn wir jetzt $\prod_{i=1}^t I_{f_i}^{m_i} S_{f_i}^{n_i} g$ noch mit geeigneten Potenzen von I_{f_i} und S_{f_i} multiplizieren, erhalten wir gerade, daß für ein $m \in \mathbb{N}$ $H_{\mathcal{A}}^m g \in (\mathcal{A}_v)$ gilt, was wir nachweisen mußten.

Wir wollen als nächstes zeigen, daß die definierende Eigenschaft einer kohärenten Menge sogar für eine beliebige gemeinsame Ableitung w_{ij} zweier u_i, u_j erfüllt ist.

Lemma 3.2.2 *Sei $\mathcal{A}$ eine kohärente Menge von Polynomen. Es gilt: Für je zwei Polynome $f_1, f_2 \in \mathcal{A}$ und w eine beliebige gemeinsame Ableitung von u_{f_1} und u_{f_2}, wobei $w = \theta_1 u_{f_1} = \theta_2 u_{f_2}$ gelten soll, existiert ein $n \in \mathbb{N}$ mit*

$$H_{\mathcal{A}}^n(S_{f_2} \cdot \theta_1 f_1 - S_{f_1} \cdot \theta_2 f_2) \in (\mathcal{A}_v) \,.$$

Beweis: Sei M die Menge aller gemeinsamen X-Ableitungen von u_{f_1} und u_{f_2}. M ist eine Teilmenge der Menge aller X-Ableitungen, deswegen ist M durch $\ll$ wohlgeordent. Wir führen den Beweis per Induktion über $\ll$ in M.

Induktionsanfang: Sei v die kleinste gemeinsame Ableitung von u_{f_1} und u_{f_2}, dann gilt die Behauptung natürlich aufgrund der Definition einer kohärenten Menge.

Induktionsschritt: Sei dazu $w = \theta_1 u_{f_1} = \theta_2 u_{f_2}$ eine gemeinsame Ableitung von u_{f_1}, u_{f_2}, wir können w dann für geeignetes ∂_i und geeignete $\theta, \theta' \in \Theta$ darstellen als $w = \partial_i w'$, wobei $w' = \theta u_{f_1} = \theta' u_{f_2}$ der $\ll$-Vorgänger von w aus M ist. Auf w' trifft somit die Induktionsvoraussetzung zu. Man erkennt ebenso, daß wir $\theta_1 = \partial_i \theta$ und $\theta_2 = \partial_i \theta'$ erhalten. Nun teilen wir unser Vorgehen auf.

1. Schritt: $g \overset{\text{def}}{=} S_{f_2} \cdot \theta f_1 - S_{f_1} \cdot \theta' f_2$. Weil auf $w' = \theta u_{f_1} = \theta' u_{f_2}$ die I.V. zutrifft, existiert ein $m \in \mathbb{N}$ mit $H_{\mathcal{A}}{}^m g \in (\mathcal{A}_{w'})$. Wir erhalten:

$$\begin{array}{rrcl} & \partial_i(H_{\mathcal{A}}^m g) & = & m H_{\mathcal{A}}^{m-1} \cdot \partial_i H_{\mathcal{A}} \cdot g + H_{\mathcal{A}}^m \cdot \partial_i g \\ \text{gdw.} & H_{\mathcal{A}}^m \cdot \partial_i g & = & \partial_i(H_{\mathcal{A}}^m g) - m H_{\mathcal{A}}^{m-1} \cdot g \cdot \partial_i H_{\mathcal{A}} \\ \text{gdw.} & H_{\mathcal{A}}^{m+1} \cdot \partial_i g & = & H_{\mathcal{A}} \partial_i (H_{\mathcal{A}}^m g) - m H_{\mathcal{A}}^m \cdot g \cdot \partial_i H_{\mathcal{A}} \,. \end{array}$$

Da aber $\partial_i(H_{\mathcal{A}}{}^m g) \in (\mathcal{A}_{\partial_i w'})$ und $H_{\mathcal{A}}{}^m \cdot g \in (\mathcal{A}_{w'})$ sind, folgt $H_{\mathcal{A}}^{m+1} \cdot \partial_i g \in (\mathcal{A}_{\partial_i w'}) = (\mathcal{A}_w)$.

2. Schritt: Mit dem g aus dem 1. Schritt gilt weiter

$$\begin{array}{rcl} S_{f_2} \cdot \theta_1 f_1 - S_{f_1} \cdot \theta_2 f_2 & = & S_{f_2} \cdot \partial_i \theta f_1 - S_{f_1} \cdot \partial_i \theta' f_2 \\ & = & \partial_i(S_{f_2} \cdot \theta f_1 - S_{f_1} \cdot \theta' f_2) - \partial_i S_{f_2} \cdot \theta f_1 + \partial_i S_{f_1} \cdot \theta' f_2 \\ & = & \partial_i g - \partial_i S_{f_2} \cdot \theta f_1 + \partial_i S_{f_1} \cdot \theta' f_2 \,. \end{array}$$

Da $\theta u_{f_1} \ll w$ und $\theta' u_{f_2} \ll w$ erfüllt ist, sind laut Definition von $(\mathcal{A}_w)$ die beiden Polynome $\theta f_1, \theta' f_2$ bereits Elemente von $(\mathcal{A}_w)$, und wir erhalten nach Multiplikation mit $H_{\mathcal{A}}{}^n$ für ein geeignetes n gemäß des 1. Schrittes

$$H_{\mathcal{A}}^n(S_{f_2} \cdot \theta_1 f_1 - S_{f_1} \cdot \theta_2 f_2) = H_{\mathcal{A}}^n \partial_i g - H_{\mathcal{A}}^n \cdot \partial_i S_{f_2} \cdot \theta f_1 - H_{\mathcal{A}}^n \cdot \partial_i S_{f_1} \cdot \theta f_2 \ \in (\mathcal{A}_w) \,,$$

was zu zeigen war. □

Jetzt folgt das für unsere späteren Anwendungen wichtigste Ergebnis zu den kohärenten Mengen.

Lemma 3.2.3 *$\mathcal{A} = \{f_1, \ldots, f_t\}$ sei eine kohärente Menge von D-Polynomen in $R\{X\}$. Weiter sei $g \in R\{X\}$ partiell reduziert bezüglich $\mathcal{A}$, und es existiere ein $m \in \mathbb{N}$ mit $H_{\mathcal{A}}^m \cdot g \in \langle \mathcal{A} \rangle$.*
Dann existiert ein $n \in \mathbb{N}$, so daß $H_{\mathcal{A}}^n \cdot g \in (\mathcal{A})$ gilt.

