Zu Berechenbarkeitsfragen der Idealtheorie

Habilitationsschrift

zur Erlangung des akademischen Grades
Dr. rer. nat. habil.

der Fakultät für Mathematik und Informatik
der Universität Leipzig

eingereicht von
Dr. rer. nat. Joachim Apel, geboren am 21. März 1962 in Aken

angefertigt an der
Universität Leipzig, Institut für Informatik

Beschluß über die Verleihung des
akademischen Grades vom 18. Mai 1998

Die Annahme der Habilitationsschrift haben empfohlen:

1.	Prof. Dr. rer. nat. habil. Dr. hc. Bruno Buchberger	Universität Linz
2.	Prof. Dr. rer. nat. habil. Heinrich Herre	Universität Leipzig
3.	Prof. Dr. rer. nat. habil. Jürgen Stückrad	Universität Leipzig
4.	Prof. Dr. rer. nat. habil. Volker Weispfenning	Universität Passau

Bibliographische Beschreibung:

Apel, Joachim

Zu Berechenbarkeitsfragen der Idealtheorie
Universität Leipzig, Diss.,
194 S., 101 Lit.

Referat:

Aufbauend auf der Buchbergerschen Theorie der Gröbnerbasen und der Robbiano-Moraschen Verallgemeinerung auf graduierte Strukturen wird die Entscheidbarkeit des Idealenthaltenseinsproblems in verschiedenen Ringen untersucht. Im Mittelpunkt steht der algorithmische Aspekt inklusive eines geeigneten Berechenbarkeitsbegriffs für Funktionen über Mengen abstrakter Objekte.
Die für die kanonische Simplifikation in Restklassenringen benötigte Totalreduktion und der Begriff der reduzierten Gröbnerbasis werden auf den Kalkül der graduierten Strukturen verallgemeinert. Außerdem wird der Versuch der Ausdehnung der Gröbnerbasistheorie graduierter Strukturen auf den Modulfall unternommen. Erwartungsgemäß erweist sich die Untersuchung einseitiger Moduln als einfach, wohingegen im Bimodulfall nicht über Teillösungen hinausgekommen wird.
In gewissen Situationen kann das Fehlen der Konfluenz der Ableitungsrelation durch Grenzwertbetrachtungen ausgeglichen werden. Die klassische Möglichkeit besteht in der Ausnutzung der durch die zugrundeliegende Filtrierung induzierten Topologie. Auch wenn Filtrierung und Topologie nicht in Beziehung zueinander stehen, können interessante Teilergebnisse erzielt werden. Einen wesentlichen Raum nimmt die Berechnung von Näherungslösungen ein.
Ein weiterer Schwerpunkt der Arbeit besteht im Aufbau einer allgemeinen Theorie involutiver Basen. Ähnlich dem Robbiano-Moraschen Kalkül basiert auch diese auf graduierten Strukturen. Sie liefert einen alternativen Entscheidungsalgorithmus für das Idealenthaltenseinsproblems in effektiven Algebren von auflösbarem Typ.
Abschließend wird kurz auf die Implementierung der erarbeiteten Algorithmen im speziell für diesen Zweck entwickelten Computeralgebrasystem Felix eingegangen.

Abkürzungsverzeichnis

bzw.	beziehungsweise
i.a.	im allgemeinen
d.h.	das heißt
m.a.W.	mit anderen Worten
o.B.d.A.	ohne Beschränkung der Allgemeinheit
vgl.	vergleiche
z.B.	zum Beispiel
$\square$	Ende eines Beweises
$\perp$	Undefiniertheit einer partiellen Funktion an einer Stelle

Inhaltsverzeichnis

Kapitel 1

Einleitung

Im Jahre 1965 schuf Buchberger in seiner Dissertation die Grundlagen für die Theorie der Gröbnerbasen[1] von Polynomidealen. Die von Buchberger im Titel seiner Arbeit [Bu65] zum Ausdruck gebrachte Beschränkung auf nulldimensionale Polynomideale ist dem ursprünglichen Anliegen des Aufbaus einer Multiplikationstafel des Restklassenringes und der dafür notwendigen endlichen Vektorraumbasis geschuldet. Grundsätzlich wurde der höherdimensionale Fall bereits in Buchbergers 65-iger Kalkül behandelt. Unabhängig davon entwickelte Hironaka in etwa zur gleichen Zeit in seiner Arbeit [Hi64] den Kalkül der Standardbasen von Idealen formaler Potenzreihenringe. Spätestens mit Robbianos Arbeit [Rob85] zur Theorie der graduierten Strukturen wurde die enge Verwandschaft zwischen Gröbner- und Standardbasen deutlich.

Während Filtrierungen und Graduierungen von Polynomringen bereits in der ersten Hälfte des 20. Jahrhunderts von verschiedenen Autoren, unter ihnen Macaulay und Gröbner, zur Lösung theoretischer Fragestellungen ausgenutzt wurden, besteht Buchbergers Verdienst in der erstmaligen konsequent konstruktiven Behandlung der Problematik, insbesondere in der Schaffung effektiver Algorithmen zum Rechnen in Restklassenringen modulo Polynomidealen. Damit wurde eine wichtige Brücke zwischen Mathematik und Informatik geschlagen. Neben dem offensichtlichen Zusammenhang zwischen der konstruktiven Algebra und dem der theoretischen Informatik zuzurechnenden Gebiet der Berechenbarkeitstheorie, erstreckt sich die Beziehung auch auf Bereiche der praktischen Informatik. So ist Buchbergers Algorithmus das Herzstück nahezu jeden Verfahrens der kommutativen Algebra und die Effizienz seiner Implementierung ist ein herausragendes Qualitätsmerkmal eines jeden Computeralgebrasystems.

Seit Ende der 70-iger Jahre ist eine anhaltend rasante Entwicklung der Theorie der Gröbnerbasen zu verzeichnen. Aus heutiger Sicht ist es nahezu unmöglich, alle Gebiete der Mathematik, Natur- und Ingenieurwissenschaften sowie Wirtschaft aufzuzählen, in denen Buchbergers Algorithmus zur Anwendung kommt. Stellvertretend seien das Lösen algebraischer Gleichungssysteme, das Führen geometrischer Beweise, das Berechnen von Eliminationsidealen, Syzygienmoduln und Hilbertfunktionen, die Berechnung von Idealdurch-

[1] Der Begriff der Gröbnerbasis wurde erst später geprägt. Bruno Buchberger selbst führte den Begriff zu Ehren seines Lehrers Wolfgang Gröbner ein.

schnitten und -quotienten, das Lösen multivariater Interpolationsprobleme und das Lösen linearer Optimierungsprobleme genannt. Diese innermathematischen Anwendungen werden ihrerseits beispielsweise in Kryptographie, Spieltheorie, Wirtschaftsmathematik, Chemie und Physik sowie zur Steuerung von Robotern eingesetzt. Mittlerweile gibt es eine ganze Reihe von Lehrbüchern, welche die Gröbnerbasisproblematik aus unterschiedlicher Sicht abhandeln. So widmen Cox, Little und O'Shea in [CLO92] ihr Augenmerk den Anwendungen in Geometrie und Robotik. Becker, Weispfenning und Kredel präsentieren in [BW93] eine streng algebraische, mit zahlreichen Anwendungen der kommutativen Algebra angereicherte Darstellung der Theorie. Außerdem stellt [BW93] enge Bezüge zur theoretischen Informatik, insbesondere der Berechenbarkeitstheorie und Logik, her. Adams und Loustaunau wählten in ihrem Buch [AdL94] ebenfalls einen streng algebraischen Zugang zur Gröbnertheorie. Akzentuierung und Anwendungsauswahl unterscheiden sich jedoch wesentlich von der in [BW93] vorgenommenen. Eine Reihe weiterer Bücher, wie zum Beispiel [BCL83] oder [Bo85], enthalten Kapitel zur Theorie der Gröbnerbasen. Insgesamt ist bisher in allen Lehrbüchern eine starke Konzentration auf den Polynomfall feststellbar. Auf nichtkommutative Verallgemeinerungen wird nur im Anhang des Buches von Becker, Weispfenning und Kredel eingegangen.

Im Zentrum der vorliegenden Arbeit steht die Frage nach der Verallgemeinerbarkeit der Theorie der Gröbnerbasen. Dabei wird auf der einen Seite versucht, die Theorie so allgemein wie möglich darzustellen. In diesem Kontext können oft nur noch Existenzaussagen getroffen werden. Auf der anderen Seite werden wir stets bemüht sein, möglichst allgemeine hinreichende Bedingung für die Berechenbarkeit der Basen herauszukristallisieren. In den meisten Fällen werden die Berechenbarkeitsnachweise durch explizite Angabe von Algorithmen geschehen. Im Vordergrund steht die Verständlichkeit der Algorithmen, Effizienzfragen spielen dagegen oft nur eine untergeordnete Rolle. So wird insbesondere nicht auf die Komplexität der behandelten Algorithmen eingegangen. Mayr und Meyer zeigten, daß die Lösung des Idealenthaltenseinsproblem in Polynomringen exponentiell-hart ist (siehe [MaMe82]). Einen Überblick zu bisherigen Komplexitätsuntersuchungen in Polynomringen findet man in [BW93].

Die Theorie der Gröbnerbasen ist eng mit dem Problem der algebraischen Simplifikation und der Frage nach der Entscheidbarkeit des Idealenthaltenseinsproblems verbunden. Im weitesten Sinne zeichnet sich eine Gröbnerbasis F eines ein- oder zweiseitigen Ideals I eines Ringes R dadurch aus, daß sie eine binäre asymmetrische Reduktionsrelation $\rightarrow \subseteq \equiv_I$ bestimmt, welche in der Kongruenz modulo des Ideals enthalten ist und deren transitiver Abschluß $\rightarrow^+$ die Eigenschaft $a \rightarrow^+ 0 \iff a \in I \setminus \{0\}$ aufweist. Präzisiert man den Zusammenhang zwischen F und $\rightarrow$ entsprechend der im klassischen Polynomfall vorliegenden Situation oder rückt man die Reduktionsrelation zu Gunsten algebraischer Zusammenhänge in den Hintergrund, so hat keine der auf diese Weise gewonnen Charakterisierungen in allen in der Literatur betrachteten Verallgemeinerungen Bestand. Die bisherigen Untersuchungen zur Verallgemeinerbarkeit der Gröbnerbasistheorie lassen sich in zwei Hauptrichtungen einteilen.

Das Prinzip der ersten Richtung besteht in der Konstruktion einer konfluenten noetherschen Reduktionsrelation $\rightarrow$. Dabei werden in entscheidendem

Maße Voraussetzungen über Teilrelationen der Idealkongruenz eingesetzt. Typische Beispiele für diese Vorgehensweise sind Reduktionsringe (siehe [Bu83], [Sti87]) und Gruppenringe (siehe [MR93],[Ros93],[Rei95],[MR96]). Natürlich fällt auch Buchbergers Originalansatz in diese Rubrik. Dagegen paßt Hironakas Theorie nicht auf dieses Muster, denn die dort benötigte Reduktionsrelation $\rightarrow$ ist nicht noethersch. Außerdem stellt der in Frage stehende Ansatz das Bindeglied zu Entscheidbarkeitsproblemen modulo Kongruenzrelationen in universellen Algebren, insbesondere zum Knuth-Bendix-Algorithmus (siehe [KB67]) und somit zum automatischen Theorembeweisen dar (siehe [Wi84]).

Die zweite Verallgemeinerungsrichtung ist stärker algebraisch ausgerichtet und verwendet eine Filtrierung $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ des Ringes R bezüglich eines geordneten Monoids $(\Gamma, \prec)$. Der Zusammenhang zwischen $\mathfrak{F}$ und $\rightarrow$ wird durch die Forderung

$$\forall a, b \in R, \gamma \in \Gamma \ : \ \left(a \rightarrow b \wedge a \in \mathcal{F}_\gamma \Rightarrow \exists \gamma' \prec \gamma \ : \ b \in \mathcal{F}_{\gamma'}\right) \tag{1.1}$$

hergestellt. Dabei werden zunächst weder Noetherschsein noch Konfluenz der Relation $\rightarrow$ verlangt. Die klassischen Ansätze Buchbergers und Hironakas passen sich ebenso in das beschriebene Konzept ein, wie Behandlung von Polynomringen über noetherschen kommutativen Ringen in denen lineare Gleichungen lösbar sind (siehe [Tri78], [Za78],[Sch79], [KK84],[Pa85], [KK88], [Mö88]), von Lokalisierungen von Polynomringen (siehe [Mo82], [AMR92]), von freien $\mathbb{K}$-Algebren (siehe [Ber78], [Mo86]), von Einhüllenden von Liealgebren (siehe [ApL85]), von Algebren von auflösbarem Typ (siehe [KW90]), von auflösbaren Polynomringen (siehe [Kr92]) und von G-Algebren (siehe [Ap88]). Mit dem Ziel der Vereinheitlichung der Theorie entwickelten Robbiano (siehe [Rob86]) und Mora (siehe [Mo88a]) den Kalkül der graduierten Strukturen. Eine große Zahl von Problemen wird damit bereits auf sehr hohem Abstraktionsniveau lösbar. Wenn es gelingt, zu einem vorgegebenem Ring eine geeignete Filtrierung zu konstruieren, so reduzieren sich die Gröbneruntersuchungen auf den Nachweis einiger Berechenbarkeitsanforderungen. Wenngleich das Konzept der graduierten Strukturen den wahrscheinlich umfassendsten Verallgemeinerungsansatz im Rahmen der Ringtheorie darstellt, so ist es dennoch auf die meisten in der Literatur mit Termersetzungsmethoden behandelten Reduktions- oder Gruppenringe leider nicht anwendbar.

In einigen topologischen Ringen kann das Nichtnoetherschsein der Ableitungsrelation $\rightarrow$ durch Grenzwertbildungen ausgeglichen werden. Das klassische Beispiel dafür sind die formalen Potenzreihenringe mit der Krullschen Topologie (vgl. z.B. [Hi64], [Mo82], [Bec90] und[AMR92]). Apel, Stückrad, Tworzewski und Winiarski stellten in [ASTW] einen entsprechenden Kalkül für den Fall des Ringes der ganzen Funktionen mit der Topologie der lokalen gleichmäßigen Konvergenz vor. Dabei steht man vor dem Problem, daß Graduierung und Topologie nicht verträglich gestaltet werden können. Als Ausweg erwies sich die Beschränkung der Graduierung auf den Unterring der Polynome, wodurch wenigstens die Division beliebiger ganzer Funktionen modulo von Polynomen erzeugter Ideale möglich wurde.

Vor wenigen Jahren deckten Zharkov und Blinkov eine enge Beziehung zwi-

schen der Theorie der Gröbnerbasen und den Methoden der Berechnung involutiver Systeme partieller Differentialgleichungen auf (siehe [ZB93]). Im Gegensatz zu den Untersuchungen von Polynomidealen waren die ebenfalls in der ersten Hälfte des 20. Jahrhunderts geschaffenen Methoden zur Lösung von Systemen partieller Differentialgleichungen bereits konstruktiv (siehe [Ja29], [Th37]). Auf diese Weise liefert die Übertragung der involutiven Methode einen alternativen Algorithmus zur Berechnung von Gröbnerbasen. Wenngleich die Arbeit von Zharkov und Blinkov zum Teil erhebliche theoretische Lücken aufweist, so ist es auf jeden Fall der Verdienst von Zharkov und Blinkov, die Aufmerksamkeit durch eine Reihe vielversprechender Beispielrechnungen auf den neuen alternativen Ansatz gelenkt zu haben. Die Pommaretmethode (siehe [Po78]) nimmt eine Ausnahmestellung unter den verschiedenen involutiven Ansätzen ein, denn sie stellt in gewisser Weise ein perfektes Bindeglied zwischen den beiden oben beschriebenen Verallgemeinerungsrichtungen dar.

Einerseits verlagert sie die Grundlagen der Reduktionsrelation $\rightarrow$ in die freie nichtkommutative Halbgruppe zurück und nähert sich somit dem Prinzip der Termersetzungssysteme an. Die Behandlung von Gruppenringen verlangt die Abtrennung der durch die definierenden Relationen der Gruppe definierten Ableitungsregeln von der Relation $\rightarrow$. Madlener und Reinert nennen diese Vorgehensweise Präfixreduktions-/Sättigungs-Verfahren, wobei die Behandlung der definierenden Relationen der Gruppe den Sättigungsschritt bildet (siehe [MR93],[MR96]). Bei der Pommaretmethode geht man analog vor, indem die definierenden Relationen der freien kommutativen Halbgruppe abgespalten werden.

Andererseits ordnet sich die Pommaretmethode bei geeigneter Wahl des Bewertungsmonoids perfekt in die Theorie der graduierten Strukturen ein (siehe [Ap95b]). Die in [Ap95b] vorgenommene Einordnung der Pommaretmethode beseitigte die theoretischen Mängel aus [ZB93] und erlaubt es außerdem, eine unmittelbare Verallgemeinerung auf Algebren von auflösbarem Typ vorzunehmen. Formuliert man die aus der Theorie der graduierten Strukturen entlehnte Vorgehensweise in der Sprache des Präfixreduktions-/Sättigungs-Verfahrens, so stellt man fest, daß der Sättigungsschritt abgeschnitten wird. Dadurch wird eine wesentliche Verbesserung des Terminationsverhaltens erzielt. Diese Feststellung ist auch Motivation dafür, ähnliche Sättigungseinschränkungen bei Gruppenalgebren zu untersuchen.

Aufgrund der Tatsache, daß sich die Pommaretmethode besonders vorteilhaft in die bisherigen Gröbnerbasiskonzepte einordnen läßt, war es auch besonders einfach, diese jüngste der involutiven Methoden auf den Polynomfall zu übertragen. Ein erheblicher Mangel der Pommaretmethode im Vergleich zur Janet- oder Thomasmethode besteht in der allgemeinen Nichtexistenz endlicher involutiver Basen. Aus diesem Grund versuchten Zharkov in [Zh94] sowie Gerdt und Blinkov in [GB96] eine Verallgemeinerung der anderen beiden Konzepte vorzunehmen. Dabei kristallisierten sie interessante Ansätze heraus, ohne dabei jedoch zu exakten Theorien zu gelangen. Ein alternativer Ansatz, die allgemeine Nichtexistenz endlicher Pommaretbasen zu umgehen, geht auf Apel zurück. Ist nur eine schnelle Berechnung von Gröbnerbasen von Interesse, so reicht es aus, die involutive Methode nach Erreichen einer Gröbnerbasis

abzubrechen. Eine effizient überprüfbare Abbruchbedingung für ein solches Verfahren wurde in [Ap98] entwickelt.

Bei genauerer Betrachtung stellt man fest, daß die involutive Methode mehr beinhaltet, als nur eine schnelle Variante zur Gröbnerbasisberechnung. Der Vorzug einer Gröbnerbasis von I gegenüber einem beliebigen Erzeugendensystem von I besteht in der Möglichkeit des direkten Ablesens eines Erzeugendensystems des Initialideals $\mathrm{In}(I)$. Das Initialideal trägt bereits wesentliche Informationen, wie zum Beispiel die Dimension oder die Hilbertfunktion, über das Ideal I in sich. Die Definition der involutiven Basen orientiert sich ebenfalls am Initialideal und auch sie erlauben keinen besseren Zugriff auf über das Initialideal hinausgehende Informationen von I. Sowohl involutive als auch Gröbnerbasen von Polynomidealen haben die Eigenschaft, daß die Initialterme der Elemente von F eine ebensolche Basis des Initialideals $\mathrm{In}(I)$ bilden. Während jedes monomiale Erzeugendensystem von $\mathrm{In}(I)$ Gröbnerbasis ist, zeichnet der Begriff der involutiven Basis selbst im Monomidealfall gewisse Erzeugendensysteme aus. Um die Hilbertfunktion eines Monomideals aus einem beliebigen Erzeugendensystem zu berechnen, bedarf es einer Rekursion. Dagegen kann bei Vorgabe einer involutiven Basis eines Monomideals sofort eine explizite Formel für die Hilbertfunktion angeben werden (siehe [Ap96]). Dieser Zusammenhang stellt eine aus theoretischer Sicht noch stärkere Motivation für die Untersuchung involutiver Basen dar, als es der empirisch ermittelte Geschwindigkeitsvorteil gegenüber dem Buchbergeralgorithmus war. Außerdem erweist sich die Nichtexistenz endlicher Pommaretbasen an dieser Stelle als ein ernsthafter Makel, welcher sich auch nicht mit Hilfe des in [Ap98] vorgestellten Algorithmus umgehen läßt. Die Lösung des Problems erfordert die Verallgemeinerung der Theorien von Janet oder Thomas. Dabei sollte der bei den Pommaretbasen empirisch ermittelte Geschwindigkeitsvorteil gegenüber dem Buchbergeralgorithmus auf jeden Fall erhalten bleiben. Andernfalls könnte man auch auf das von Schwarz angewandte Verfahren zurückgreifen und die involutive Vervollständigung der Gröbnerbasisberechnung nachstellen (siehe [Swa92]). Der in [Ap96] entwickelte Kalkül umfaßt unter anderem die Möglichkeit, involutive Basen mit einem Aufwand zu konstruieren, der höchstens so groß ist wie im Pommaretfall.

Die vorliegende Arbeit ist wie folgt aufgebaut:

2. Effektive algebraische Strukturen Es werden grundlegende Begriffe der theoretischen Informatik, die insbesondere Berechenbarkeitstheorie, universeller Algebra und elementarer Logik zuzuordnen sind, bereitgestellt und der Versuch unternommen, die Frage, unter welchen Bedingungen eine algebraische Struktur als effektiv angesehen werden kann, zu beantworten.

In der Algebra ist es oftmals üblich, zueinander isomorphe algebraische Strukturen miteinander zu identifizieren. Dieses Vorgehen ist praktisch unvermeidlich, da die Beschreibung einer Struktur durch Angabe einer logischen Theorie, wenn auch der Theoriebezug häufig nur indirekt vorhanden ist, erfolgt und auf diesem Niveau zunächst gar keine Unterscheidung der Modelle möglich ist. Aufgrund der möglichen Existenz nichtberechenbarer Isomorphismen ist eine solche Einteilung in Isomorphieklassen im allgemeinen zu grob, um

darauf einen sinnvollen Effektivitätsbegriff aufzubauen. Die Problematik wird an folgendem einfachen Beispiel deutlich. Sei $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ eine endliche Körpererweiterung der rationalen Zahlen. Anwendung elementarer Sätze der Körpertheorie beweist die Isomorphie von $\mathbb{K}$ zu einem Körper der Bauart $\mathbb{Q}(T_1, \ldots, T_m)(y) \simeq \mathbb{Q}(T_1, \ldots, T_m)[Y]/p(Y)$, wobei $m \geq 0$ gilt, T_1 transzendent über den rationalen Zahlen und T_{i+1} für alle $i = 1, \ldots, m-1$ transzendent über $\mathbb{Q}(T_1, \ldots, T_i)$ ist. Darüberhinaus ist y algebraisch über $\mathbb{Q}(T_1, \ldots, T_m)$ mit dem charakteristischem Polynom $p(Y) \in \mathbb{Q}(T_1, \ldots, T_m)[Y]$. Wenngleich der Körper $\mathbb{Q}(T_1, \ldots, T_m)[Y]/p(Y)$ intuitiv als effektive Struktur angesehen werden darf, ist gleiches im allgemeinen für $\mathbb{K}$ nicht sinnvoll.

Kapitel 2 behandelt die Frage, wann eine logische Theorie ein effektives Modell besitzt. Außerdem wird ein Kategorizitätsbegriff für Theorien zur Beschreibung effektiver algebraischer Strukturen entwickelt. Die Antwort auf die Frage nach der Effektivität des Körpers $\mathbb{K}$ stellt sich dann wir folgt dar. Im allgemeinen ist $\mathbb{K}$ kein effektiver Körper. Daran ändert auch die intuitive Effektivität von $\mathbb{Q}(T_1, \ldots, T_m)[Y]/p(Y)$ nichts, denn diese erfordert zunächst den Übergang zu einer geeigneten Konstantenexpansion.

3. Algorithmische Probleme der Ringtheorie Es erfolgt die Bereitstellung der in der Arbeit benötigten Grundlagen der Ring- und Idealtheorie. Neben den begrifflichen Festlegungen stehen vor allem die Fragen der Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter ein- oder zweiseitiger Moduln über nichtkommutativen Ringen sowie die Berechenbarkeit endlicher Erzeugendensysteme ihrer Syzygienmoduln im Vordergrund.

4. Graduierte Strukturen Die in dieser Arbeit vorgenommenen Untersuchungen zur Theorie der Gröbner- und Standardbasen ordnen sich in die zweite der oben beschriebenen Hauptrichtungen von Verallgemeinerungen ein. Kapitel 4 beschäftigt sich mit Grundaussagen zu Modul- und Ringfiltrierungen, graduierten Ringen und Moduln sowie homogenen Idealen und Untermoduln.

5. Gröbnerbasen in graduierten Strukturen In diesem Kapitel bauen wir zunächst den Gröbnerbasisbegriff graduierter Strukturen auf. Den Ideen von Robbiano und Mora folgend, zeigen wir grob gesprochen, wie sich die Entscheidbarkeit des Idealenthaltenseinsproblems und die Lösbarkeit des Syzygienproblems ein- beziehungsweise zweiseitiger Ideale eines noetherschen Ringes im wesentlichen auf die Entscheidbarkeit des Enthaltenseinsproblems und die Lösbarkeit des Syzygienproblems endlich erzeugter homogener Ideale seines assoziierten graduierten Ringes reduzieren lassen. Im Anschluß daran wenden wir uns einer Reihe natürlicher Fragestellungen zu, die bisher noch nicht im allgemeinen Kontext graduierter Strukturen untersucht wurden. Dabei beschränken wir uns in diesem Kapitel auf die Betrachtung von Filtrierungen $\mathfrak{F}$ bezüglich wohlgeordneter Monoide $(\Gamma, \prec)$. Somit ist auf jeden Fall gesichert, daß die Ableitungsrelation $\rightarrow$ noethersch ist.

Die in Buchbergers Originalabhandlung entwickelte Reduktionsrelation bezüglich einer Gröbnerbasis ist konfluent. Allerdings erfüllt sie nicht Bedingung

(1.1) und ordnet sich daher nicht unmittelbar in die Theorie der graduierten Strukturen ein. Dagegen ist die in das Konzept der graduierten Strukturen passende Kopfreduktion, bei welcher nur am höchsten Term eines Polynoms reduziert wird, leider nicht mehr konfluent. Die Buchbergersche Totalreduktion liefert einen kanonischen Simplifikator und besitzt damit einen ästhetischen Vorteil gegenüber der nur auf einen Nullsimplifikator führenden Kopfreduktion. Aufgrund der wohlbekannten Tatsache, daß sich aus einem Nullsimplifikator stets auch ein kanonischer Simplifikator konstruieren läßt, drängt sich die Frage nach einem (effizienten) Algorithmus zur konfluenten Verfeinerung der Ableitungsrelation $\rightarrow$ auf.

Verfolgt man das Ziel der kanonischen Darstellung der auftretenden mathematischen Objekte weiter, so stößt man auf die Problematik der reduzierten Gröbnerbasen von Polynomidealen. So schließt sich in natürlicher Weise die Frage nach der Existenz und Eindeutigkeit von verallgemeinerten reduzierten Gröbnerbasen an.

Die wesentliche Grundlage des Prinzips der Totalreduktion besteht in der Tatsache, daß sich die Polynomringe, ebenso wie alle anderen in Spezialuntersuchungen betrachteten Ringe und Algebren, in eine direkte Summe zyklischer Moduln zerlegen lassen. Der Ring und sein assoziierter graduierter Ring sind zueinander isomorphe Moduln. Die Zerlegung eines Ringelements in seine Bestandteile bezüglich der direkten Summe ermöglicht es, nach Abschluß der Kopfreduktion den höchsten Summanden abzutrennen und die Reduktion an den kleineren Bestandteilen fortzusetzen. Die so beschriebene Totalreduktion führt stets auf einen Reduktionsrest, welcher nur noch irreduzible Bestandteile aufweist. Die angestrebte Eindeutigkeit dieses Rests erfordert zusätzlich, daß wir es mit Moduln über einem Körper als Operatorenbereich, das heißt mit Vektorräumen, zu tun haben. Die gleichen Eigenschaften der Polynomringe stellen auch die Grundlage für die Existenz und Eindeutigkeit reduzierter Gröbnerbasen dar. Weder die Modulisomorphie von Ring und assoziiertem graduiertem Ring noch deren Zerlegbarkeit in eine direkte Summe eindimensionaler Vektorräume folgen aus der Theorie graduierter Strukturen. Dennoch werden wir zeigen, daß sich sowohl das Prinzip der konfluenten Verfeinerung von $\rightarrow$ zu einer Totalreduktion als auch der Begriff der reduzierten Gröbnerbasis in sinnvoller Weise auf entsprechende Eigenschaften des assoziierten graduierten Rings zurückführen lassen.

Die große Allgemeinheit der Theorie der graduierten Strukturen stellt sowohl einen Vor- als auch einen Nachteil dar. Der Nachteil besteht darin, daß die Theorie eine Vielzahl nicht effektiver Modelle aufweist. Gemäß dem Grundanliegen dieser Arbeit werden wir versuchen, möglichst große Teilklassen effektiver Modelle herauszukristallisieren. Im Ergebnis dessen gelangen wir zu hinreichenden Bedingungen für die Berechenbarkeit von Gröbnerbasen ein- beziehungsweise zweiseitiger Ideale. Alle im Zusammenhang mit der zweiten Verallgemeinerungsrichtung aufgezählten Spezialfälle fallen in die beschriebenen Klassen effektiver Strukturen. Darüberhinaus ergibt sich unter anderem die Möglichkeit der Kombination verschiedener Konzepte. So fügen sich beispielsweise auch Ringe von auflösbarem Typ über (nicht notwendigerweise kommutativen) noetherschen Ringen in denen lineare Gleichungen lösbar sind in das

Konzept ein. Den meisten in der Literatur untersuchten Verallgemeinerungen ist die Nullteilerfreiheit der betrachteten Ringe eigen. Ähnlich zu den in [Ap92] vorgenommenen Untersuchungen wird hier bewußt auf diese Forderung verzichtet. Auf diese Weise wird ein (teilweiser) Abschluß der Klasse effektiver Strukturen gegen die Bildung von Faktorringen erzielt. Damit wird es möglich, die Behandlung endlich erzeugter Linksmoduln über derartigen Ringen auf die Behandlung einseitiger Ideale eines (anderen) Rings des gleichen Typs zurückzuführen. Grundlage dafür ist das Nagatasche Idealisierungsprinzip.