Beweis: Wir haben $H_{\mathcal{A}}^m \cdot g \in \langle \mathcal{A} \rangle$, darum kann man eine Darstellung

$$H_{\mathcal{A}}^m \cdot g = \sum_{i=1}^{r} C_i \cdot \theta_i f_i + \sum_{j=1}^{s} D_j f_j \tag{3.2}$$

wählen, in der die C_i, D_j Elemente aus $R\{X\} \setminus \{0\}$ sind, und die $\theta_i \in \Theta$ alle $ord(\theta_i) > 0$ erfüllen sollen.
1. Fall: Es gibt eine Darstellung der Form (3.2), für die $r = 0$ gilt. Die Behauptung ist damit bewiesen, weil dann ja bereits diese Gleichung besagt, daß $H_{\mathcal{A}}^m \cdot g \in (\mathcal{A})$ ist.
2. Fall: Es gibt keine Darstellung der Form (3.2), für die $r = 0$ gilt. Wir können also für jede der Gleichungen (3.2) die endlich vielen X-Ableitungen $\theta_1 u_{f_1}, \ldots, \theta_r u_{f_r}$ (mit $ord(\theta_i) > 0$) betrachten, die in (3.2) auftreten, es muß jetzt mindestens eine geben! Unter diesen X-Ableitungen besitzt nun eine maximale Höhe, diese bezeichnen wir mit v_r.
Wir haben jetzt jeder Darstellung (3.2) eindeutig eine X-Ableitung v_r zugeordnet, unter all den so erhaltenen v_r muß es nun wiederum eines minimaler Höhe geben. Von nun an betrachten wir nur noch die zu diesem minimalen v_r gehörende Darstellung (3.2) und bezeichnen dieses v_r kurz mit v. Ohne Einschränkung können wir uns außerdem die Notation so wählen, daß $\theta_i u_{f_i} \ll \theta_j u_{f_j}$ oder $\theta_i u_{f_i} = \theta_j u_{f_j}$ gilt, falls $1 \leq i < j \leq r$ ist. für diese Notation existiert immer eine natürliche Zahl q, $1 \leq q \leq r$, so daß $\theta_j u_{f_j} \ll v$ für $1 \leq j < q$ und $\theta_j u_{f_j} = v$ für $q \leq j \leq r$ gilt. Multipliziere (3.2) mit S_{f_r}, das liefert uns:

$$\begin{aligned} S_{f_r} \cdot H_{\mathcal{A}}^m \cdot g &= \sum_{j=1}^{r} S_{f_r} \cdot C_j \cdot \theta_j f_j + \sum_{j=1}^{s} S_{f_r} \cdot D_j \cdot f_j \\ &= \sum_{j=1}^{q-1} S_{f_r} \cdot C_j \cdot \theta_j f_j + \sum_{j=q}^{r} C_j \cdot (S_{f_r} \cdot \theta_j f_j - S_{f_j} \cdot \theta_r f_r) \\ &\quad + \sum_{j=q}^{r} C_j \cdot S_{f_j} \cdot \theta_r f_r + \sum_{j=1}^{s} D'_j \cdot f_j \,. \end{aligned}$$

Wir haben $H_{\mathcal{A}} = \prod_{f \in \mathcal{A} \setminus \{f_r\}} I_f S_f \cdot I_{f_r} \cdot S_{f_r}$ nach Definition, weiterhin existieren für $q \leq j \leq r$ geeignete $n_j \in \mathbb{N}$, die $H_{\mathcal{A}}^{n_j}(S_{f_r} \cdot \theta_j f_j - S_{f_j} \cdot \theta_r f_r) \in (\mathcal{A}_v)$ ergeben, da ja für diese j $\theta_j u_{f_j} = v = \theta_r u_{f_r}$ gilt, und $\mathcal{A}$ kohärent ist. Die Multiplikation der letzten Gleichung mit $\prod_{j=q}^{r} H_{\mathcal{A}}^{n_j} \cdot \prod_{f \in \mathcal{A} \setminus \{f_r\}} I_{f_j} S_{f_j} \cdot I_{f_r}$ ergibt somit folgendes:

$$H_{\mathcal{A}}^{m'} g = \sum_{j=1}^{r'} C'_j \cdot \theta'_j f_j + \sum_{j=1}^{s'} D''_j f_j + \theta_r f_r \cdot E \,,$$

wobei $C'_j, D''_j, E \in R\{X\}$ sind, $ord(\theta'_j) > 0$ und $\theta'_j u_j \ll v$ für $1 \leq j \leq r'$ gilt. Nach Lemma (2.3.3) existiert ein $T \in R\{X\}$, $T \ll v$, mit $\theta_r f_r = S_{f_r} v + T$, was eingesetzt in die letzte Gleichung ergibt:

$$H_{\mathcal{A}}^{m'} g = \sum_{j=1}^{r'} C'_j \cdot \theta'_j f_j + \sum_{j=1}^{s'} D''_j f_j + E \cdot (S_{f_r} v + T)\,. \tag{3.3}$$

Da S_{f_r} kein Nullteiler ist, können wir das multiplikative System $S = \{S_{f_r}^n | n \in \mathbb{N}\}$ betrachten und den D-Ring $R'\{X\} \stackrel{\text{def}}{=} S^{-1}R\{X\}$ bilden, in dem wir durch Potenzen von S_{f_r} teilen können. Lese nun (3.3) als Gleichung in v im Ring $R'\{X\}$. Dabei stellen wir für die linke Seite fest, daß $v = \theta_r u_{f_r}$ nicht in g auftreten kann, da g partiell reduziert bzgl. $\mathcal{A}$ ist, ebenso kann $\theta_r u_{f_r}$ nicht in $H_{\mathcal{A}}$ auftreten. Für die rechte Seite halten wir fest, daß v zumindest nicht in T und den $\theta_j f_j$ vorkommt, da $T \ll v$ und $\theta_j f_j \ll v$ (für $1 \leq j \leq r'$). Nun setze in (3.3) $v = -\frac{T}{S_{f_r}}$ ein, wir erhalten:

$$H_{\mathcal{A}}^{m'} g = \sum_{j=1}^{r'} C_j^* \cdot \theta'_j f_j + \sum_{j=1}^{s'} D_j^* f_j \tag{3.4}$$

mit $C_j^*, D_j^* \in R'\{X\}$, $\theta'_j u_{f_i} \ll v$. Der Hauptnenner der hier auftretenden Elemente aus $S^{-1}R\{X\}$ ist eine Potenz von S_{f_r}, Multiplikation von 3.4 mit $H_{\mathcal{A}}$ in dieser Potenz liefert uns wieder eine Gleichung in $R\{X\}$:

$$H_{\mathcal{A}}^{n} g = \sum_{j=1}^{r'} \bar{C}_j \cdot \theta'_i f_i + \sum_{j=1}^{s'} \bar{D}_j f_j \tag{3.5}$$

mit $\bar{C}_j, \bar{D}_j \in R\{X\}$, $ord(\theta'_j) > 0$ und $\theta'_j u_{f_j} \ll v$, für $1 \leq j \leq r'$. Diese Gleichung ist nun wieder von der ursprünglichen Gestalt (3.2), und nach unserer Annahme muß $r' \neq 0$ gelten. Es gibt damit wieder ein $v_{r'}$, das jedoch kleinere Höhe als v haben muß, da ja alle $\theta'_j u_{f_j} \ll v$ sind. Das ist dann aber ein Widerspruch zu unserer Wahl von v! □

Anzumerken ist an dieser Stelle nochmals, daß wir für den D-Polynomring immer die Möglichkeit haben, diesen als Polynomring in unendlich vielen (algebraischen) Unbestimmten aufzufassen. Das bedeutet speziell für die obige Aussage, die ja eine Aussage über endlich viele Polynome ist, daß wir uns bereits auf einen Polynomring in nur endlich vielen Unbestimmten beschränken können. Wir stellen die Konsequenz dieses Lemmas, die wir über die kohärenten Mengen benutzen werden, nochmals explizit heraus.

Korollar 3.2.4 *Sei $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine kohärente Menge von Polynomen, $g \in R\{X\}$ reduziert bzgl. $\mathcal{A}$ und $H_{\mathcal{A}} g \notin \sqrt{(f_1, \ldots, f_t)}$ (in $R[X, \ldots, \theta X]$, mit θX höchste X-Ableitung in $f_1, \ldots, f_t, g$).*
Dann folgt: $H_{\mathcal{A}} \cdot g \notin \{\mathcal{A}\}_{\mathfrak{r}}$, dem von $f_1, \ldots, f_t$ in $R\{X\}$ erzeugten radikalen D-Ideal.