Neben der Untersuchung von Gröbnerbasen von Idealen erhebt sich die Frage nach der Verallgemeinerbarkeit auf endlich erzeugte R-Moduln. Damit können dann unter anderem auch höhere Syzygienmoduln berechnet werden. Im Polynomfall nahmen Möller und Mora eine derartige Verallgemeinerung vor (siehe [MöMo86]). Aus der graduierten Struktur eines Ringes R läßt sich leicht eine graduierte Struktur eines endlich erzeugten freien R-Linksmoduls konstruieren. Der Aufbau einer Gröbnerbasistheorie bezüglich dieser graduierten Struktur verläuft völlig geradlinig. In der Einfachheit ist der Hauptgrund dafür zu suchen, daß die in der Literatur vorgenommenen Verallgemeinerungen der Gröbnertheorie nicht oder nur am Rande auf den Linksmodulfall eingehen. Ganz anders verhält es sich mit dem Bimodulfall, welcher tatsächlich mit einer ganzen Reihe neuer Probleme einhergeht und bisher nicht in der Literatur auftauchte.

Der Einfachheit Rechnung tragend, gehen wir kurz auf den Fall der Behandlung von Gröbnerbasen einseitiger Moduln ein. Dabei werden wir die oben beschriebene natürliche Modulgraduierung jedoch weiter verfeinern, wodurch sich die Gröbnerbasisberechnung einfacher gestaltet. Dabei gelangen wir schließlich zu der Feststellung, daß die im Links- beziehungsweise Rechtsidealfall erforderlichen Berechenbarkeitsbedingungen bereits zur Behandlung endlich erzeugter R-Links- oder R-Rechtsmoduln ausreichen. Anschließend untersuchen wir den R-Bimodulfall und kristallisieren die wichtigsten Problemstellen heraus. Trotzt wesentlicher Verschärfung der Berechenbarkeitsbedingungen gegenüber dem Idealfall werden wir im allgemeinen nur zu Semientscheidbarkeitsaussagen gelangen.

6. Topologische Methoden Will man die Methode von Hironaka beschreiben, so muß man Filtrierungen $\mathfrak{F}$ bezüglich eines geordneten Monoids $(\Gamma, \prec)$ betrachten, bei welchem $\prec$ keine Wohlordnung ist. In solch einer Situation ist es üblich, den Hironakaschen Begriff der Standardbasis anstelle des Begriffs der Gröbnerbasis zu verwenden. Die der Bedingung (1.1) genügenden Reduktionsrelationen $\rightarrow$ sind nun nicht mehr notwendigerweise noethersch. Ist $\prec$ wenigstens beschränkt wohlgeordnet, das soll bedeuten, daß jede nach unten beschränkte Teilmenge von Γ bezüglich der Einschränkung von $\prec$ wohlgeordnet ist, dann definiert die Filtrierung $\mathfrak{F}$ auf dem Ring R eine Hausdorff-Topologie $\mathfrak{T}$. Ist R beispielsweise ein Unterring des Ringes der formalen Potenzreihen über der Variablenmenge X, Γ das Monoid der Potenzprodukte in X und $\prec$ eine gradverträgliche Ordnung, bei der stets das gradgrößere Potenzprodukt kleiner bezüglich $\prec$ ist, so stimmt $\mathfrak{T}$ mit der Krullschen Topologie überein. Jede un-

endliche Ableitungssequenz $a_1 \to a_2 \to \cdots$ ist eine Chauchy-Folge in $\mathfrak{T}$ und es ist sinnvoll, den Grenzwert $\lim_{i\to\infty} a_i$ in der Komplettierung von R als Ergebnis des Reduktionsprozesses anzusehen. Unser Augenmerk liegt auf der Berechenbarkeit der resultierenden Divisionsverfahren. Aufgrund der Überabzählbarkeit formaler Potenzreihenringe kann in den interessantesten Anwendungen leider keine Berechenbarkeit vorliegen. Grob gesprochen wird sich zeigen, daß, sofern R einen effektiven Unterring besitzt, dessen assoziierter graduierter Ring isomorph zu dem von R ist, für alle Bestandteile der Divisionsformel Näherungen beliebig vorgegebener Genauigkeit $\gamma \in \Gamma$ algorithmisch berechnet werden können.

Bei den vorangegangenen Betrachtungen ergab sich die Topologie aus der Filtrierung des untersuchten Ringes R. Die anschließenden Berechnungen erfordern im allgemeinen den Übergang zur Komplettierung von R bezüglich der Topologie $\mathfrak{T}$. Wenigstens bei der Untersuchung lokaler Ringe ist eine derartige Vorgehensweise durchaus hilfreich.

Auf Probleme stößt man, wenn man einen topologischen Ring R mit der Topologie $\mathfrak{T}'$ untersuchen will und eine Filtrierung $\mathfrak{F}$ einführt, die eine mit $\mathfrak{T}'$ unverträgliche Topologie $\mathfrak{T}$ induziert. So wird der Ring E der ganzen Funktionen (über dem Körper der komplexen Zahlen) für die Untersuchung geometrischer Fragestellungen mit der Topologie der lokalen gleichmäßigen Konvergenz versehen. Gleichzeitig ist E Unterring eines formalen Potenzreihenringes S und es kann die auf E durch die Krullsche Topologie von S induzierte Topologie betrachtet werden. Beide Topologien sind unvergleichbar. Führt man auf E eine Filtrierung $\mathfrak{F}$ bezüglich des geordneten Monoids $(T, \prec)$ der Potenzprodukte ein, wobei $\prec$ nur beschränkte aber keine echte Wohlordnung ist, dann konvergieren die daraus resultierenden Ableitungssequenzen $a_1 \to a_2 \to \cdots$ im allgemeinen nicht in der Topologie der lokalen gleichmäßigen Konvergenz. Andererseits ist E Oberring eines Polynomringes R. Faßt man die Polynome als Funktionen auf und führt auf R die Topologie der lokalen gleichmäßigen Konvergenz ein, so ist E gerade die Komplettierung von R. Für Wohlordnungen $\prec$ des Monoids T ist die Menge der in einer ganzen Funktion $f \in E$ mit von Null verschiedenem Koeffizienten auftretenden Potenzprodukte im allgemeinen nach oben unbeschränkt. Daher lassen sich Filtrierungen von R bezüglich $(T, \prec)$ nicht auf E erweitern. Aufbauend auf einer Filtrierung des Polynomrings R gelingt es jedoch, einen Divisionsalgorithmus ganzer Funktionen $f \in E$ modulo eines von einer Menge $F \subset R$ von Polynomen erzeugten Ideals $I \subseteq E$ zu entwickeln. Grob gesprochen wird dazu jedes in f auftretende Monom im Polynomring R modulo $(F) \cdot R$ dividiert und die dabei enstehenden Divisionsformeln aufsummiert. Das Hauptproblem besteht im Nachweis der Wohldefiniertheit der Summation. Zum Abschluß des Kapitels fragen wir nach der Berechenbarkeit der Division. Allein die Tatsache, daß wir über dem Körper der komplexen Zahlen rechnen, erlaubt von vorherein höchstens die Bestimmung von Näherungslösungen. Im Unterschied zu den im Zusammenhang mit der Krullschen Topologie erzielten Resultaten, wird sich zeigen, daß die Elemente von F exakt gegeben sein müssen. Wenigstens in den Koeffizienten der ganzen Funktion f werden sich aber auch die Bestandteile der in diesem Kapitel entwickelten Divisionsformel als stetig erweisen. Insbesondere wird eine Abschätzung getroffen, an welchem

Potenzprodukt f zum Zwecke der Division abgeschnitten werden darf. Dem Funktionscharakter des Rests $\mathrm{rem}_{IE}(a)$ von f bei Division modulo $I = (F) \cdot E$ Rechnung tragend, gelingt es auch, Algorithmen zu entwickeln, die bei vorgegebener positiver Genauigkeit $\epsilon \in \mathbb{R}$ den Funktionswert von $\mathrm{rem}_{IE}(a)$ an einer gegebenen Stelle $(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ approximieren.

7. Involutive Basen Während es für Gröbnerbasen F eines Polynomideals I charakteristisch ist, daß die führenden Potenzprodukte der Elemente von F bereits das von den führenden Potenzprodukten aller Idealelemente gebildete Monoidideal $\mathrm{lpp}(I)$ erzeugen, besteht die grundlegende Eigenschaft involutiver Basen darin, daß zusätzlich eine Zerlegung von $\mathrm{lpp}(I)$ in paarweise disjunkte Kegel erfolgt. Ganz analog verhält es sich bei Linksidealen von Algebren auflösbaren Typs.

Die Definition der entsprechenden Kegel beruht auf einer Einschränkung der Division des Monoids T aller Potenzprodukte. Durch die Einschränkung entsteht eine Teilrelation $\mathcal{D}$, welche wir partielle Division nennen werden. $\mathcal{D}$ ordnet jedem Potenzprodukt einen direkten Faktor des Monoids T zu und es gilt genau dann $u \mid_{\mathcal{D}} v$, wenn $u \mid v$ erfüllt ist und der Quotient $\frac{v}{u}$ dem zu u gehörigen direkten Faktor angehört. Für eine beliebige Menge V von Potenzprodukten lassen sich zulässige partielle Divisionen $\mathcal{D}$ auszeichnen, diese haben unter anderem die Eigenschaft, daß die Kegel der $\mathcal{D}$-Vielfachen zweier beliebiger Elemente von V entweder disjunkt oder ineinander enthalten sind. Diese Eigenschaft allein reicht jedoch noch nicht aus, um die algorithmische Konstruierbarkeit involutiver Basen zu sichern. In dieser Arbeit wird die Konstruierbarkeit durch Einführung einer linearen Ordnung $\sqsubset$ auf V und die Forderung, daß ein bezüglich $\sqsubset$ größeres Element $u \in V$ höchstens dann $\mathcal{D}$-Teiler eines gewöhnlichen Vielfachen eines kleineren Elements $v \in V$ sein darf, wenn u selbst Vielfaches von v ist. Ob und auf welche Weise diese Anforderung abgeschwächt werden kann, ist bisher nicht bekannt.

Die Menge aller partiellen Divisionen wird durch Definition einer geeigneten Halbordnung zu einem Verband. Stehen zwei partielle Divisionen in der Verbandshalbordnung zueinander, so wird die größere als Verfeinerung der kleineren bezeichnet. Die Teilmenge aller auf einer festen Menge V zulässigen partiellen Divisionen beschreibt einen unteren Halbverband. Mit Hilfe einfacher Potenzproduktidealoperationen kann die Menge aller auf einer gegebenen endlichen Menge $V \subset T$ zulässigen partiellen Divisionen berechnet werden. Mit ähnlichen Mitteln lassen sich auch submaximale und maximale Verfeinerungen partieller Divisionen konstruieren. Es wird eine Einordnung der klassischen Konzepte von Janet, Thomas und Pommaret in den entwickelten Kalkül vorgenommen.

Mit Hilfe zulässiger partieller Divisionen wird der Begriff einer involutiven Basis eines Linksideals einer Algebra von auflösbarem Typ definiert und eine Reihe dazu äquivalenter Bedingungen hergeleitet. Diese Äquivalenzen erlauben es dann, Algorithmen zum Überprüfen der involutiven Basiseigenschaft und zum Vervollständigen eines beliebigen Erzeugendensystems zu einer involutiven Basis zu entwickeln. Abschließend wird die Frage nach möglichen

Verbesserungen der Algorithmen diskutiert und ein Vergleich mit dem Buchbergeralgorithmus vorgenommen.

8. Implementationsfragen Die Entwicklung der in der Arbeit dargestellten Algorithmen verlief parallel zum Aufbau des Spezialcomputeralgebrasystems Felix (siehe [AK91]). Am Ende dieser Arbeit werden wir die Fähigkeiten des Systems anhand einer sehr komplexen Anwendung, welche im Zusammenhang mit der Klassifikation von Differentialkalkülen bearbeitet wurde (siehe [AS94]), näher beleuchten.

Kapitel 2

Effektive algebraische Strukturen

2.1 Einführende Bemerkungen

Viele klassische Algorithmen der Mathematik, wie zum Beispiel der Euklidische oder der Gaußsche Algorithmus, sind von der Gestalt, daß sie erst dann zu einem Algorithmus im Sinne der Berechenbarkeitstheorie, d.h. zu einer Berechnungsvorschrift einer berechenbaren Funktion, werden, wenn sie in algebraischen Strukturen mit berechenbaren Grundoperationen eingesetzt werden. Wenngleich beispielsweise problemlos nachgewiesen werden kann, daß jeder univariate Polynomring über einem beliebigen Körper ein Euklidischer Ring ist, so gibt es dennoch keine Hoffnung, den größten gemeinsamen Teiler zweier Polynome zu berechnen, falls der Körper so beschaffen ist, daß von einem konkreten Element nicht einmal feststellbar ist, ob es sich dabei um das Nullelement handelt. Wir sprechen dann auch von relativer Berechenbarkeit der durch die Anweisungsfolge definierten Funktion in Bezug auf die Effektivität der zugrundeliegenden algebraischen Struktur. Im Moment formulieren wir grob, daß eine algebraische Struktur *effektiv* genannt wird, wenn in ihr alle Grundoperationen und -relationen berechenbar beziehungsweise entscheidbar sind. Später werden wir die Definition präzisieren.

In dieser Arbeit werden wir den Berechenbarkeitsnachweis einer Funktion häufig durch die explizite Angabe einer Vorschrift zu ihrer Berechnung führen. In jedem Fall verlangen wir von einer Anweisungsfolge zur Berechnung einer n-stelligen Funktion f, daß sie korrekt in dem Sinne ist, daß sie im Falle des Anhaltens bei einer Eingabe $x_1, \ldots, x_n$ immer den Funktionswert $f(x_1, \ldots, x_n)$ liefert. Dabei wird vorausgesetzt, daß die auftretenden unvollständig spezifizierten Funktionen durch eine im gleichen Sinne korrekte Berechnungsvorschrift gegeben sind. Belassen wir es nur bei diesen Korrektheitsforderungen, so berechnet unsere Anweisungsfolge möglicherweise nicht ganz f, sondern wir wissen nur, daß es eine (im Extremfall leere) rekursiv aufzählbare Teilmenge $\Omega \subseteq A^n$ von n-Tupeln der Trägermenge A gibt, so daß die untersuchte Anweisungsfolge ein Algorithmus für die eingeschränkte Funktion $f\,|_\Omega$ ist. In diesem Falle werden wir bestrebt sein, ein im Sinne der Mengeninklusion möglichst großes Ω zu fin-

den. Um zu beweisen, daß die vorliegende Anweisungsfolge die Einschränkung $f\,|_\Omega$ berechnet, ist zusätzlich zum Korrektheitsbeweis noch ein Terminationsbeweis erforderlich. In diesem ist nachzuweisen, daß die Abarbeitung der Anweisungsfolge bei Eingabe eines beliebigen n-Tupels aus $dom\,(f\,|_\Omega) = dom(f) \cap \Omega$ anhält. Im Idealfall gelingt ein solcher Terminationsbeweis für $\Omega = A^n$. Andernfalls kann auch bereits der Berechenbarkeitsnachweis einer geeigneten Einschränkung von Interesse sein.