Denn: Angenommen, es gilt $H_\mathcal{A} \cdot g \in \{\mathcal{A}\}_\mathfrak{r}$, d.h. mit Lemma 1.2.3, es existiert ein $m \in \mathbb{N}$ mit $H_\mathcal{A}^m \cdot g^m = (H_\mathcal{A} \cdot g)^m \in \langle f_1, \ldots, f_t \rangle$. g^m ist zumindest noch partiell reduziert bzgl. $\mathcal{A}$, weswegen wir jetzt mit der Voraussetzung der Kohärenz und Lemma 3.2.3, angewandt auf g^m, schließen können, daß es ein $n \in \mathbb{N}$ gibt mit $H_\mathcal{A}^n \cdot g^m \in (f_1, \ldots, f_t)$. Für $l \stackrel{\text{def}}{=} kgV(m, n)$ können wir dann $(H_\mathcal{A} \cdot g)^l \in (f_1, \ldots, f_t)$ in $R\{X\}$, also bereits in $R[X, \ldots, \theta X]$ folgern. Das bedeutet aber $H_\mathcal{A} \cdot g \in \sqrt{(f_1, \ldots, f_t)}$.

Jetzt haben wir also ein Kriterium gewonnen, daß uns unsere Fragestellung insoweit beantwortet, daß wir sagen können: Für Polynome $f_1, \ldots, f_n$, die eine kohärente Menge $\mathcal{A}$ bilden, und g reduziert bzgl. dieser f_i, existiert ein radikales D-Ideal, damit dann auch ein D-Erzwingungsideal $\mathfrak{M}$ mit $f_i \in \mathfrak{M}$ und $H_\mathcal{A} g \notin \mathfrak{M}$, wenn es eine algebraische Lösung des Systems „$f_1 = 0 \wedge \ldots \wedge f_n = 0 \wedge H_\mathcal{A} g \neq 0$“ in einem Polynomring $F[X, \ldots, X_m]$ gibt. Es bleibt zu klären, ob sich jedes lösbare System auf diesen Fall zurückführen läßt.

3.3 Differentiell abgeschlossene Körper

Wir sind nun in der Lage, eine Teilklasse der D-Körper zu beschreiben, für die wir später Quantorenelimination nachweisen können. Jeder D-Körper besitzt eine Erweiterung in dieser Teilklasse, was aus den bisherigen Abschnitten folgt. Damit ergibt sich recht schnell, daß dieses die existentiell abgeschlossenen D-Körper sein müssen.
Zunächst müssen wir uns aber noch überlegen, ob diese Beschreibung eine Axiomatisierung in der 1. Stufe zuläßt.

Definition 16 *Ein Körper F heißt* **differentiell abgeschlossen**, *wenn:*

1. *F ist D-Körper ($F \models$ **pDF**$_0$).*
2. *F ist algebraisch abgeschlossen.*
3. *Für alle $f_1, \ldots, f_t, g \in F\{X\}$ mit $\mathcal{A} = \{f_1, \ldots, f_t\}$ eine kohärente Menge, g reduziert bzgl. $\mathcal{A}$ und $H_\mathcal{A} g \notin \sqrt{(f_1, \ldots, f_t)}$ (in $R[X, \ldots, \theta X]$) existiert ein $\alpha \in F$ mit $f_1(\alpha) = 0, \ldots, f_n(\alpha) = 0$ und $g(\alpha) \neq 0$ (als D-Polynome).*

Durch unsere Untersuchungen ist es jetzt möglich zu zeigen, daß jedes Modell von **pDF**$_0$ in einem differentiell abgeschlossen D-Körper enthalten ist, was aber nicht mehr überrascht, da wir ja über die Systeme aus Punkt *3)* wissen, daß es zu diesen $f_1, \ldots, f_t$ ein Erzwingungsideal bzgl. g gibt, wir müssen also nur sukzessive die Lösungen hinzuadjungieren.

Satz 3.3.1 *Jedes $K \models$ **pDF**$_0$ läßt sich zu einem $F \models$ **pDCF**$_0$ erweitern.*

Beweis: Zuerst wählt man einen algebraischen Abschluß $\bar{K}$ von K, der als separabler Erweiterungskörper nach Lemma 1.5.3 eine eindeutige D-Struktur besitzt, die die von K fortsetzt. $\bar{K}$ bezeichnen wir einfach wieder mit K.
Wir verwenden jetzt die übliche Kettenkonstruktion. Dazu zählen wir uns die Systeme von Polynomen aus $K\{X\}$ von der Gestalt aus *3)* der letzten Definition auf, etwa durch $(S_\beta)_{\beta<\gamma}$, wobei γ die Mächtigkeit von K sein soll. Mit $\mathfrak{p}_\beta$ bezeichnen wir das D-Erzwingungsideal bzgl. $H_{\mathcal{A}}g$, das die f aus S_β umfaßt. Man beachte immer, daß wir nachher $H_{\mathcal{A}}g(\alpha) \neq 0$ erhalten werden, woraus wir natürlich $g(\alpha) \neq 0$ folgern dürfen.
<u>1. Schritt:</u> Nun adjungieren wir die Lösungen dieser Systeme nacheinander hinzu, d.h. wir definieren uns induktiv (i.a. transfinit induktiv) ein aufsteigende Folge von Körper K_β durch $K_0 \stackrel{\text{def}}{=} K$, $K_\beta \stackrel{\text{def}}{=} Quot\,(K_{\beta-1}/\mathfrak{p}_{\beta-1})$ für eine Nachfolgerzahl β und $K_\lambda \stackrel{\text{def}}{=} \bigcup_{\alpha<\lambda} K_\alpha$ für eine Limeszahl λ. Daß wir bei Faktorisierung und Übergang zum Quotientenkörper einen D-Erweiterungskörper erhalten, haben wir im 1. Kapitel gesehen. Für den Vereinigungskörper nehmen wir für $1 \leq i \leq m$ $\partial_i^{K_\lambda} \stackrel{\text{def}}{=} \bigcup_{\alpha<\lambda} \partial_i^{K_\alpha}$, wobei $\partial_i^{K_\alpha}$ die Derivationen auf K_α bezeichnen sollen. $\partial_i^{K_\lambda}$ ist wohldefiniert, da für $\alpha < \beta < \lambda$ $\partial_i^{K_\beta}$ immer eine Fortsetzung von $\partial_i^{K_\alpha}$ ist. Die Ableitungs- und Vertauschungsregeln werden selbstverständlich auch auf $\partial_i^{K_\lambda}$ vererbt.
Wir definieren $F^{(1)} \stackrel{\text{def}}{=} K_\gamma$. Im D-Erweiterungskörper $F^{(1)}$ sind jetzt alle zu betrachtenden Systeme mit Koeffizienten aus K lösbar.
<u>2. Schritt:</u> Dieses Verfahren wenden wir induktiv an, denn $F^{(n)}$ sei der D-Körper, den wir erhalten, wenn wir $F^{(n-1)}$ gemäß dem 1. Schritt erweitern. Wir erhalten $F \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} F^{(n)}$. Natürlich gilt $K \subset F$ und in F sind jetzt alle Systeme der geforderten Art mit Koeffizienten aus F lösbar, da die Systeme nur endlich viele Koeffizienten enthalten, es wegen der aufsteigende Körperkette ein n geben muß, so daß alle Koeffizienten bereits in $F^{(n)}$ liegen. Damit ist das System dann nach Konstruktion in $F^{(n+1)} \subset F$ lösbar. □