Enthält die Anweisungsfolge Funktionsaufrufe, so erfordert der Berechenbarkeitsnachweis auch die Berechenbarkeitsnachweise aller gerufenen Funktionen. Führt man dagegen Korrektheits- und Terminationsbeweis einer Berechnungsvorschrift nur unter der Annahme, daß jede innerhalb der Vorschrift aufgerufene Funktion bei einer beliebigen Eingabe aus ihrem Definitionsbereich nach endlicher Zeit ein korrektes Ergebnis liefert, so ist damit die relative Berechenbarkeit der Hauptfunktion in Bezug auf die Unterfunktionen nachgewiesen.

Kommen wir noch einmal auf das eingangs erwähnte Beispiel des Euklidischen Algorithmus zurück. Betrachtet man ihn in einem effektiven Euklidischen Ring, wie zum Beispiel dem Ring der ganzen Zahlen oder einem univariaten Polynomring über einem effektiven Körper, so wird er zu einem Algorithmus im strengen Sinne der Berechenbarkeitstheorie und er berechnet gerade die Funktion, die je zwei Ringelementen ihren größten gemeinsamen Teiler (ggT) zuordnet. Man kann also sagen, daß der Euklidische Algorithmus relativ zur Effektivität der zugrundeliegenden algebraischen Struktur algorithmisch ist.

Betrachten wir einen überabzählbaren und damit auf keinen Fall effektiven Euklidischen Ring, wie zum Beispiel einen univariaten Polynomring über den reellen oder komplexen Zahlen, so ist der Euklidische Algorithmus nicht mehr im strengen Sinne algorithmisch. Jedoch ist wenigstens die Einschränkung der von ihm beschriebenen ggT-Funktion auf einen beliebigen effektiven Euklidischen Unterring berechenbar und für diese Einschränkung stellt er einen Berechnungsalgorithmus dar. Ebenso können Einschränkungen auf beliebige Mengen vorgenommen werden, welche nicht notwendigerweise Trägermenge eines Unterrings sind und auf welchen die Abarbeitung stets abbricht.

Gegenstand der vorliegenden Arbeit sind Untersuchungen zur Berechenbarkeit von Funktionen und Entscheidbarkeit von Prädikaten in Ringen, Algebren und Moduln. Die dabei entwickelten Algorithmen werden immer wieder einen ähnlichen Charakter aufweisen, wie wir ihn gerade beim Euklidischen Algorithmus diskutiert haben. Daher ist es notwendig, die bisher naiv verwendeten Begriffe zur Berechenbarkeit und Effektivität exakt zu fassen. Bevor wir jedoch eine Definition einer effektiven algebraischen Struktur geben können, müssen wir zunächst festlegen, in welcher Form uns eine algebraische Struktur gegeben sein soll. Dabei haben wir es mit einem Wechselspiel logischer Theorien und algebraischer Modelle zu tun. Wir beginnen daher mit kurzen Einführungen in die Begriffswelt der Theorien der partiell-rekursiven Funktionen, der universellen Algebra und des Prädikatenkalküls erster Stufe.

Für die Schreibweise der Hintereinanderausführung zweier Funktionen $g : A \to B$ und $f : B \to C$ treffen wir in der vorliegenden Arbeit die folgende Konvention. $g \circ f$ bezeichnet die Funktion mit Vorbereich A und Nachbereich C, die für alle $a \in A$ der Abbildungsvorschrift $(g \circ f)(a) = f(g(a))$ genügt. Mit

anderen Worten, die Funktionen werden von links nach rechts abgearbeitet.

2.1.1 Partiell-rekursive Funktionen

Wir stützen uns auf das Berechenbarkeitsmodell der *partiell-rekursiven Funktionen* (siehe z.B. [Wa94]). Zur Definition des Begriffs der partiell-rekursiven Funktion benötigen wir zunächst die Funktoren *Comp* der Komposition, *Rek* der primitiven Rekursion und μ der μ-Rekursion, welche aus Funktionen über dem Bereich der natürlichen Zahlen weitere derartige Funktionen konstruieren.

- Die Komposition $Comp(f, g_1, \ldots, g_m) : \mathbb{N}^n \to \mathbb{N}$ der Funktionen $f : \mathbb{N}^m \to \mathbb{N}$ und $g_1, \ldots, g_m : \mathbb{N}^n \to \mathbb{N}$ ist durch

  $$Comp(f, g_1, \ldots, g_m)(x_1, \ldots, x_n) := f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

  definiert.

- Die primitive Rekursion $Rek(g, h) : \mathbb{N}^n \to \mathbb{N}$ von $g : \mathbb{N}^{n-1} \to \mathbb{N}$ und $h : \mathbb{N}^{n+1} \to \mathbb{N}$ genügt den Bedingungen:

  $$\begin{aligned} Rek(g,h)(x_1, \ldots, x_{n-1}, 0) &:= g(x_1, \ldots, x_{n-1}) \\ Rek(g,h)(x_1, \ldots, x_{n-1}, y+1) &:= h(x_1, \ldots, x_{n-1}, y, \\ &\qquad Rek(g,h)(x_1, \ldots, x_{n-1}, y)) \end{aligned}$$

- Sei $f : \mathbb{N}^n \to \mathbb{N}$, dann beschreibt

  $$\mu f(x_1, \ldots, x_n) := \begin{cases} y & : \text{ falls } f(x_1, \ldots, x_{n-1}, y) = 0 \text{ und} \\ & \quad \forall z < y \, : \, f(x_1, \ldots, x_{n-1}, z) > 0 \\ \bot & : \text{ sonst} \end{cases}$$

  die μ-Rekursion von f.

Dabei beachte man, wenn auf der rechten Seite einer der obigen Definitionen ein Bezug auf einen Funktionswert einer Funktion an einer nicht zu ihrem Definitionsbereich gehörigen Stelle auftritt, so ist die zusammengesetzte Funktion an der betreffenden Stelle undefiniert. Weiterhin impliziert die Gültigkeit der Ungleichung $f(x_1, \ldots, x_{n-1}, z) > 0$ die Definiertheit von f an der Stelle $(x_1, \ldots, x_{n-1}, z)$.

Wir definieren die Nullfunktion $Z : \mathbb{N} \to \mathbb{N}$ mit $\forall x \in \mathbb{N} \, : \, Z(x) = 0$, die Nachfolgerfunktion $S : \mathbb{N} \to \mathbb{N}$ mit $\forall x \in \mathbb{N} \, : \, S(x) = x + 1$ und für jedes $m = 1, 2, \ldots$ und $1 \leq n \leq m$ eine Projektionsfunktion $I_n^m : \mathbb{N}^m \to \mathbb{N}$ mit $\forall x_1, \ldots, x_m \in \mathbb{N} \, : \, I_n^m(x_1, \ldots, x_m) = x_n$.

Die Menge PRF der partiell-rekursiven Funktionen ist die kleinste Menge endlichstelliger Funktionen über den natürlichen Zahlen, die die Nullfunktion, die Nachfolgerfunktion und alle Projektionsfunktionen enthält und abgeschlossen gegenüber Komposition, primitiver Rekursion und μ-Rekursion ist.

Im Falle $f \in PRF$ nennen wir die Funktion *berechenbar*. Durch

$$\chi_M(a) = \begin{cases} 1 & : \quad a \in M \\ 0 & : \quad a \in \mathbb{N} \backslash M \end{cases}$$

kann man jeder Teilmenge $M \subseteq \mathbb{N}$ der natürlichen Zahlen eine *charakteristische Funktion* $\chi_M : \mathbb{N} \to \mathbb{N}$ zuordnen. Ist χ_M eine partiell-rekursive Funktion, dann nennen wir die Menge M *entscheidbar*. Eine Menge M heißt *rekursiv aufzählbar*, falls es eine partiell-rekursive Funktion $f : \mathbb{N} \to \mathbb{N}$ gibt, die M als Bildbereich hat.

Eine Funktion g wird *relativ* zu einer Menge $\mathcal{F}$ von Funktionen über den natürlichen Zahlen *berechenbar* genannt, falls g durch endlich viele Kompositionen, primitive Rekursionen und μ-Rekursionen aus Funktionen von $\mathcal{F}$ und partiell-rekursiven Funktionen konstruierbar ist (siehe [Sh67]). Ist g relativ zu $\mathcal{F}$ berechenbar, so impliziert die Berechenbarkeit aller Funktionen aus $\mathcal{F}$ auch die Berechenbarkeit von g, das heißt $\mathcal{F} \subseteq PRF \Rightarrow g \in PRF$.

Sei Ω ein höchstens abzählbar unendliches Alphabet. Dann läßt sich die Berechenbarkeit von Funktionen über der Wortmenge Ω^* durch *Gödelisierung* auf die Theorie der partiell-rekursiven Funktionen zurückführen. Allgemein versteht man unter einer *Gödelisierung* der Menge Ω^* eine injektive Funktion $\nu : \Omega^* \to \mathbb{N}$ mit entscheidbarem Bildbereich $im(\nu)$, wobei sowohl ν als auch die Umkehrabbildung ν^{-1} algorithmisch sind. Vermöge einer beliebigen Gödelisierung übertragen sich die Begriffe der Berechenbarkeit, rekursiven Aufzählbarkeit und Entscheidbarkeit durch Abbildung in die Menge der natürlichen Zahlen auf Funktionen und Teilmengen von Ω^*. Zu jeder unendlichen, entscheidbaren Teilmenge M der natürlichen Zahlen läßt sich eine bijektive Abbildung $\tau : M \to \mathbb{N}$ finden, so daß τ und τ^{-1} berechenbar sind. Daher stellt es keine Einschränkung dar, in Zukunft von einer Gödelisierung die Bijektivität zu fordern.

2.1.2 Universelle Algebra

Unter einer *Signatur* verstehen wir ein Tripel $\Sigma = (F, R, \sigma)$. Dabei ist F eine Menge von Operations- und R eine Menge von Relationssymbolen. F und R sind disjunkt und $\sigma : F \cup R \to \mathbb{N}$ ist eine Abbildung der Vereinigung beider Mengen in die natürlichen Zahlen. $\sigma(S)$ gibt die Stelligkeit eines Symbols $S \in F \cup R$ an.

Sei A eine Menge von Objekten. Eine totale Funktion $g : A^n \to A$ heißt n-stellige *Operation* über A. Gilt $n = 0$, so zeichnet g ein Element von A aus, wir nennen g auch eine Konstante aus A. Eine Teilmenge $R \subseteq A^n$ wird n-stellige *Relation* über A genannt. Ein *algebraisches System* (auch algebraische Struktur genannt) der Signatur $\Sigma = (F, R, \sigma)$ ist ein Tripel $\mathcal{A} = (A, \{g_f\}_{f \in F}, \{P_\rho\}_{\rho \in R})$ bestehend aus einer *Trägermenge* A, einer Menge $G = \{g_f\}_{f \in F}$ von Operationen und einer Menge $P = \{P_\rho\}_{\rho \in R}$ von Relationen, wobei g_f eine $\sigma(f)$-stellige Funktion und P_ρ eine $\sigma(\rho)$-stellige Relation ist.

Für den Rest dieses Abschnitts setzen wir die Endlichkeit der Vereinigungsmengen $F \cup R$ voraus und vereinbaren die alternative Signaturangabe $\Sigma = (f_1, \ldots, f_n; \rho_1, \ldots, \rho_m; \sigma)$. Seien $\Sigma_1 = (f_1, \ldots, f_n; \rho_1, \ldots, \rho_m; \sigma_1)$ und $\Sigma_2 = (f_1, \ldots, f_n, \ldots, f_{n'}; \rho_1, \ldots, \rho_m, \ldots, \rho_{m'}; \sigma_2)$, mit $\sigma_1(f_i) = \sigma_2(f_i)$ für alle $i = 1, \ldots, n$ und $\sigma_1(\rho_j) = \sigma_2(\rho_j)$ für alle $j = 1, \ldots, m$, zwei Signaturen und $\mathcal{A}_1 = (A; g_1, \ldots, g_n; P_1, \ldots, P_m)$ und $\mathcal{A}_2 = (A; g_1, \ldots, g_{n'}; \rho_1, \ldots, \rho_{m'})$ zwei algebraische Systeme der Signaturen Σ_1 beziehungsweise Σ_2, wobei $\mathcal{A}_2$ aus $\mathcal{A}_1$

durch Hinzunahme zusätzlicher Operationen und Relationen hervorgeht. Dann wird $\mathcal{A}_2$ eine Σ_2-*Expansion* von $\mathcal{A}_1$ und $\mathcal{A}_1$ eine Σ_1-*Reduktion* von $\mathcal{A}_2$ genannt. Dafür schreiben wir auch $\mathcal{A}_2 = (\mathcal{A}_1; g_{n+1}, \ldots, g_{n'}; P_{m+1}, \ldots, P_{m'})$.

Enthält ein algebraisches System keine Relationen, so wird es auch *abstrakte Algebra* genannt. Enthält es dagegen keine Operationen, so wird es als *Relationalsystem* bezeichnet.

Eine nichtleere Teilmenge $B \subseteq A$ der Trägermenge des algebraischen Systems $\mathcal{A} = (A; g_1, \ldots, g_n; P_1, \ldots, P_m)$ der Signatur $\Sigma = (f_1, \ldots, f_n; \rho_1, \ldots, \rho_m; \sigma)$ heißt abgeschlossen gegenüber der Operation g_i, falls für alle $(b_1, \ldots, b_{\sigma(f_i)}) \in B^{\sigma(f_i)}$ die Enthaltenseinsbeziehung $g_i(b_1, \ldots, b_{\sigma(f_i)}) \in B$ gilt. Bezeichne $g_i \mid_B$ die Einschränkung der Funktion g_i auf B und $P_j \mid_B$ die durch $P_j \mid_B = P_j \cap B^{\sigma(\rho_j)}$ erklärte Einschränkung der Relation P_j auf B. Dann nennen wir $\mathcal{B} = (B; g_1 \mid_B, \ldots, g_n \mid_B; P_1 \mid_B, \ldots, P_m \mid_B)$ ein *algebraisches Untersystem* von $\mathcal{A}$, falls B gegenüber allen Operationen $g_1, \ldots, g_n$ abgeschlossen ist. Ist $\mathcal{B}$ ein algebraisches Untersystem von $\mathcal{A}$, so wird $\mathcal{A}$ auch *algebraisches Obersystem* von $\mathcal{B}$ genannt. Zu jeder nichtleeren Teilmenge $C \subseteq A$ gibt es ein kleinstes (bezüglich Inklusion der Trägermengen) algebraisches Untersystem $\mathcal{B}$ von $\mathcal{A}$ derart, daß C Teilmenge der Trägermenge von $\mathcal{B}$ ist. Die Menge C wird ein *Erzeugendensystem* von $\mathcal{B}$ genannt. Im allgemeinen ist es nicht sinnvoll, nach dem Erzeugnis der leeren Menge $C = \emptyset$ zu fragen, da leere Trägermengen unzulässig sind. Enthält Σ jedoch wenigstens eine Konstante c, so kann man das Erzeugnis von $\{c\}$ auch als von $\emptyset$ erzeugt auffassen.