<u>Satz</u> **3.3.2** *Die Definition 16 läßt sich durch eine (unendliche) Menge von Sätzen der 1. Stufe ausdrücken.*

Beweis: Zu den beiden ersten Punkten ist nichts mehr zu sagen, es ist klar wie diese zu formulieren sind.
Wir müssen also den dritten Punkt klären. Es liegt natürlich nahe, daß wir nacheinander alle X-Ableitungen $\theta_r X$ durchlaufen, und alle möglichen endlichen Mengen von Polynomen aus $F[X,\ldots,\theta_r X]$ aufzählen, und dann folgende Menge von Aussagen der Gestalt

$$\Big\{ f_1,\ldots,f_s (=\mathcal{A}) \text{ kohärent }, g \text{ red. bzgl. } \mathcal{A} \text{ und } H_{\mathcal{A}}g \notin \sqrt{(\mathcal{A})} \\ \Longrightarrow \exists x \ \textstyle\bigwedge_{i=1}^{n} f_i(x) \doteq 0 \wedge g(x) \neq 0 \quad \Big| \quad f_1,\ldots,f_s,g \in F\{X\} \Big\}$$

erhalten. Um $H_{\mathcal{A}}g \notin \sqrt{(\mathcal{A})}$ zu formulieren, haben wir gerade die algebraische Abgeschlossenheit gefordert. Denn mit dem Hilbertschen Nullstellensatz, der in einer Formulierung besagt, daß bei einem algebraisch abgeschlossenen Körper F $g \in \sqrt{(f_1, \ldots, f_s)}$ (in $F[X_1, \ldots, X_m]$) genau dann gilt, wenn es ein $\bar{\alpha} \in F^m$ gibt mit $f_1(\bar{\alpha}) = 0, \ldots, f_s(\bar{\alpha}) = 0$ und $g(\bar{\alpha}) \neq 0$, müssen wir jetzt bloß die Existenz eines solchen $\bar{\alpha}$ fordern.
Die Aussage über die f_i und g wandeln wir zuerst um in:

$$\begin{array}{l}\bigwedge_{i=1}^{s} f_i \text{ reduziert bzgl. } \mathcal{A} \setminus \{f_i\} \text{ und } g \text{ reduziert bzgl. } \mathcal{A} \text{ und} \\ \bigwedge_{i=1}^{s} \bigwedge_{j=i}^{i-1} \bigvee_{n \in \mathbb{N}} H_{\mathcal{A}}^n \cdot g \cdot h_{ij} \in (\mathcal{A}_{v_{ij}})\ ,\end{array}$$

wobei wir die Abkürzung $h_{ij} \overset{\text{def}}{=} S_{f_j} \cdot \theta_{ij} f_i - S_{f_i} \cdot \theta_{ji} f_j$ verwenden. Zuerst sagen wir, daß die f_i nicht-konstant sind, das muß ja für selbstreduzierte Mengen immer gelten. Um auszudrücken, daß Polynome reduziert zueiander sind, müssen wir jeweils Aussagen über die Parameter in den Polynomen machen, die vor den X-Ableitungen stehen. Wenn wir z.B. zwei Polynome f_1, f_2 aus $F[X, \ldots, \theta_l X]$ haben, müssen wir nacheinander die endlich vielen Fälle abhandeln, was erfüllt sein muß, wenn $\theta_r X = \theta_l X$ oder $\theta_r X \ll \theta_l X$ Leitableitung von f_1, bzw. f_2 sein soll. Das können wir durch „es gibt einen von Null verschiedenen Koeffizienten vor einem Term mit $\theta_r X$ in f_1“ sagen. Da $\theta_r X$ höher ist als die anderen möglichen X-Ableitungen, hieße das, daß $\theta_r X$ die Leitableitung wäre. In diesem Fall müssen wir dann weiter fordern, daß in f_2 alle Koeffizienten von Termen, die Monome mit $\theta_r X$ und Ableitungen davon enthalten, verschwinden. So verfahren wir weiter, wenn wir sagen wollen, daß eine X-Ableitung, die kleiner als $\theta_r X$ ist, die Leitableitung sein soll (wenn $\theta_r X$ nicht und wenn $\theta_{r-1} X$ auftritt, dann ...). Damit haben wir gesagt, daß f_2 partiell reduziert bzgl. f_1 ist. Und so verfahren wir analog für f_2, indem wir sukzessive durch „Wenn“-Abfragen sagen: Wenn alle höheren (bis $\theta_r X$) X-Ableitungen, nicht aber dieses θX in f_2 auftritt, darf diese X-Ableitung und Ableitungen davon nicht in f_1 auftreten. Damit hätten wir jetzt gesagt: „$\{f_1, f_2\}$ ist eine partiell reduzierte Menge“.
Beim Abfragen, welches der θX die Leitableitung ist, können wir natürlich auch die möglichen Potenzen in absteigender Reihenfolge durchtesten, und somit feststellen, welches die Leitableitung und welches ihre höchste Potenz in dem betreffenden Polynom ist. Es ist klar, wie man dann für das andere Polynom wieder sagen kann, daß θX nur in kleinerer Potenz vorkommen soll. Wir haben also „$\{f_1, f_2\}$ ist reduziert“ formuliert.
Selbstverständlich kann man das jetzt auf jede beliebige endliche Menge von Polynomen $\{f_1, \ldots, f_s\}$ anwenden, und auf dieselbe Art und Weise für ein weiteres Polynom g auch sagen: „g reduziert bzgl. $\{f_1, \ldots, f_s\}$“. Wir nutzen dabei immer aus, daß für feste $f_1, \ldots, f_s, g$ nur endlich viele Paramter auftreten, und wir alle möglichen Kombinationen der oben angegeben Abfragen für die Parameter aufschreiben können.
Bleibt noch zu überlegen, wie sich die spezielle Eigenschaft einer kohärenten Men-

ge ausdrücken läßt. Für ein Paar f_i, f_j ist uns bekannt, daß $A_{v_{ij}}$ eine endliche Menge ist. Die Zugehörigkeit eines Polynomes g zu dem von $A_{v_{ij}}$ im D-Polynomring erzeugten (algebraischen) Ideal müssen wir durch die Existenz von Koeffizienten-Polynomen vor den Elementen aus $A_{v_{ij}}$ ausdrücken, was wir wieder durch die Aussage schaffen: Es gibt ein Parametertupel (für die Koeffizienten-Polynome) ungleich dem Null-Tupel, und g ist Linearkombination aus diesen Polynomen. Um alle möglichen Koeffizienten-Polynome abzufragen, müssen wir nacheinander alle endlichen Polynomringe $F[X, \ldots, \theta X]$, und in diesen alle möglichen Potenzen zulassen, was sich durch unendlich viele solcher $\exists$-Aussagen, bei denen über immer mehr Parameter quantifiziert wird, erreichen läßt.
Wir haben allerdings das Problem, daß wir ja $\bigvee_{n\in\mathbb{N}} H_{\mathcal{A}}^n h_{ij} \in A_{v_{ij}}$ sagen müssen, es gilt eine unendliche Disjunktion, genauer eine endliche Konjunktion solcher Disjunktionen, die wir zu einer einzigen zusammenfassen, auszudrücken. Das bereitet uns keine Schwierigkeiten, da unser Axiomen-Schema von der Gestalt $\{\ldots \bigvee_{n\in\mathbb{N}} \phi_n \longrightarrow \psi \mid f_1, \ldots, f_s, g\}$ ist, eine Disjunktion in der Prämisse einer Implikation aber immer durch eine unendliche Konjunktion der Art $\bigwedge_{n\in\mathbb{N}} \neg\phi_n \wedge \psi$ ersetzt werden kann. Damit können wir n als zusätzlichen Paramter für unser unendliches Axiomen-Schema hinzunehmen, also die Menge $\{\ldots \bigwedge_k^n \neg\phi_n \wedge \psi \mid f_1, \ldots, f_s, g; n\}$. Für uns bedeutet das Gesagte demnach, daß wir eine Menge von Axiomen der Gestalt