$\mathcal{A} = (A; g_1, \ldots, g_n; P_1, \ldots, P_m)$ und $\mathcal{B} = (B; h_1, \ldots, h_n; Q_1, \ldots, Q_m)$ seien zwei algebraische Systeme der Signatur $\Sigma = (f_1, \ldots, f_n; \rho_1, \ldots, \rho_m; \sigma)$. Eine Funktion $\varphi : A \to B$ wird Σ-*Homomorphismus* von $\mathcal{A}$ nach $\mathcal{B}$ genannt, falls die folgenden Bedingungen erfüllt sind:

i) Für jede Operation g_i und beliebige Elemente $a_1, \ldots, a_{\sigma(f_i)} \in A$ gilt:

$$\varphi(g_i(a_1, \ldots, a_{\sigma(f_i)})) = h_i(\varphi(a_1), \ldots, \varphi(a_{\sigma(f_i)})) \quad .$$

ii) Für jede Relation P_i und beliebige Elemente $a_1, \ldots, a_{\sigma(\rho_i)} \in A$ gilt:

$$(a_1, \ldots, a_{\sigma(f_i)}) \in P_i \Rightarrow (\varphi(a_1), \ldots, \varphi(a_{\sigma(f_i)})) \in Q_i \quad .$$

Gilt in der zweiten Bedingung sogar die Äquivalenz anstelle der Implikation, so sprechen wir von einem *starken* Σ-*Homomorphismus*. Ist φ ein bijektiver, starker Σ-Homomorphismus, so wird φ als Σ-Isomorphismus zwischen $\mathcal{A}$ und $\mathcal{B}$ bezeichnet. Ist der Σ-Homomorphismus φ injektiv, so nennen wir ihn Σ-Monomorphismus, ist er surjektiv, so wird er Σ-Epimorphismus genannt. Ein Σ-Homomorphismus $\varphi : \mathcal{A} \to \mathcal{A}$ einer Algebra $\mathcal{A}$ in sich selbst heißt Σ-Endomorphismus und falls φ Σ-Isomorphismus ist, so nennen wir φ einen Σ-Automorphismus.

Die durch $(a, b) \in ker_u(\varphi) \Longleftrightarrow_{def} \varphi(a) = \varphi(b)$ definierte binäre Relation $ker_u(\varphi)$ wird der *Kern* des Σ-Homomorphismus φ genannt. Der Index u dient zur Unterscheidung von den später benötigten Kernen von Gruppen- und Ringhomomorphismen. Eine Äquivalenzrelation $C \subseteq A \times A$ wird eine *Kongruenzrelation* des algebraischen Systems $\mathcal{A} = (A; g_1, \ldots, g_n; P_1, \ldots, P_m)$ der

Signatur $\Sigma = (f_1, \ldots, f_n; \rho_1, \ldots, \rho_m, \sigma)$ genannt, falls für jede Operation g_i, $i = 1, \ldots, n$, und beliebige Paare $(a_j, b_j) \in C$, $j = 1, \ldots, \sigma(f_i)$, die Beziehung $\big(g_i(a_1, \ldots, a_{\sigma(f_i)}), g_i(b_1, \ldots, b_{\sigma(f_i)})\big) \in C$ gilt. Durch

$$\bar{g}_i([a_1], \ldots, [a_{\sigma(f_i)}]) := [g_i(a_1, \ldots, a_{\sigma(f_i)})] \quad (a_j \in A)$$

und

$$([a_1], \ldots, [a_{\sigma(\rho_i)}]) \in \bar{P}_i :\Longleftrightarrow \exists b_j \in [a_j] \; : \; (b_1, \ldots, b_{\sigma(\rho_i)}) \in P_i \quad (a_j \in A)$$

werden Operationen und Relationen auf der Menge $\bar{A} = A/C = \{[a] \mid a \in A\}$ der Äquivalenzklassen von A modulo C definiert. Das dabei entstehende algebraische System $\mathcal{A}/\mathcal{C} = \big(\bar{A}; \bar{g}_1, \ldots, \bar{g}_n; \bar{P}_1, \ldots, \bar{P}_m\big)$ der Signatur Σ wird die *Faktorstruktur* von $\mathcal{A}$ nach der Kongruenzrelation C genannt. Die durch $a \mapsto [a]$ definierte Abbildung von $\mathcal{A}$ nach $\mathcal{A}/\mathcal{C}$ ist ein surjektiver Σ-Homomorphismus. Umgekehrt ist der Kern eines von $\mathcal{A}$ ausgehenden Σ-Homomorphismus stets eine Kongruenzrelation und der Homomorphiesatz sagt aus, daß das homomorphe Bild von $\mathcal{A}$ unter einem starken Homomorphismus φ isomorph zur Faktorstruktur $\mathcal{A}/ker_u(\varphi)$ ist. Im Falle abstrakter Algebren ist jeder Homomorphismus stark und die Faktoralgebren $\mathcal{A}/\mathcal{C}$ sind bis auf Isomorphie die einzigen homomorphen Bilder einer abstrakten Algebra $\mathcal{A}$.

Sei $\Sigma = (F, \emptyset, \sigma)$ die Signatur einer Klasse abstrakter Algebren. Eine Sonderstellung in der Klasse aller abstrakten Algebren der Signatur Σ nehmen die sogenannten *Termalgebren* ein. Sei X eine Menge von Objekten mit der Eigenschaft $X \cap F = \emptyset$. Die Trägermenge $T(\Sigma, X) \subseteq (X \cup F)^*$ der Termalgebra $\mathcal{T}_\Sigma(X)$ ist die kleinste Menge von Wörtern über dem Alphabet $X \cup F$, die X und alle nullstelligen Funktionssymbole umfaßt und abgeschlossen ist gegenüber der Bildung von Wörtern $f t_1 \cdots t_{\sigma(f)}$, wobei $f \in F$ und $t_i \in T(\Sigma, X)$. Die Elemente von $T(\Sigma, X)$ nennen wir Σ-*Terme in* X. Falls Σ und X aus dem Kontext heraus klar sind, so sprechen wir auch einfach von Termen. Die zu f gehörige Operation in $\mathcal{T}_\Sigma(X)$ wird ebenfalls mit f bezeichnet und ist durch $f(t_1, \ldots, t_{\sigma(f)}) := f t_1 \cdots t_{\sigma(f)}$ definiert. Es ist offensichtlich, daß X die Algebra $\mathcal{T}_\Sigma(X)$ erzeugt.

Die Sonderrolle von $\mathcal{T}_\Sigma(X)$ kommt darin zum Ausdruck, daß es zu jeder abstrakten Algebra $\mathcal{A}$ der Signatur Σ und jeder Funktion $j : X \to A$ einen eindeutig bestimmten Homomorphismus $\iota : \mathcal{T}_\Sigma(X) \to \mathcal{A}$ gibt, der j fortsetzt, das heißt $\iota \mid_X = j$. Dieser Sachverhalt wird auch damit umschrieben, daß man sagt,$\mathcal{T}_\Sigma(X)$ ist freie Algebra mit freiem Erzeugendensystem X in der Klasse aller Σ-Algebren. Aus dem Homomorphiesatz folgt, daß es zu jeder Σ-Algebra $\mathcal{A}$ eine Menge X gibt, so daß $\mathcal{A}$ homomorphes Bild der Termalgebra $\mathcal{T}_\Sigma(X)$ ist.

Sei $\Sigma = (F, R, \sigma)$ und nicht notwendigerweise $R = \emptyset$. Dann verstehen wir unter einer von X erzeugten Σ-Termalgebra eine Σ-Expansion der Termalgebra $\mathcal{T}_{(F, \emptyset, \sigma|_F)}(X)$.

Weitergehende Ausführungen zur Theorie der universellen Algebra findet man beispielsweise in [Lu76] oder [Co81].

2.1.3 Elementare Logik

Sei $\Sigma = (F, R, \sigma)$ eine Signatur und X eine Menge von Individuenvariablen mit $X \cap (R \cup F) = \emptyset$. Beschreiben wir zunächst die Syntax der elementaren Logik[1]. Die Menge der *logischen Formeln* der Signatur Σ in den Individuenvariablen X ist die kleinste Wortmenge über dem Alphabet $F \cup R \cup X \cup \{(,), \neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists\}$ die alle Atomformeln enthält und abgeschlossen ist gegenüber der Bildung von $\neg(A), (A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B), \forall x(A(x))$ und $\exists x(A(x))$. Dabei hat eine Atomformel die Gestalt $\rho t_1 \cdots t_{\sigma(\rho)}$, A und B sind logische Formeln und $A(x)$ bezeichnet eine logische Formel, in der x vollfrei vorkommt, d.h. $A(x)$ enthält weder die Zeichenkette $\forall x$ noch $\exists x$. In Zukunft werden wir die üblichen Regeln zum Weglassen von Klammern anwenden.

Wir vereinbaren die Bezeichnungen $\mathfrak{Alg}(\Sigma)$ für die Klasse aller algebraischen Systeme der Signatur Σ, $\mathfrak{Fm}(\Sigma)$ für die Menge aller logischen Formeln der Signatur Σ, $\mathfrak{Alg}$ für die Klasse aller algebraischen Systeme beliebiger Signatur und $\mathfrak{Fm}$ für die Klasse aller logischen Formeln des Prädikatenkalküls erster Stufe. Eine Formelmenge $\mathfrak{F} \subseteq \mathfrak{Fm}(\Sigma)$ nennen wir eine *(elementare) Theorie*. Die Semantik des Prädikatenkalküls erster Stufe wird durch eine binäre Relation $\models \subseteq \mathfrak{Alg} \times \mathfrak{Fm}$ vermittelt.

$val_{\mathcal{A},j} : \mathfrak{Fm}(\Sigma) \rightarrow \{0, 1\}$ bezeichne die übliche Wertfunktion, die jeder Formel $H \in \mathfrak{Fm}(\Sigma)$ bei fester Interpretation $\mathcal{A} \in \mathfrak{Alg}(\Sigma)$ und fester Belegung $j : X \rightarrow A$ einen der Werte 0 oder 1 zuordnet. Gilt für festes $\mathcal{A}$ und festes H bei jeder Belegung $j : X \rightarrow A$ die Gleichheit $val_{\mathcal{A},j}(H) = 1$, so nennen wir H in $\mathcal{A}$ gültig und schreiben dafür $\mathcal{A} \models H$. In diesem Fall bezeichnen wir $\mathcal{A}$ auch als ein *Modell* der logischen Formel H.

Sei H eine logische Formel der Signatur Σ. Die Teilklasse $\mathfrak{Mod}(H) = \{\mathcal{A} \in \mathfrak{Alg}(\Sigma) \mid \mathcal{A} \models H\}$ aller Σ-Algebren in denen H gültig ist, wird die *Modellklasse* von H genannt. Umgekehrt heißt die Menge $\mathfrak{Th}(\mathcal{A}) = \{H \in \mathfrak{Fm}(\Sigma) \mid \mathcal{A} \models H\}$ aller in einer festen algebraischen Σ-Struktur $\mathcal{A}$ gültigen Formeln die *Theorie* von $\mathcal{A}$. Die Begriffe der Modellklasse und der Theorie werden durch $\mathfrak{Mod}(\mathfrak{F}) = \bigcap_{H \in \mathfrak{F}} \mathfrak{Mod}(H)$ beziehungsweise $\mathfrak{Th}(\mathfrak{A}) = \bigcap_{\mathcal{A} \in \mathfrak{A}} \mathfrak{Th}(\mathcal{A})$ auf beliebige Mengen $\mathfrak{F} \subseteq \mathfrak{Fm}(\Sigma)$ von Formeln und Klassen $\mathfrak{A} \subseteq \mathfrak{Alg}(\Sigma)$ von algebraischen Strukturen erweitert.

Durch $X \models A \iff \forall \mathcal{A} \in \mathfrak{Mod}(X) \ : \ \mathcal{A} \models A$ erklären wir die Folgerungsrelation $\models \subseteq Pow(\mathfrak{Fm}(\Sigma)) \times \mathfrak{Fm}(\Sigma)$ der elementaren Logik. Die Menge $\{A \mid X \models A\}$ aller aus X folgenden Formeln bezeichnen wir mit $X^{\models}$. Wir stellen nun eine Reihe später benötigter Definitionen bereit, dabei bedienen wir uns jeweils der semantischen Fassung. Auf die Einführung einer syntaktischen Ableitungsrelation $\vdash \subseteq Pow(\mathfrak{Fm}(\Sigma)) \times \mathfrak{Fm}(\Sigma)$ werden wir hier verzichten. Die Berechtigung des Verzichts besteht im Gödelschen Vollständigkeitssatz, welcher die Gleichheit $\models = \vdash$ zum Inhalt hat. Wir weisen aber auch darauf hin, daß eine Ableitungsrelation im Rahmen konstruktiver und beweistheoretischer Betrachtungen unabdingbar wäre.

Falls $\mathfrak{Mod}(\mathfrak{F}) \neq \emptyset$ gilt, so nennen wir die Theorie $\mathfrak{F}$ *konsistent*. Im Falle $\mathfrak{F}^{\models} = \mathfrak{G}^{\models}$ werden die Theorien $\mathfrak{F}$ und $\mathfrak{G}$ *äquivalent* genannt. Falls es eine

[1] Neben den Begriffen der elementaren oder höheren Logik werden synonym auch die Bezeichnungen Prädikatenkalkül erster beziehungsweise höherer Stufe verwendet.

entscheidbare, zu $\mathfrak{F}$ äquivalente Theorie gibt, so heißt $\mathfrak{F}$ *axiomatisierbar*. Eine konsistente Theorie $\mathfrak{F}$ der Signatur Σ wird *vollständig* genannt, falls jede einfache Erweiterung $\mathfrak{F} \subset \mathfrak{F}' \subseteq \mathfrak{Fm}(\Sigma)$ von ihr entweder inkonsistent oder zu $\mathfrak{F}$ äquivalent ist. Schließlich nennen wir eine konsistente Theorie $\mathfrak{F}$ *kategorisch*, falls je zwei ihrer Modelle zueinander isomorph sind.