$$\Big\{\mathcal{A} \text{ kohärent }, g \text{ red. bzgl. } \mathcal{A}\ , H_{\mathcal{A}}^n g \notin \sqrt{(\mathcal{A})} \longrightarrow \exists x\ (\textstyle\bigwedge_{i=1}^n f_i(x) \doteq 0$$
$$\wedge g(x) \not\doteq 0)\Big| \quad \underbrace{f_1, \ldots, f_s}_{\mathcal{A}}, g \in F\{X\}\ ,\ n \in \mathbb{N}\Big\}$$

für den Punkt *3)* angeben müssen. □

<u>**Notation:**</u> Wir bezeichnen die (unendliche) Menge von 1. Stufe-Sätzen aus Definition 16 mit $\mathbf{pDCF}_0$.

3.4 Quantorenelimination für pDCF$_0$ und Anwendungen

Nun bereiten wir den Nachweis der Quantorenelimination durch ein Lemma vor. Es sei noch bemerkt, falls wir ein $F \models \mathbf{pDF}_0$ gegeben haben und eine Substruktur k von F betrachten, daß dann k ein D-Ring ist. $F \sqsupseteq k$ ist also insbesondere eine D-Ringerweiterung. Falls $F \models \mathbf{pDCF}_0$ gilt, und die Substruktur k ein Körper ist, können wir einen algebraischen Abschluß von k in F wählen,da ja F insbesondere auch algebraisch abgeschlossen ist. F ist dann sogar ein separabler Erweiterungskörper von k, da wir Charakteristik 0 haben.

Lemma 3.4.1 *Sei $F \models \mathbf{pDF}_0$ und $k \sqsubseteq F$ eine Substruktur von F.*

a) $Quot_F(k)$, der Quotientenkörper von k in F ist S-abgeschlossen. Je zwei beliebige Quotientenkorper von k mit einer Fortsetzung der D-Struktur sind über k D-isomorph.

b) Sei $F \supset k$ sogar eine D-Körpererweiterung. Weiterhin sei ein Zwischenkörper $F \supset K \supset k$ mit $K \supset k$ separabel algebraisch gegeben. Dann ist K in F S-abgeschlossen, und somit Träger einer Substruktur.

c) Sei wieder zusätzlich $k \models \mathbf{pDF}_0$, $\bar{k}_F$ der in F gewählte und $\bar{k}$ ein beliebiger algebraische Abschluß von k. Dann existiert ein D-Isomorphismus von $\bar{k}$ nach $\bar{k}_F$, der auf k die Identität ist.

Beweis: Zu a) Dieses folgt unmittelbar aus Satz 1.3.3.

Zu b) Wir müssen uns einzig überlegen, daß K unter den Derivationen abgeschlossen ist.
Die Derivationen von k werden durch die von F fortgesetzt. Die von K in F erzeugte Struktur $[K]^F$ ist eine Erweiterung von k, deren Derivationen die von k fortsetzen. Da K eine separable Erweiterung von k ist, wissen wir mit der Gleichung (1.4) aus Lemma 1.5.1, daß die Bilder von Elementen aus K unter Derivationen durch die Minimalpolynome vorgeschrieben sind und bereits in K liegen.

Zu c) Wir wissen mit b), daß $\bar{k}$ Substruktur von F ist. Seien $\partial'_1, \ldots, \partial'_m$ die Fortsetzungen der Derivationen auf $\bar{k}$, bzw. $\partial_1, \ldots, \partial_m$ die auf $F \supset \bar{k}_F$ gegebenen. Da $\bar{k}$ und $\bar{k}_F$ zwei algebraische Abschlüsse von k sind, existiert ein k-Isomorphismus $\pi : \bar{k} \to \bar{k}_F$. Wir definieren auf $\bar{k}$ neue Abbildungen γ_i durch $\gamma_i \stackrel{\text{def}}{=} \pi^{-1} \circ \partial_i \circ \pi$ für $1 \leq i \leq m$. Wie man unmittelbar nachrechnet, sind die γ_i Derivationen auf $\bar{k}$, und weil wir $\pi\restriction_k = id_k$ haben, sind sie sogar Fortsetzungen der $\partial_i\restriction_k$. Wir wissen aber, daß die Fortsetzungen der Derivationen eindeutig sind, weswegen $\pi^{-1} \circ \partial_i \circ \pi = \gamma_i = \partial'_i$ gelten muß. Das bedeutet aber gerade, daß π bereits ein D-Isomorphismus mit $\pi\restriction_k = id_k$ ist. □

Um die Quantorenelimination für $\mathbf{pDCF}_0$ zu zeigen, wollen wir ein bekanntes Kriterium testen, das man z.B. in [PRESTEL] auf S. 187 findet. Dieses fordert von uns nur die Überprüfung einfacher Existenzaussagen, wewegen unsere Beschränkung auf eine Variable jetzt gerechtfertigt ist.

Satz 3.4.2 $\mathbf{pDCF}_0$ *hat Quantorenelimination.*

Beweis: Seien dazu zwei Modelle F_1 und F_2 von $\mathbf{pDCF}_0$ mit einer gemeinsamen Substruktur k gegeben. Weiter sei $\phi(x;\bar{a})$ eine einfache Existenzaussage mit Parametern aus k, für die $F_1 \models \phi(x;\bar{a})$ gilt. Es ist $F_2 \models \phi(x;\bar{a})$ zu zeigen.

Als erstes machen wir ohne Einschränkungen folgende Annahmen über k: wir nehmen an, daß $k \models \mathbf{pDF}_0$ gilt, da wir jeweils zu den Quotientenkörpern übergehen und dann mit Lemma 3.4.1 a) argumentieren können. Zweitens wissen wir ebenso durch Lemma 3.4.1 c), daß die algebraischen Abschlüsse von k in F_1, bzw. F_2 D-isomorph über k sind. Das rechtfertigt es, k algebraisch abgeschlossen anzunehmen.
Zum Dritten erinnern wir an den Anfang dieses Kapitels, wo wir uns überlegt haben, daß wir eine einfache Existenzaussage modulo $\mathbf{pDF}_0$ von der Gestalt $\exists x\ (\bigwedge_{i=1}^{s} f_i(x) \doteq 0 \wedge g(x) \not\doteq 0)$ annehmen können, wobei wir uns die f_i und g als Polynome aus $k\{X\}$ vorstellen. Wir setzen somit $F_1 \models \exists x\ (\bigwedge_{i=1}^{s} f_i(x) \doteq 0 \wedge g(x) \not\doteq 0)$ voraus.
<u>1. Fall:</u> Es gilt $s = 0$, wir müssen also zeigen, daß es in F_2 ein α gibt mit $g(\alpha) \neq 0$. Aber die Axiome unter *3)* sichern speziell die Existenz einer Lösung für „$g \not\doteq 0$“.
<u>2. Fall:</u> $s > 0$, es gibt also ein $\alpha \in F_1$ mit $f_i(\alpha) = 0$, $1 \leq i \leq s$, und $g(\alpha) \neq 0$. Wähle dann $\mathfrak{p} \stackrel{\text{def}}{=} \{h \in k\{X\} \mid h(\alpha) = 0\}$, das g nicht, aber die f_i enthält. Sei $\mathcal{A} = \{f_1', \ldots, f_t'\}$ eine charakteristische Menge von $\mathfrak{p}$, die gemäß Bemerkung 3.2.1 kohärent ist. Natürlich gilt auch für diese Polynome $f_i'(\alpha) = 0$. Jetzt müssen wir noch mit Lemma 2.4.3 von g aus zum Rest $\bar{g}$ von g bzgl. $\mathcal{A}$ übergehen, somit haben wir für passende $m_i', n_i' \in \mathbb{N}$:

$$\prod_{i=1}^{t} I_{f_i'}^{m_i'} S_{f_i'}^{n_i'} g - \bar{g} \in \langle f_1', \ldots, f_t' \rangle\ . \tag{3.6}$$