Die Signatur $\Sigma = (F, P, \sigma)$ enthalte wenigstens ein nullstelliges Funktionssymbol und das algebraische System $\mathcal{A} \in \mathfrak{Alg}(\Sigma)$ sei ein Modell der Theorie $\mathfrak{F} \subseteq \mathfrak{Fm}(\Sigma)$. Wir betrachten die Signatur $\Sigma' = (F, \emptyset, \sigma \mid_F)$, die sich durch Entfernen aller Relationssymbole aus Σ ergibt. Aufgrund der Existenz eines Konstantensymbols in Σ' existiert die Termalgebra $\mathcal{T}_{\Sigma'}(\emptyset)$ und es gibt einen eindeutig bestimmten Homomorphismus $\iota : \mathcal{T}_{\Sigma'}(\emptyset) \to \mathcal{A}_{\Sigma'}$ der Termalgebra in das Σ'-Redukt $\mathcal{A}_{\Sigma'}$ von $\mathcal{A}$. Außerdem existiert eine Σ-Expansion $\mathcal{T}_{\Sigma}(\emptyset)$ von $\mathcal{T}_{\Sigma'}(\emptyset)$, so daß ι ein starker Homomorphismus von $\mathcal{T}_{\Sigma}(\emptyset)$ in $\mathcal{A}$ ist. Falls ι surjektiv ist, so wird $\mathcal{A}$ ein *kanonisches Modell* von $\mathfrak{F}$ genannt. Mit anderen Worten ausgedrückt bedeutet die Surjektivität von ι gerade, daß jedes Element der Trägermenge von $\mathcal{A}$ Interpretation eines variablenfreien Terms ist. Umgekehrt nennen wir eine Theorie $\mathfrak{F}$ der Signatur Σ eine *kanonische Theorie*, falls jedes Funktions- und Relationssymbol aus Σ in wenigstens einer der Formeln aus $\mathfrak{F}$ vorkommt und sie ein kanonisches Modell der Signatur Σ besitzt.

Sei $\Sigma = (F, P, \sigma)$ eine Signatur und C eine Menge von Objekten, so daß $C \cap (F \cup P) = \emptyset$. Dann nennen wir die Signatur $\Sigma_C = (F \cup C, P, \sigma')$, mit $\sigma'(S) = \sigma(S)$ für alle $S \in F \cup P$ und $\sigma'(c) = 0$ für alle $c \in C$, eine *Konstantenerweiterung* von Σ. Zu jeder konsistenten Theorie $\mathfrak{F} \subset \mathfrak{Fm}(\Sigma)$ existiert eine geeignete Konstantenerweiterung Σ_C und eine konsistente kanonische Theorie $\mathfrak{F}^*$, so daß $\mathfrak{F} \subseteq \mathfrak{F}^* \subset \mathfrak{Fm}(\Sigma_C)$ (siehe [He49]).
Weiterführende Ausführungen zur mathematischen Logik findet man beispielsweise in [Bet59], [Sh67] oder [GH90].

2.2 Effektive Modelle und Theorien

Wir kommen nunmehr auf das Hauptanliegen dieses Kapitels, nämlich die Frage nach der Effektivität einer algebraischen Struktur, zurück. Unsere Intention ist, daß in einer derartigen Struktur jede Grundoperationen berechenbar und jede Grundrelation entscheidbar sein soll.

Intuitiv ist ein univariater Polynomring $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$ genau dann als effektiv anzusehen, wenn $\mathbb{K}$ ein effektiver Körper ist. Genau dann sollen zum Beispiel der Euklidische, der Gaußsche oder der Buchbergersche Algorithmus berechenbare Funktionen beschreiben. Betrachten wir die Effektivität des Körpers $\mathbb{K}$ einmal aus diesem Blickwinkel.

Sei $\mathbb{K}$ ein Zwischenkörper der rationalen Zahlen $\mathbb{Q}$ und eines geeigneten Oberkörpers $\mathbb{L}$, welcher durch Adjunktion endlich vieler Elemente $x_1, \ldots, x_r \in \mathbb{L}$ zu $\mathbb{Q}$ entsteht, d.h. $\mathbb{Q} \subseteq \mathbb{K} = \mathbb{Q}(x_1, \ldots, x_r) \subseteq \mathbb{L}$. Durch Anwendung elementarer Argumente der Körpertheorie (siehe z.B. [vW67]) weist man leicht die Existenz von Elementen $X_1, \ldots, X_n, y \in \mathbb{K}$ mit den folgenden Eigenschaften nach: $0 \leq n \leq r$, X_1 ist transzendent über $\mathbb{Q}$, X_i ist transzendent über $\mathbb{Q}(X_1, \ldots, X_{i-1})$ für $i = 2, \ldots, n$, y ist algebraisch über $\mathbb{Q}(X_1, \ldots, X_n)$ mit

charakteristischem Polynom $p(Y) \in \mathbb{Q}(X_1, \ldots, X_n)[Y]$ und es gilt

$$\mathbb{K} = \mathbb{Q}(X_1, \ldots, X_n, y) \simeq \mathbb{Q}(X_1, \ldots, X_n)[Y]/p(Y) \; .$$

Der Körper $\mathbb{Q}(X_1, \ldots, X_n)[Y]/p(Y)$ ist intuitiv effektiv. Auch eine Übertragung dieser Auffassung auf $\mathbb{Q}(X_1, \ldots, X_n, y)$ erscheint vernünftig.

Dennoch gibt es gute Argumente, nicht jeden auf die obige Weise gebildeten Körper $\mathbb{K}$ als effektiv anzusehen. Eine notwendige Anforderung an einen effektiven Körper $\mathbb{K}$ ist die Entscheidbarkeit seiner Gleichheitsrelation. Insbesondere muß die Nulläquivalenz eines rationalen Ausdrucks in den Elementen $x_1, \ldots, x_r$ entscheidbar sein. Bereits für Zahlkörper, d.h. $\mathbb{L} = \mathbb{C}$, bereitet die Entscheidbarkeit der Nulläquivalenz große Probleme (siehe z.B. [La71]). Dem Autor ist allerdings nicht bekannt, ob bereits die Unentscheidbarkeit der Nulläquivalenz bewiesen werden konnte. Für den Fall von Funktionenkörpern $\mathbb{K}$ und $\mathbb{L}$ liegen jedoch definitiv Unentscheidbarkeitsnachweise vor. Sei P der Ring aller reellwertigen Funktionen, die sich aus der Konstanten π, den rationalen Zahlen und der Variablen X sowie den Funktionen $+, *, sin$ und abs mit Hilfe von endlich vielen Kompositionen bilden lassen. Der Ring P ist nullteilerfrei und wir wählen seinen Quotientenkörper als $\mathbb{L}$.

Ausgehend von einem Unentscheidbarkeitsresultat Richardsons für Terme einer umfangreicheren Klasse reellwertiger Funktionen (siehe [Ri68]) konnte Caviness die Entscheidbarkeit des 10. Hilbertschen Problems auf die Entscheidbarkeit der Nulläquivalenz eines Terms zur Beschreibung einer Funktion von P reduzieren (siehe [Ca70]). Kurze Zeit später veröffentlichte Matijasevic sein berühmtes Resultat der Unentscheidbarkeit des 10. Hilbertschen Problems (siehe [Mat70]) und als eines der vielen Folgeresultate ergab sich auch die Unentscheidbarkeit der Nulläquivalenz von P und somit von $\mathbb{L}$. Eine Beweisskizze sowie eine Reihe ähnlich gelagerter Probleme findet man im Übersichtsartikel [BL83] von Buchberger und Loos.

Die Ursache der unterschiedlichen Einschätzung der Effektivität von $\mathbb{K}$ beruht darauf, daß die Körperelemente in verschiedenen Sprachen dargestellt wurden. Im Grunde genommen muß in beiden Fällen zu unterschiedlichen Konstantenexpansionen des Körpers $\mathbb{K}$ übergegangen werden. Damit ergibt sich die Möglichkeit der Übertragung der Berechenbarkeitsbetrachtungen der abstrakten Struktur $\mathbb{K}$ in eine Wortmenge und somit vermöge einer anschließenden Gödelisierung in die Menge der natürlichen Zahlen. Das obige Beispiel zeigt, daß die Effektivität einer abstrakten algebraischen Struktur im allgemeinen von der Wahl der Standardbeschreibung abhängen wird.

Sei A eine Menge abstrakter Objekte. Eine surjektive Abbildung $f : \mathbb{N} \to A$ heißt *Numerierung* von A und das Paar (A, f) wird als *numerierte Menge* bezeichnet. Seien Ω ein Alphabet und $b : \Omega^* \to A$ eine partielle, surjektive Abbildung mit entscheidbarem Definitionsbereich $dom(b) \subseteq \Omega^*$. Dann nennen wir b eine *Beschreibungsvorschrift* von A. Hintergrund für diese Begriffsbildung ist die Vorstellung, daß die Eingaben einer Berechnung immer durch eine endliche Beschreibung gegeben sein müssen. Bei Bedarf kann man ohne Beschränkung der Allgemeinheit die Gleichheit $dom(b) = \Omega^*$ annehmen, da jedes nicht dem Definitionsbereich angehörige Wort formal auf ein beliebig fest

gewähltes $a_0 \in A$ abgebildet werden kann. Aufgrund der Gödelisierbarkeit der Wortmenge Ω^* sind die Begriffe der Numerierung und der Beschreibungsvorschrift völlig gleichwertig. Während sich Numerierungen besser für theoretische Untersuchungen eignen, stellen Beschreibungsvorschriften einen direkten und unmittelbaren Bezug zur natürlichen Termdarstellung abstrakter algebraischer Objekte dar.

Im weiteren beschränken wir uns auf die Betrachtung unendlicher algebraischer Strukturen $\mathcal{A} = (A; G; P)$. Der einfachere, weniger interessante Fall endlicher Strukturen $\mathcal{A}$ kann analog dazu behandelt werden. Nur müssen anstelle bijektiver Numerierungen immer solche betrachtet werden, deren Einschränkung auf die Teilmenge der ersten m natürlichen Zahlen, wobei m die Mächtigkeit von A ist, bijektiv ist. Dann behalten alle nachfolgenden Aussagen sinngemäß ihre Gültigkeit.

$\mathcal{A} = (A; G; P)$ habe die Signatur $\Sigma = (F; R; \sigma)$ und $\nu : \mathbb{N} \to A$ sei eine bijektive Numerierung der Trägermenge von $\mathcal{A}$. Dann kann man auf wohlbekannte Weise eine zu $\mathcal{A}$ vermöge ν^{-1} Σ-isomorphe algebraische Struktur $\mathcal{A}^{(\nu)}$ über der Trägermenge $\mathbb{N}$ konstruieren, indem man folgendermaßen die Funktionen und Relationen für $\mathcal{A}^{(\nu)}$ einführt. Sei $f \in F$ ein Funktionssymbol und $g \in G$ die dazugehörige Operation von $\mathcal{A}$. Wir definieren die Funktion $g^{(\nu)} : \mathbb{N}^{\sigma(f)} \to \mathbb{N}$ durch

$$g^{(\nu)}\left(a_1, \ldots, a_{\sigma(f)}\right) := \nu^{-1}\left(g\left(\nu(a_1), \ldots, \nu(a_{\sigma(f)})\right)\right) \quad .$$

Weiterhin setzen wir

$$p^{(\nu)} := \left\{ \left(a_1, \ldots, a_{\sigma(\rho)}\right) \mid \left(\nu(a_1), \ldots, \nu(a_{\sigma(\rho)})\right) \in p \right\}$$

für $\rho \in R$ und dazugehöriges $p \in P$.

Definition 2.1 *Sei $\mathcal{A} = (A; g_1, \ldots, g_m; P_1, P_2, \ldots, P_k)$ eine algebraische Struktur der Signatur $\Sigma = (f_1, \ldots, f_m; \rho_1, \ldots, \rho_k; \sigma)$ und $b : \Omega^* \to A$ eine Beschreibungsvorschrift von A über dem Alphabet Ω.*

Die algebraische Struktur $\mathcal{A}$ wird eine in Bezug auf die Beschreibungsvorschrift b effektive algebraische Struktur *genannt, falls eine surjektive, berechenbare Funktion $\nu : \Omega^* \to \mathbb{N}$ und eine bijektive Numerierung $\mu : \mathbb{N} \to A$ von A existieren, so daß das Diagramm*

$$\begin{array}{ccc} A & \xleftarrow{\;b\;} & \Omega^* \\ & {\scriptstyle\mu}\nwarrow & \big\downarrow{\scriptstyle\nu} \\ & & \mathbb{N} \end{array} \tag{2.1}$$

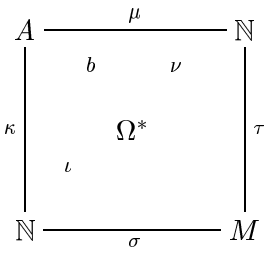
kommutativ ist und alle Operationen $g_i^{(\mu)}$, $i = 1, \ldots, m$, rekursive Funktionen und alle Relationen $P_i^{(\mu)}$, $i = 1, \ldots, k$, rekursive Mengen sind.

Lemma 2.2 *Zu einer Beschreibungsvorschrift $b : \Omega^* \to A$ einer unendlichen Menge A existieren genau dann eine surjektive, berechenbare Funktion $\nu : \Omega^* \to \mathbb{N}$ und eine bijektive Numerierung $\mu : \mathbb{N} \to A$, so daß das Diagramm (2.1) kommutativ ist, wenn die Bildgleichheit $\{(u, v) \mid b(u) = b(v)\} \subseteq \Omega^* \times \Omega^*$ unter b entscheidbar ist.*

Beweis: ($\Rightarrow$) Für beliebige Wörter u und v gilt die Äquivalenz

$$b(u) = b(v) \Longleftrightarrow \mu(\nu(u)) = \mu(\nu(v)) \Longleftrightarrow \nu(u) = \nu(v) \ .$$

Aufgrund der Berechenbarkeit der Funktion ν und der Entscheidbarkeit der Gleichheit natürlicher Zahlen ist die rechte Beziehung und folglich auch die Bildgleichheit unter b entscheidbar.
($\Leftarrow$) Zur Veranschaulichung stellen wir die nachfolgend konstruierten Abbildungen vorab in einem kommutativen Diagramm dar.



(2.2)

Sei $\iota : \Omega^* \to \mathbb{N}$ eine beliebige bijektive Gödelisierung. ι induziert eine Numerierung $\kappa = \iota^{-1} \circ b$ von A. Für alle natürlichen Zahlen n und m gilt die Beziehung

$$\kappa(n) = \kappa(m) \Longleftrightarrow b(\iota^{-1}(n)) = b(\iota^{-1}(m)) \ .$$

Aufrund der Berechenbarkeit von ι^{-1} und der Entscheidbarkeit der Bildgleichheit unter b ist auch die Bildgleichheit unter κ entscheidbar.

Wir setzen

$$M = \{i \in \mathbb{N} \mid \forall j \in \mathbb{N} : j < i \longrightarrow \kappa(i) \neq \kappa(j)\} \ .$$

Die Entscheidbarkeit der Bildgleichheit unter κ sichert die Entscheidbarkeit der Teilmenge $M \subseteq \mathbb{N}$. Die Funktion $\sigma : \mathbb{N} \to M$, die jedem $i \in \mathbb{N}$ das eindeutig bestimmte Element $j \in M$ mit $\kappa(i) = \kappa(j)$ zuweist, ist berechenbar und surjektiv. Die Einschränkung $\sigma|_M$ ist die identische Abbildung auf M. Da M eine unendliche, entscheidbare Menge ist, existiert eine bijektive, berechenbare Abbildung $\tau : M \to N$, deren inverse Abbildung τ^{-1} ebenfalls berechenbar ist.

Die Abbildung $\nu = \iota \circ \sigma \circ \tau$ ist berechenbar und surjektiv. Wegen $\kappa(M) = A$ ist die durch $\mu(n) = \kappa(\tau^{-1}(n))$ definierte Abbildung $\mu : \mathbb{N} \to A$ surjektiv. Außerdem ist sie auch injektiv, denn die Bilder der Elemente aus M unter der Abbildung κ sind paarweise verschieden. Somit ist μ eine bijektive Numerierung von A. Durch Nachrechnen überzeugt man sich von der Kommutativität des in Diagramm (2.2) enthaltenen Teildiagramms der Gestalt (2.1). □

Lemma 2.2 rechtfertigt es, eine unendliche Menge A abstrakter Objekte in Bezug auf eine Beschreibungsvorschrift $b : \Omega^* \to A$ mit entscheidbarer Bildgleichheit *gödelisierbar* zu nennen. Sind $\nu : \Omega^* \to \mathbb{N}$ eine surjektive, berechenbare Funktion und $\mu : \mathbb{N} \to A$ eine bijektive Numerierung von A mit der Eigenschaft, $\nu \circ \mu = b$, dann nennen wir μ^{-1} eine *Gödelisierung* von A bezüglich b. Diese Begriffsbildungen erfolgen in Anlehnung an den in Abschnitt 2.1.1 eingeführten Begriff der Gödelisierung einer Wortmenge.

Unter einer *Übersetzung* einer Beschreibungsvorschrift $d : \Gamma^* \to A$ in eine zweite Beschreibungsvorschrift $b : \Omega^* \to A$ verstehen wir eine berechenbare Abbildung $\tau : \Gamma^* \to \Omega^*$ mit der Eigenschaft $d = \tau \circ b$. Man überzeugt sich leicht von der Gültigkeit des folgenden Lemmas.

Lemma 2.3 *Falls A in Bezug auf b gödelisierbar ist und eine Übersetzung von d nach b existiert, dann ist A auch in Bezug auf d gödelisierbar.*

Falls $\mathcal{A}$ eine effektive algebraische Struktur bezüglich b ist und eine Übersetzung von d nach b existiert, dann ist $\mathcal{A}$ auch in Bezug auf d eine effektive algebraische Struktur.

Wenn wir in Zukunft einfach von einer gödelisierbaren Menge A abstrakter Objekte sprechen werden, so beziehen wir uns dabei immer auf eine, meist nur implizit gegebene, a priori Standardbeschreibungsvorschrift der Elemente von A durch Terme über einem geeigneten Alphabet Ω. So ist beispielsweise der Körper $\mathbb{Q}(X_1, \ldots, X_n)[Y]/p(Y)$ aus dem Einführungsbeispiel gödelisierbar, während $\mathbb{Q}(x_1, \ldots, x_r)$ im allgemeinen nicht gödelisierbar zu sein braucht.

Im weiteren beschäftigen wir uns mit dem Problem, eine algebraische Struktur $\mathcal{A}$ durch eine logische Theorie $\mathfrak{F}$ zu beschreiben. Wir untersuchen den Zusammenhang zwischen der Effektivität von $\mathcal{A}$ und Eigenschaften von $\mathfrak{F}$. Dabei verlangen wir, daß die effektive algebraische Struktur $\mathcal{A}$ bis auf berechenbare Isomorphie eindeutig durch $\mathfrak{F}$ beschrieben werden soll. Gemäß Lemma 2.2 erfordert die Effektivität einer algebraischen Struktur $\mathcal{A}$ in jedem Falle die Entscheidbarkeit der identischen Gleichheitsrelation $\equiv_A = \{(a, a) \mid a \in A\}$ über ihrer Trägermenge A. Das trifft insbesondere auch dann zu, wenn die identische Gleichheit nicht bereits eine Relation der Struktur $\mathcal{A}$ ist. Von jetzt an werden wir annehmen, daß die Signatur Σ das zweistellige Prädikatensymbol $=$ enthält und daß dieses in allen untersuchten Σ-Strukturen als die identische Gleichheit über der Trägermenge interpretiert wird. Unsere logischen Untersuchungen werden daher im Prädikatenkalkül mit Identität angesiedelt sein.

Satz 2.4 *Sei $\mathcal{A} = (A; g_1, \ldots, g_m; \equiv_A, P_2, \ldots, P_k)$ eine (unendliche) algebraische Struktur der Signatur $\Sigma = (f_1, \ldots, f_m; =, \rho_2, \ldots, \rho_k; \sigma)$ und Σ_C bezeichne die Konstantenerweiterung von Σ, die sich durch Hinzunahme der Konstantensymbole $c_0, c_1, \ldots$ ergibt. $\mathcal{A}_C$ sei eine Σ_C-Expansion von $\mathcal{A}$, bei der jedes Element von A Interpretation wenigstens einer Konstante c_i ist. Dann ist $\mathcal{A}$ genau dann eine effektive algebraische Struktur (bezüglich der durch Σ_C und der Interpretation der Konstanten $c_0, c_1, \ldots$ aufgeprägten Beschreibungsvorschrift), wenn die Menge der in der Konstantenexpansion $\mathcal{A}_C$ gültigen variablenfreien Atomformeln entscheidbar ist.*

Beweis: Sei $\hat{b} : \mathcal{T}_{\Sigma_C}(\emptyset) \to \mathcal{A}$ der Σ_C-Homomorphismus, welcher die Interpretation der Konstantensymbole $c_0, c_1, \ldots$ fortsetzt. Da jedes Element von A Interpretation einer Konstanten c_i ist, ist $\hat{b}$ surjektiv und somit ist die durch $b \mid_{T(\Sigma_C, \emptyset)} = \hat{b}$ und $\forall w \notin T(\Sigma_C, \emptyset) : b(w) = \hat{b}(c_0)$ definierte Funktion $b : \Sigma_C^* \to A$ eine Beschreibungsvorschrift von A. Im folgenden legen wir b als Standardbeschreibungsvorschrift zugrunde.

($\Rightarrow$) Sei $\mathcal{A}$ eine effektive algebraische Struktur in Bezug auf b. Nach Definition induziert b eine bijektive Numerierung $\mu : \mathbb{N} \to A$ von A, wobei $\nu = b \circ \mu^{-1}$ eine surjektive, berechenbare Funktion von Σ_C^* auf $\mathbb{N}$ ist und alle Operationen und Prädikate von $\mathcal{A}^{(\mu)}$ berechenbar beziehungsweise entscheidbar sind.

Seien ρ ein n-stelliges Prädikatensymbol von Σ und $t_1, \ldots, t_n \in T(\Sigma_C, \emptyset)$ variablenfreie Terme der Signaturerweiterung Σ_C. Es gilt

$$\mathcal{A}_C \models \rho(t_1, \ldots, t_n) \Longleftrightarrow (b(t_1), \ldots, b(t_n)) \in p \Longleftrightarrow (\nu(t_1), \ldots, \nu(t_n)) \in p^{(\mu)},$$

wobei p die Interpretation von ρ in $\mathcal{A}$ bezeichnet. Aufgrund der Entscheidbarkeit von $p^{(\mu)}$ und der Berechenbarkeit von ν ist die rechte Seite entscheidbar und es folgt die behauptete Entscheidbarkeit der Menge der in $\mathcal{A}_C$ gültigen variablenfreien Atomformeln.

($\Leftarrow$) Sei die Menge der in $\mathcal{A}_C$ gültigen variablenfreien Atomformeln entscheidbar. Wegen

$$\mathcal{A}_C \models t = s \Longleftrightarrow b(t) \equiv_A b(s)$$

für alle $t, s \in T(\Sigma_C, \emptyset)$ hat das die Entscheidbarkeit der Bildgleichheit unter b zur Folge. Nach Lemma 2.2 existieren somit eine berechenbare, surjektive Funktion $\nu : \Sigma_C^* \to \mathbb{N}$ und eine bijektive Numerierung $\mu : \mathbb{N} \to A$ mit der Eigenschaft $\nu \circ \mu = b$.

Seien ρ ein n-stelliges Prädikatensymbol von Σ und p seine Interpretation in $\mathcal{A}$. Dann gilt für alle natürliche Zahlen $i_1, \ldots, i_n$ die Beziehung

$$(i_1, \ldots, i_n) \in p^{(\mu)} \Longleftrightarrow (\mu(i_1), \ldots, \mu(i_n)) \in p \Longleftrightarrow \mathcal{A}_C \models \rho(c_{j_1}, \ldots, c_{j_n}) \,,$$

wobei $j_k, \quad k = 1, \ldots, n$, die kleinste natürliche Zahl mit $\nu(c_{j_k}) = i_k$ ist. Aufgrund der Berechenbarkeit von ν können die j_k auf algorithmischem Wege bestimmt werden. Nach Voraussetzung ist die rechte Seite entscheidbar, also sind alle Prädikate von $\mathcal{A}_C^{(\mu)}$ entscheidbar.

Seien g eine n-stellige Operation von $\mathcal{A}$, f das zu ihr gehörige Symbol der Signatur Σ und $i_1, \ldots, i_n$ beliebige natürliche Zahlen. Dann gilt

$$g^{(\mu)}(i_1, \ldots, i_n) \equiv_A i \Longleftrightarrow \mathcal{A}_C \models f(c_{j_1}, \ldots, c_{j_n}) = c_j \,,$$

wobei die j und $j_k, \; k = 1, \ldots, n$, analog zu oben als die kleinsten natürlichen Zahlen mit $\nu(c_j) = i$ beziehungsweise $\nu(c_{j_k}) = i_k$ erklärt sind. Die $c_{j_1}, \ldots, c_{j_n}$ sind algorithmisch auffindbar und sukzessives Testen der Gültigkeit von

$$\begin{aligned}
\mathcal{A}_C &\models f(c_{j_1}, \ldots, c_{j_n}) = c_0 \,, \\
\mathcal{A}_C &\models f(c_{j_1}, \ldots, c_{j_n}) = c_1 \,, \\
&\vdots \\
\mathcal{A}_C &\models f(c_{j_1}, \ldots, c_{j_n}) = c_j
\end{aligned}$$

liefert nach endlicher Zeit die kleinste natürliche Zahl j, für welche die Folgerungsbeziehung zutrifft. Die Existenz eines derartigen j folgt aus der Totalität von f und der Tatsache, daß jedes Element von A Interpretation einer der Konstanten $c_0, c_1, \ldots$ ist. Die Berechnung von $i = \nu(c_j)$ schließt die Konstruktion

des Funktionswertes $g^{(\mu)}(i_1, \ldots, i_n)$ ab. Damit ist die Effektivität von $\mathcal{A}$ in Bezug auf b nachgewiesen. □

Satz 2.4 zeigt, daß wir die Effektivität einer algebraischen Struktur auf die Entscheidbarkeit einer elementaren Theorie zurückführen können und wir werden deshalb auch gelegentlich von einem *effektiven Modell* sprechen. Unsere Betrachtungen lehnen sich an Ershovs Untersuchungen zu *konstruktiven Modellen* und *konstruktiven Algebren* an (siehe [Er80]). Der hier gewählte Aufbau weicht jedoch an einigen Stellen von dem Ershovschen ab.

Wenden wir uns nun der Frage zu, auf welche Art und Weise eine effektive algebraische Struktur $\mathcal{A}$ effektiv durch eine Theorie $\mathfrak{F}$ beschrieben werden kann. Dabei lassen wir den trivialen Fall endlicher Strukturen wiederum außer acht und setzen im folgenden die Unendlichkeit der Trägermenge von $\mathcal{A}$ voraus. Um von einer effektiven Beschreibung von $\mathcal{A}$ sprechen zu können, ist es notwendig, daß $\mathfrak{F}$ axiomatisierbar ist und $\mathcal{A}$ durch $\mathfrak{F}$ bis auf Isomorphie eindeutig bestimmt wird. Dabei darf die Klasse der zulässigen Modelle gegebenfalls eingeschränkt werden. Anhand einer Reihe klassischer Resultate (siehe z.B. [Bet59] oder [Sh67]) wollen wir zunächst einige mögliche Bedingungen an $\mathfrak{F}$ und Einschränkungen der Klasse zulässiger Modelle untersuchen. Nach dem Satz von Löwenheim und Skolem besitzt jede elementare Theorie mit einem unendlichen Modell auch Modelle von beliebiger höherer Mächtigkeit. Folglich ist keine elementare Theorie mit unendlichem Modell $\mathcal{A}$, insbesondere auch nicht die vollständige Theorie $\mathfrak{F} = \mathfrak{Th}(\mathcal{A})$, kategorisch. Wir wissen aber, daß eine effektive, unendliche Struktur $\mathcal{A}$ nur abzählbar unendlich sein kann und können daher unser Interesse auf Modelle der Mächtigkeit ω der natürlichen Zahlen beschränken. Damit wird $\mathcal{A}$ durch Angabe einer den drei Bedingungen

i) $\mathcal{A}$ ist Modell von $\mathfrak{F}$

ii) $\mathfrak{F}$ hat keine endlichen Modelle

iii) $\mathfrak{F}$ ist ω-kategorisch, das heißt alle Modelle der Mächtigkeit ω von $\mathfrak{F}$ sind untereinander isomorph

genügenden Theorie $\mathfrak{F}$ bis auf Isomorphie eindeutig bestimmt. Nach dem Satz von Łoś und Vaught ist jede die Bedingungen *i), ii)* und *iii)* erfüllende Theorie vollständig. Der Gödelsche Unvollständigkeitssatz besagt, daß es keine vollständige, axiomatisierbare Erweiterung der Theorie der natürlichen Zahlen gibt. Somit existiert bereits für einfachste effektive Algebren keine effektive ω-kategorische Theorie. Eine andere Möglichkeit, $\mathcal{A}$ bis auf Isomorphie eindeutig zu charakterisieren, besteht in der Verwendung nichtelementarer Formeln des Prädikatenkalküls höherer Stufe. Legt man Henkins allgemeinen Modellbegriff zugrunde, so sind die vollständigen Theorien unendlicher algebraischer Strukturen nach wie vor nicht kategorisch und erst die Beschränkung auf Standardmodelle liefert einen zufriedenstellenden Kategorizitätsbegriff. Dabei geht zum einen die Vollständigkeit des Kalküls verloren, zum anderen besitzt die Kategorizität nur einen relativen Charakter bezüglich des gewählten Modells der Mengenlehre. Letztendlich wollen wir uns dafür entscheiden, nur elementare Theorien $\mathfrak{F}$ zuzulassen und eine sehr schwache Kategorizität zu erzwingen, indem wir uns auf die Betrachtung kanonischer Modelle beschränken.

Definition 2.5 *Sei $\mathcal{A}$ eine bezüglich einer beliebigen Beschreibungsvorschrift b effektive algebraische Struktur der Signatur Σ und $\mathfrak{F} \subset \mathfrak{Fm}(\Sigma)$ eine konsistente, axiomatisierbare, kanonische Theorie des Prädikatenkalküls erster Stufe mit Identität. Falls alle kanonischen Modelle von $\mathfrak{F}$ isomorph zu $\mathcal{A}$ sind, so nennen wir $\mathfrak{F}$ eine* effektive Theorie von $\mathcal{A}$.