Da $I_{f_i}(\alpha) \neq 0$, $S_{f_i}(\alpha) \neq 0$ und $H_{\mathcal{A}}(\alpha) \neq 0$ gilt, weil $\mathcal{A}$ eine charakteristische Menge von $\mathfrak{p}$ ist, erhalten wir $\bar{g}(\alpha) \neq 0$.
Wenn wir jetzt „$f_1' \doteq 0, \ldots, f_t' \doteq 0, \bar{g} \not\doteq 0$“ (*) als System von Polynomen in einem Polynomring $k[X, \ldots, \theta X]$ auffassen, besagt die Existenz unseres α insbesondere auch die Existenz einer algebraischen Lösung $\bar{a} \in F_1^m$, nämlich $(\alpha, \ldots, \theta\alpha)$. Da wir k als algebraisch abgeschlossen annehmen können, gibt es eine Lösung bereits in $\bar{k}$. Damit erfüllt das System (*) die Voraussetzung eines Axiomes aus *3)* der Definition für $\mathbf{pDCF}_0$, somit existiert wegen $F_2 \models \mathbf{pDCF}_0$ ein $\beta \in F_2$, eine D-Lösung für (*) in F_2.
Wir müssen jetzt nur noch zurückverfolgen, ob dieses β die ursprünglichen Polynome ebenfalls in der gewünschten Weise löst. (3.6) liefert aber gerade $g(\beta) \neq 0$ und $I_{f_i}(\beta) \neq 0$, $S_{f_i}(\beta) \neq 0$ f.a. i. Somit muß $H_{\mathcal{A}}(\beta) \neq 0$ sein. Da es für die Elemente f_i aus $\mathfrak{p}$ ein $n_i \in N$ mit $H_{\mathcal{A}}^{n_i} f_i \in \langle f_1', \ldots, f_t' \rangle$ geben muß, $H_{\mathcal{A}}(\beta)$ aber ungleich 0 ist, sind alle $f_i(\beta) = 0$.Mit diesem β können wir demnach $F_2 \models (f_1(x) \doteq 0 \wedge \ldots \wedge f_s(x) \doteq 0 \wedge g(x) \not\doteq 0)[\beta]$ schließen. □

Wir wollen jetzt zeigen, daß $\mathbf{pDCF}_0$ der Modellbegleiter von $\mathbf{pDF}_0$ ist. Da ja der Modellbegleiter insbesondere mit den existentiell abgeschlossenen Strukturen von $\mathbf{pDF}_0$ zusammenfällt, wäre damit also die Axiomatisierung gelungen.

Satz 3.4.3 $\mathbf{pDCF}_0$ *ist der Modellbegleiter, und axiomatisiert damit die Klasse der existentiell abgeschlossenen Strukturen von* $\mathbf{pDF}_0$.

Beweis: Als Modellbegleiter muß $\mathbf{pDCF}_0$ drei Bedingungen erfüllen: *(i)*$\mathbf{pDF}_0 \subset \mathbf{pDCF}_0$, *(ii)*$\mathbf{pDCF}_0$ ist modellvollständig und *(iii)* jedes Modell von $\mathbf{pDF}_0$ läßt sich zu einem Modell von $\mathbf{pDCF}_0$ erweitern.
Die ersten beiden Punkte sind durch die Definition, bzw. die Qantorenelimination, die immer Modellvollständigkeit impliziert, von $\mathbf{pDCF}_0$ klar, der dritte ist nach Lemma 3.3.1 erfüllt. □

Zusätzlich kennt man in der Modelltheorie noch den Begriff der Modellvervollständigung. Damit bezeichnet man den Modellbegleiter $\Sigma^* \supset \Sigma$, falls dieser für alle $A \models \Sigma$ und $B, C \models \Sigma^*$ mit $A \subseteq B$ und $A \subseteq C$ zusätzlich $(B, (a)_{a\in A}) \equiv (C, (a)_{a\in A})$ erfüllt, was als allgemeine Form des Hilbertschen Nullstellensatzes bezeichnet wird. Es ist wohlbekannt, daß für eine $\forall\exists$-Menge Σ der Modellbegleiter Σ^* diese Eigenschaft besitzt, falls Σ^* Quantorenelimination hat.

Satz 3.4.4 $\mathbf{pDCF}_0$ *ist die Modellvervollständigung von* $\mathbf{pDF}_0$.

Schließlich sei noch bemerkt, daß wir mit $\mathbf{pDCF}_0$ dieselben D-Körper meinen, die Kolchin als „*constrainedly closed*“ bezeichnet hat. Man vergleiche mit der Prop. 3 auf S. 145 aus [KOLCHIN 2].

Bemerkung 3.4.5 *Ein D-Körper F ist genau dann „constrainedly closed“, wenn er differentiell abgeschlossen ist.*

Denn: In einem „constrainedly closed“ Körper F gilt (iii) aus der gerade zitierten Proposition. Sei $\mathcal{A}$ eine kohärente Menge und ein bzgl. dieser reduziertes Polynom g mit $H_{\mathcal{A}}g \notin \sqrt{(\mathcal{A})}$ gegeben, dann wissen wir, daß es eine Erzwingungsideal $\mathfrak{M}$ bzgl. $H_{\mathcal{A}}g$ und $\mathfrak{M} \supset \mathcal{A}$ gibt. Mit (iii) gibt es ein $\alpha \in F$, für daß $H_{\mathcal{A}}g(\alpha) \neq 0$, damit $g(\alpha) \neq 0$ und $h(\alpha) = 0$ f.a.$h \in \mathfrak{M}$, damit $f(\alpha) = 0$ f.a.$f \in \mathcal{A}$. F ist somit differentiell abgeschlossen.
Umgekehrt sei jetzt ein Primideal $\mathfrak{p}$ und ein $g \notin \mathfrak{p}$ vorgegeben. Wähle eine charakteristische Menge von $\mathfrak{p}$, die damit wieder kohärent ist, dann wähle $\bar{g}$, den Rest von g bzgl. $\mathcal{A}$. $g \notin \mathfrak{p}$, d.h. mit 2.6.3 für kein $n \in \mathbb{N}$ ist $H_{\mathcal{A}}^n g \in \langle\mathcal{A}\rangle$, also $(H_{\mathcal{A}}g)^n \notin \langle\mathcal{A}\rangle$, was wiederum $H_{\mathcal{A}}g \notin \{\mathcal{A}\}_{\mathfrak{r}}$ bedeutet, was $H_{\mathcal{A}}g \notin \sqrt{(\mathcal{A})}$ in einem geeigneten Ring $F[X, \ldots, \theta X]$ zur Folge hat. Damit gibt es nach $\mathbf{pDCF}_0$ eine gemeinsame Nullstelle α für die Polynome aus $\mathcal{A}$ und $H_{\mathcal{A}}g(\alpha) \neq 0$ (d.h. wieder $H_{\mathcal{A}}(\alpha) \neq 0$ und $g(\alpha) \neq 0$). Für alle Polynome h aus $\mathfrak{p}$ gilt aber mit passendem n: $(H_{\mathcal{A}}(\alpha))^n h(\alpha) = 0$, somit $h(\alpha) = 0$.

Jeder D-Körper, den wir untersuchen, enthält $\mathbb{Q}$ als Primkörper. In der Bemerkung 1.1.1 haben wir gezeigt, daß jede Derivation auf $\mathbb{Q}$ trivial sein muß. Also ist die Struktur $\mathbb{Q}$ mit m trivialen Derivationen in jedem D-Körper enthalten, sie ist eine Primsubstruktur. Eine Theorie mit Quantorenelimination, die eine Primsubstruktur besitzt, ist bekanntlich vollständig.

Satz 3.4.6 $\mathbf{pDCF}_0$ *ist vollständig.*

Nun wollen wir als eine der üblichen Anwendungen den Nullstellensatz angeben. Dieser geht auf [SEIDENBERG] zurück.

Satz 3.4.7 (Nullstellensatz; Seidenberg)
k sei ein D-Körper und $f_1, \ldots, f_n, g \in k\{X\}$. Existiert in einem D-Erweiterungskörper von k eine Lösung für

$$f_1(X) = 0 \wedge \ldots \wedge f_n(X) = 0 \wedge g(X) \neq 0 \; , \tag{3.7}$$

dann existiert in jeder *D-Erweiterung $F \supset k$ und $F \models \mathbf{pDCF}_0$ eine Lösung.*

Beweis: Wir müssen lediglich die Eigenschaft der Modellvervollständigung anwenden. Sei $K \supset k$ die Erweiterung, in der (3.7) lösbar ist. Wir erweitern K wiederum zu einem $F_K \models \mathbf{pDCF}_0$, weiter sei $F \models \mathbf{pDCF}_0$ eine beliebige Erweiterung von k. Wir haben für diese Situation: $(F_K, (a)_{a \in k}) \equiv (F, (a)_{a \in k})$. Nach Voraussetzung haben wir $(F_K, (a)_{a \in k}) \models \exists x \, (\bigwedge_{i=1}^n f_i(x) \doteq 0 \wedge g(x) \not\doteq 0)$, was sich dann zu $(F, (a)_{a \in k}) \models \exists x \, (\bigwedge_{i=1}^n f_i(x) \doteq 0 \wedge g(x) \not\doteq 0)$ überträgt, was zu zeigen war. $\square$

3.5 ω-Stabilität und das Primmodell

Ein weiteres Ziel ist es, die ω-Stabilität für $\mathbf{pDCF}_0$ nachzuweisen. Wenn wir das geschafft haben, können wir die Sätze von Morley und Shelah über Primmodelle anwenden.

Der entscheidende Schritt ist nun, die Quantorenelimination auszunutzen. Diese besagt ja, das jeder Ausdruck $\phi(\bar{x}; \bar{y})$ äquivalent zu einem quantorenfreien Ausdruck ($\bar{y}$ sollen die möglichen Parameter sein) ist, den wir in disjunktiver Normalform annehmen können. Somit ist ϕ von der Gestalt

$$\phi(\bar{x}; \bar{y}) = \bigvee_{j=1}^{s} f_{j1}(\bar{x}) \doteq 0 \wedge \ldots \wedge f_{jt_j}(\bar{x}) \doteq 0 \wedge g(\bar{x}) \not\doteq 0 \; ,$$

die Ungleichungen haben wir wieder zu einer einzigen zusammengefaßt. Die Gültigkeit eines Ausdruckes ϕ hängt demnach nur von der Gültigkeit eines Geichungssystems $f_1 = 0 \wedge \ldots \wedge f_t = 0 \wedge g \neq 0$ ab.
Mit $S_1(A)$ werden wir im weiteren die (vollständigen) 1-Typen eines Modelles M von $\mathbf{pDCF}_0$ mit Parametern aus A bezeichnen, wobei A Teilmenge dieses Modelles sein soll.
Zunächst ist es möglich zu zeigen, daß für einen D-Körper K auf der einen Seite die D-Primideale aus $K\{X\}$ eineindeutig den 1-Typen aus $S_1(K)$ auf der anderen entsprechen. Wir bereiten das vor: Sei $q \in S_1(K)$, dann ist $\mathfrak{p}_q \stackrel{\text{def}}{=} \{f \in$

$K\{X\} \mid$ „$f(x) \doteq 0$“ $\in q\}$ ein primes D-Ideal. Wenn wir „$h(x) \doteq 0$“ $\in q$ haben, gibt es ein $K \subset F \models \mathbf{pDCF}_0$ mit $F \models h(x) \doteq 0[a]$ für ein $a \in F$. Für ein beliebiges ∂_i gilt $(\partial_i h)(a) = 0$, d.h. $\partial_i h \in \mathfrak{p}_q$. $\mathfrak{p}_q$ ist prim, da für $h_1 h_2 \in \mathfrak{p}_q$ nach Definition „$h_1 h_2(x) \doteq 0$“ ein Element von q ist. In dem zugehörigen F gibt es ein a, für das dann $h_1 h_2(a) = h_1(a) h_2(a) = 0$, also $h_1(a) = 0$ oder $h_2(a) = 0$ gilt. Wegen der Vollständigkeit erhalten wir „$h_1(x) \doteq 0$“ $\in q$ oder „$h_2(x) \doteq 0$“ $\in q$, damit $h_1 \in \mathfrak{p}_q$ oder $h_2 \in \mathfrak{p}_q$.

<u>**Lemma**</u> **3.5.1** *K sei ein D-Körper. Die Abbildung $q \mapsto \mathfrak{p}_q$ ist eine Bijektion von $S_1(K)$ auf die Menge der D-Primideale in $K\{X\}$.*

Beweis: Die Injektivität dieser Abbildung überlegen wir uns, indem wir uns zwei verschiedene 1-Typen $q_1 \neq q_2$ vorgeben. Es gibt also ein ϕ mit $\phi \in q_1$ aber $\phi \notin q_2$, wegen der Vollständigkeit dann $\neg\phi \in q_2$. Wir wissen, daß es demnach $f_1, \ldots, f_t, g$ geben muß mit $f_1 \doteq 0 \wedge \ldots \wedge f_t \doteq 0 \wedge g \not\doteq 0 \in q_1$, aber die Negation davon $f_1 \not\doteq 0 \vee \ldots \vee f_t \not\doteq 0 \vee g \doteq 0 \in q_2$ ist. Das bedeutet aber, daß eines der f_i nicht in $\mathfrak{p}_{q_2}$ enthalten oder $g \in \mathfrak{p}_{q_2}$ ist, andererseits aber $f_i \in \mathfrak{p}_{q_1}$ f.a. i und $g \notin \mathfrak{p}_{q_1}$ erfüllt ist. Das bedeutet $\mathfrak{p}_{q_1} \neq \mathfrak{p}_{q_2}$, die Injektivität.

Für die Surjektivität müssen wir uns ein $\mathfrak{p} \in K\{X\}$ vorgeben. Wir konstruieren

$$K \overset{\imath}{\hookrightarrow} K\{X\} \overset{kan}{\twoheadrightarrow} K\{X\}/\mathfrak{p} \overset{\imath}{\hookrightarrow} Quot\,(K\{X\}/\mathfrak{p}) \overset{\text{def}}{=} F\,.$$

Sei α das Bild von X in F, dann erfüllt ein $h \in K\{X\} \subset F\{X\}$ $h(\alpha) = 0$ genau dann, wenn $h \in \mathfrak{p}$. F erweitern wir nun zu einem differentell abgeschlossenen D-Körper gemäß 3.3.1, diesen Körper bezeichnen wir wieder mit F. Wir betrachten $q \overset{\text{def}}{=} tp_F(\alpha|K)$. Wegen $h(\alpha) = 0$ gdw. $h \in \mathfrak{p}$ folgt $\mathfrak{p}_q = \mathfrak{p}$, also ist q ein Urbild zu $\mathfrak{p}$. $\square$

Mit diesem Lemma können wir jetzt sofort die ω-Stabilität für $\mathbf{pDCF}_0$ nachweisen.

<u>**Satz**</u> **3.5.2** $\mathbf{pDCF}_0$ *ist ω-stabil.*

Beweis: Wir müssen für eine Teilmenge $A \subset F$, wobei F ein Modell von $\mathbf{pDCF}_0$ ist, mit $|A| \leq \omega$ nachweisen, daß $|S_1(A)| \leq \omega$ gilt.
Als erstes gehen wir in einem Modell $F \supset A$ von $\mathbf{pDCF}_0$ zum von A erzeugten D-Unterkörper in F über, dessen Mächtigkeit dann nicht größer als ω sein kann. Natürlich gilt $|S_1(A)| \leq |S_1(K)|$. Da nach dem letzten Lemma sich 1-Typen aus $S_1(K)$ und prime D-Ideale aus $K\{X\}$ eindeutig entsprechen, haben wir $|S_1(K)| = |\{\mathfrak{p} \subset K\{X\} \mid \mathfrak{p}$ primes D-Ideal$\}|$. Für radikale D-Ideale, und damit insbesondere für D-Primideale, wissen wir mit dem Basissatz, daß diese durch endlich viele D-Polynome bestimmt sind, wir können demnach die Anzahl der Ideale durch die Anzahl aller endlichen Teilmengen von $K\{X\}$ abschätzen. Es gibt $max(|\mathbb{N}|, |K|)$,

also in diesem Falle ω viele endliche Teilmengen. Wir erhalten die gewünschte Abschätzung

$$|S_1(A)| \leq |S_1(K)| \leq |\{\mathcal{N} \subset K\{X\} \mid \mathcal{N} \text{ endlich}\}| = \omega .$$

$\square$

Ein Modell M heißt *atomar* über $A \subset M$, wenn für jedes n jedes Tupel $\bar{a}^n \in \bar{A}^n$ einen Haupttypen realisiert. Sei Σ eine vollständige Theorie, $M \models \Sigma$ und $A \subset M$. Wir bezeichnen M bekanntlich als *Primerweiterung* über A, falls es zu jedem weiteren Modell M' von Σ, das A umfaßt, eine elementare Einbettung von M nach M' gibt, die auf A die Identität ist. Wir wissen, daß unter gewissen Voraussetzungen, die z.B. hier für $\mathbf{pDCF}_0$ gelten, solch eine Primerweiterung existiert, wir zitieren die Sätze von Morley und Shelah.

Satz 3.5.3 *Sei Σ eine vollständige und ω-stabile Theorie und A sei eine Substruktur eines Modelles M von Σ.*

a) Es existiert ein $M^* \models \Sigma$, das prim und atomar über A ist.

b) Zwei Primmodelle M^* und N^* über A sind A-isomorph.

Für einen D-Körper K können wir also festhalten: K ist immer in einem $F \models \mathbf{pDCF}_0$ enthalten, wegen der ω-Stabilität existiert nach dem letzten Satz ein Primmodell von $\mathbf{pDCF}_0$ über K, das sich elementar über K in jeden weiteren differentiell abgeschlossenen Körper einbetten läßt, der K umfaßt, und alle weiteren differentiell abgeschlossen Erweiterungskörper mit diesen Eigenschaften sind K-isomorph.

Definition 17 *Sei K ein D-Körper, dann nennen wir eine Primerweiterung von* $\mathbf{pDCF}_0$ *über K einen* **Differential-Algebraischen Abschluß** *von K.*

Auf diese Weise haben wir durch unsere modelltheoretischen Konstruktionsmethoden in der Primerweiterung eines D-Körpers ein Analogon zum Algebraischen Abschluß konstruiert.

Abschließende Bemerkung

Wir können also resümieren, daß es uns gelungen ist, für die Differentialkörper mit kommutierenden Derivationen die klassischen modelltheoretischen Ergebnisse, wie sie im Zusammenhang mit Untersuchungen von Körperklassen bekannt sind, nachzuweisen.

Nachdem wir die nötigen algebraischen Objekte eingeführt hatten, haben wir die grundlegenden Tatsachen bezüglich D-Ring- und D-Körpererweiterungen entwickelt.

Weiter folgten die wichtigen Untersuchungen über den zugehörigen D-Polynomring. Dieser hat uns ein technisch etwas aufwendigeres Instrumentarium abverlangt, womit es dann aber gelang zu erkennen, daß sich dieser fast genauso übersichtlich verhält wie der gewöhnliche. Als Beispiel sei nochmals der Basissatz für radikale D-Ideale erwähnt, der im Prinzip die wichtigsten Konsequenzen des Hilbertschen Basissatzes überträgt.

Dann stellte sich das Problem, einfache D-algebraische D-Körpererweiterungen zu charakterisieren. Wir wurden auf die kohärenten Mengen geführt, mit denen wir die differentiell abgeschlossenen D-Körper (die Modelle von $\mathbf{pDCF}_0$) beschrieben haben. Für diese konnten wir Quantorenelimination zeigen, was dann schnell zur Folge hatte, daß $\mathbf{pDCF}_0$ der Modellbegleiter der Klasse der D-Körper ist.

Ausgehend von einer 1-1-Korrespondenz von D-Primidealen und vollst. 1-Typen, gelangten wir zur ω-Stabilität von $\mathbf{pDCF}_0$, wodurch wir auf Grund allgemeiner modelltheoretischer Sachverhalte die Existenz eines natürlichen Analogons zum Algebraischen Abschluß eines Körpers erhielten.

Literaturverzeichnis

[BLUM] L. Blum, *Differentially closed fields: a model-theoretic tour*, in *Constributions to Algebra*, ed. H. Bass, P. Cassidy und J. Kovacic, Academic Press 1977

[FLUM] J. Flum, *Vorlesung über Modelltheorie*, gehalten an der Universität Freiburg im Wintersemester 1993/94

[KAPLANSKY] I. Kaplansky, *Differential Algebra*, Hermann 1957

[KOLCHIN 1] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press 1973

[KOLCHIN 2] E. R. Kolchin, *Constrained extensions of differential fields*, Advances in Mathematics 12 (1974), S. 141–170

[PRESTEL] A. Prestel, *Einführung in die mathematische Logik und Modelltheorie*, Vieweg 1986

[ROBINSON] A. Robinson, *On the concept of a differentially closed field*, Bull. Res. Council Israel Sect. F, 8

[SEIDENBERG] A. Seidenberg, *An elimination theory for differential algebra*, University of California Press Volume 3, No. 2 (1956), S. 31-66

[WOOD] C. Wood, *The model theory of differential fields revisited*, Israel Journal of Mathematics vol. 25, S. 331–352

Ich versichere, daß ich die vorliegenden Arbeit selbstständig und nur mit den angegebenen Hilfsmitteln bearbeitet habe.

Freiburg, den 26. September 1996