Satz 2.6 *Sei $\mathcal{A}$ eine (in Bezug auf eine beliebige Beschreibungsvorschrift b) effektive algebraische Struktur der Signatur Σ. Dann existiert eine effektive Theorie $\mathfrak{F}$ einer geeigneten Konstantenexpansion $\mathcal{A}_C$ von $\mathcal{A}$.*

Beweis: Die Effektivität von $\mathcal{A}$ hat die Existenz einer bijektiven Numerierung $\mu : \mathbb{N} \to A$, deren inverse Abbildung μ^{-1} eine Gödelisierung von A (bezüglich b) ist und für die alle Operationen und Prädikate von $\mathcal{A}^{(\mu)}$ berechenbar beziehungsweise entscheidbar sind, zur Folge.

Die Konstruktion der zu $\mathcal{A}^{(\mu)}$ gehörigen Operationen und Relationen bewirkt, daß μ sogar ein Σ-Isomorphismus zwischen $\mathcal{A}^{(\mu)}$ und A wird. Folglich gilt insbesondere $\mathfrak{Th}(\mathcal{A}^{(\mu)}) = \mathfrak{Th}(\mathcal{A})$.

Sei $d : \Omega^* \to \mathcal{A}^{(\mu)}$ eine beliebige berechenbare Beschreibungsvorschrift der algebraischen Struktur $\mathcal{A}^{(\mu)}$ über einem beliebigen Alphabet Ω. Man beachte, an dieser Stelle ist es möglich, die Berechenbarkeit der Beschreibungsvorschrift d zu fordern, da die Trägermenge von $\mathcal{A}^{(\mu)}$ nicht einfach aus abstrakten Objekten besteht, sondern gleich der Menge $\mathbb{N}$ der natürlichen Zahlen ist. Dann ist $\mathcal{A}^{(\mu)}$ offensichtlich effektiv bezüglich d, ein geeignetes kommutatives Diagramm der Gestalt (2.1) ist

$$\begin{array}{ccc} \mathcal{A}^{(\mu)} & \xrightarrow{\ d\ } & \Omega^* \\ & {\scriptstyle id}\searrow & \big\downarrow {\scriptstyle d} \\ & & \mathbb{N} \end{array}$$

Σ_C bezeichne die Signaturerweiterung von Σ, die sich durch Hinzunahme neuer Konstantensymbole $c_0, c_1, \ldots$ ergibt. $\mathcal{A}_C$ sei die Σ_C-Konstantenexpansion von $\mathcal{A}$, bei der jedes c_i, $i = 0, 1, \ldots$, durch $\mu(i)$ interpretiert wird.

Außerdem sei $\mathcal{A}_C^{(\mu)}$ die Σ_C-Konstantenexpansion von $\mathcal{A}^{(\mu)}$, bei welcher c_i für jedes $i \in \mathbb{N}$ durch i interpretiert wird. Nach Satz 2.4 ist die Menge $\mathfrak{F}_1$ der in $\mathcal{A}_C^{(\mu)}$ (und somit in $\mathcal{A}_C$) gültigen variablenfreien Formeln entscheidbar. Damit ist auch die Komplementmenge $\mathfrak{F}_2$ aller nicht in $\mathcal{A}_C^{(\mu)}$ (und somit nicht in $\mathcal{A}_C$) gültigen variablenfreien Atomformeln entscheidbar. Sei $\tilde{\mathfrak{F}}_2 = \{\neg F \mid F \in \mathfrak{F}_2\}$. Die Menge $\mathfrak{F} = \mathfrak{F}_1 \cup \tilde{\mathfrak{F}}_2$, das sogenannte *Diagramm* von $\mathcal{A}_C$, ist eine offene, axiomatisierbare Theorie der Signatur Σ_C. Offensichtlich ist $\mathcal{A}_C$ ein kanonisches Modell von $\mathfrak{F}$ und sämtliche kanonischen Modelle eines Diagramms sind zueinander isomorph. □

Neben der trivialen Wahl des Diagramms einer Konstantenexpansion $\mathcal{A}_C$, bei welcher jedes Element von $\mathcal{A}$ Interpretation mindestens einer Konstanten c_i ist, gibt es häufig noch weitere Möglichkeiten, effektive Theorien von Konstantenexpansionen einer effektiven algebraischen Struktur zu finden. Sei $K \subseteq A$ die Menge aller Interpretationen von Konstantensymbolen von Σ und $E \subseteq A$ ein Erzeugendensystem von $\mathcal{A}$. Dann reicht es bereits aus, die Signatur Σ um $\{c_e \mid e \in E \backslash K\}$ zu einer Signatur Σ_E zu erweitern.

Satz 2.7 *Seien $\mathcal{A}$ eine algebraische Struktur der Signatur Σ und $\mathcal{A}_E$ eine Konstantenexpansion von $\mathcal{A}$ zu einer um eine Menge E von Konstantensymbolen erweiterten Signatur Σ_E. Die Interpretationsabbildung $\hat{b} : T(\Sigma_E, \emptyset) \to A$ von $\mathcal{A}_E$ sei surjektiv. Dann ist $\mathcal{A}$ genau dann eine effektive algebraische Struktur bezüglich einer Beschreibungsvorschrift $b : \Sigma_E^* \to A$ mit $b \mid_{T(\Sigma_E,\emptyset)} = \hat{b}$, wenn die Menge der in $\mathcal{A}_E$ gültigen variablenfreien Atomformeln entscheidbar ist.*

Beweis: ($\Longrightarrow$) trivial.

($\Longleftarrow$) Da $\hat{b}$ surjektiv ist, läßt sich die Definition von b zum Beispiel durch $\forall w \notin T(\Sigma_E, \emptyset) \; : \; b(w) = \hat{b}(e_0)$ für ein beliebig fest gewähltes $e_0 \in E$ zu einer Beschreibungsvorschrift von $\mathcal{A}_E$ vervollständigen. Wenn die Menge der in $\mathcal{A}_E$ gültigen variablenfreien Atomformeln entscheidbar ist, so ist wegen

$$\hat{b}(t) = \hat{b}(s) \Longleftrightarrow \mathcal{A}_E \models t = s$$

für alle $s, t \in T(\Sigma_E, \emptyset)$ insbesondere auch die Bildgleichheit unter $\hat{b}$ und somit unter b entscheidbar. Aus Lemma 2.2 folgt die Existenz einer Gödelisierung $\nu : A \to \mathbb{N}$ der Trägermenge A von $\mathcal{A}_E$ bezüglich b. Die Eigenschaften einer Gödelisierung sichern die Existenz einer berechenbaren Funktion $\tau : \mathbb{N} \to T(\Sigma_E, \emptyset)$ mit $b(\tau(i)) = \nu^{-1}(i)$.

Wir erweitern Σ um Konstantensymbole $c_0, c_1, \ldots$ zur Signatur Σ_C und bezeichnen die Konstantenexpansion von $\mathcal{A}$, in welcher c_i für jedes $i \in \mathbb{N}$ durch $\nu^{-1}(i)$ interpretiert wird, mit $\mathcal{A}_C$. Für jeden Term $t \in T(\Sigma_C, \emptyset)$ bezeichne $\tilde{t}$ den Term aus $T(\Sigma_E, \emptyset)$, den man erhält, wenn man alle Vorkommen von Konstantensymbolen c_i durch die entsprechenden Terme $\tau(i)$ ersetzt. Dann gilt für jede variablenfreie Atomformel $\rho t_1 \cdots t_n$ der Signatur Σ_C die Äquivalenz

$$\mathcal{A}_C \models \rho t_1 \cdots t_n \Longleftrightarrow \mathcal{A}_E \models \rho \tilde{t}_1 \cdots \tilde{t}_n$$

und die vorausgesetzte Entscheidbarkeit der rechten Seite zieht die Entscheidbarkeit der linken Seite nach sich. Aus Satz 2.4 folgt schließlich die Behauptung. □

Satz 2.8 *Seien $\mathcal{A}$ eine effektive algebraische Struktur bezüglich der Beschreibungsvorschrift $b : \Omega^* \to A$ und $\equiv \subseteq A \times A$ eine Kongruenzrelation von $\mathcal{A}$. Falls der natürliche Homomorphismus $\iota : \mathcal{A} \to \mathcal{A}/\equiv$ stark ist, so ist die aus den Restklassen $[a]_\equiv$, $a \in A$, bestehende Faktoralgebra $\mathcal{A}/\equiv$ genau dann bezüglich der durch $\bar{b}(w) = [b(w)]_\equiv$ definierten Beschreibungsvorschrift $\bar{b} : \Omega^* \to A/\equiv$ effektiv, wenn die Expansion $(\mathcal{A}; \equiv)$ der Algebra $\mathcal{A}$ bezüglich b effektiv ist.*

Beweis: ($\Longrightarrow$) Sei $\mathcal{A}/\equiv$ bezüglich $\bar{b}$ effektiv. Wir betrachten das folgende kommutative Diagramm:

$$\begin{array}{ccccc} A/\equiv & \xleftarrow{\;\iota\;} & A & \xrightarrow{\;b\;} & \Omega^* \\ & & \mu \big\downarrow & \nearrow_{\nu} & \\ & & \mathbb{N} & & \end{array} \tag{2.3}$$

Dabei sind $\nu : \Omega^* \to A$ eine surjektive, berechenbare Funktion und $\mu : \mathbb{N} \to A$ eine bijektive Numerierung, für welche alle Operationen und Relationen von $\mathcal{A}^{(\mu)}$ berechenbar beziehungsweise entscheidbar sind. $\iota : A \to A/\equiv$ bezeichnet den kanonischen Homomorphismus von A in die Faktorstruktur $A/\equiv$ und somit gilt $\bar{b} = b \circ \iota$.

Für beliebige natürliche Zahlen i und j lassen sich auf algorithmischem Wege Wörter $u, v \in \Omega^*$ mit $\nu(u) = i$ und $\nu(v) = j$ berechnen. Aufgrund der Äquivalenz

$$i \equiv^{(\mu)} j \iff \iota(\mu(i)) = \iota(\mu(j)) \iff \iota(b(u)) = \iota(b(v)) \iff \bar{b}(u) = \bar{b}(v)$$

und der aus der Effektivität von $\mathcal{A}/\equiv$ bezüglich $\bar{b}$ folgenden Entscheidbarkeit der Bildgleichheit unter $\bar{b}$ ist auch die Relation $\equiv^{(\mu)}$ entscheidbar. Damit ist die Effektivität der Expansion $(\mathcal{A}, \equiv)^{(\mu)}$ von $\mathcal{A}^{(\mu)}$ nachgewiesen.

($\Longleftarrow$) Sei $(\mathcal{A}; \equiv)$ effektiv. Wir betrachten das folgende kommutative Diagramm:

$$\begin{array}{ccccc} & & A/\equiv & \xrightarrow{\ \iota\ } & A \\ & \tilde{\mu} & \Big| & & \Big| \; b \\ \mathbb{N} & & \hat{\mu} \Big| & & \Big| \mu \quad \Omega^* \\ & \tau & \Big| & & \Big| \; \nu \\ & & M & \xrightarrow[\ \hat{\iota}\ ]{} & \mathbb{N} \end{array} \tag{2.4}$$

ν, μ und ι haben die gleichen Eigenschaft wie im Beweis der ersten Richtung. Zusätzlich ist auch die Relation $\equiv^{(\mu)}$ von $(\mathcal{A}, \equiv)^{(\mu)}$ entscheidbar. Dann ist auch die durch

$$\hat{\iota}(i) = \min(j \mid i \equiv^{(\mu)} j)$$

definierte Abbildung $\hat{\iota} : \mathbb{N} \to \mathbb{N}$ berechenbar. Der Bildbereich $M = im(\hat{\iota})$ kann vermöge $\hat{\iota}(i) \mapsto [i]_{\equiv^{(\mu)}}$ mit $\mathcal{A}^{(\mu)}/\equiv^{(\mu)}$ identifiziert werden. Unter dieser Identifikation wird $\hat{\iota}$ natürlicher Homomorphismus von $\mathcal{A}^{(\mu)}$ nach $\mathcal{A}^{(\mu)}/\equiv^{(\mu)}$. Die Berechenbarkeit beziehungsweise Entscheidbarkeit der Operationen und Relationen von $\mathcal{A}^{(\mu)}$ überträgt sich über den berechenbaren starken Homomorphismus auf $\mathcal{A}^{(\mu)}/\equiv^{(\mu)}$.

Im weiteren setzen wir die Unendlichkeit von M voraus. Der Beweis läßt sich geradlinig auf den endlichen Fall übertragen. Die Menge M ist entscheidbar, daher existiert eine bijektive, berechenbare Funktion $\tau : M \to \mathbb{N}$. Bei entsprechender Definition der Operationen und Relationen auf dem Bildbereich $\mathbb{N}$ wird τ Isomorphismus. Die Berechenbarkeit beziehungsweise Entscheidbarkeit der Operationen und Relationen bleibt unter τ erhalten.

Nach Konstruktion ist μ ein Isomorphismus zwischen $\mathcal{A}^{(\mu)}$ und $\mathcal{A}$. Die das Diagramm kommutativ ergänzenden Funktion $\hat{\mu}$ und $\tilde{\mu}$ sind ebenfalls Isomorphismen. Schließlich ist die Funktion $\hat{\nu} = \nu \circ \hat{\iota} \circ \tau$ berechenbar und surjektiv. Damit weist das Diagramm

$$\begin{array}{ccc} A/\equiv & \xrightarrow{\ \bar{b}\ } & \Omega^* \\ & \tilde{\mu} & \Big| \; \hat{\nu} \\ & & \mathbb{N} \end{array} \tag{2.5}$$

alle Eigenschaften eines Diagramms (2.1) auf und die Effektivität von $\mathcal{A}/\equiv$ bezüglich $\bar{b}$ ist gezeigt. □

Zusammenfassend bietet sich folgendes Vorgehen bei der Untersuchung einer algebraischen Struktur auf Effektivität an. Zuerst suche man ein algebraisches Erzeugendensystem der Struktur, man führe für jedes erzeugende Element ein Konstantensymbol ein und gehe zu einer entsprechenden Erweiterungssignatur über. Nach Satz 2.7 sind im folgenden keine weiteren Strukturerweiterungen mehr erforderlich. In zahlreichen interessanten Fällen der klassischen Algebra erweisen sich bereits endliche Mengen von Konstantensymbolen als ausreichend. Weiterhin sind die algebraischen Strukturen oftmals direkt als ein gewisses algebraisches Erzeugnis gegeben, damit sind die notwendigen Konstanten bereits a-priori bekannt. Eine andere Art, eine algebraische Struktur zu definieren, besteht in der Festlegung, daß es sich um eine kleinste gegen eine gewisse Bedingung abgeschlossene Oberstruktur handeln soll. Die Bedingung postuliert die Existenz von Elementen mit gewissen Eigenschaften und das Erzeugnis der Menge dieser Elemente zusammen mit den Erzeugenden der Grundstruktur liefert ein Erzeugendensystem des in Frage stehenden Abschlusses. Im allgemeinen handelt es sich hierbei um ein nicht minimales, unendliches Erzeugendensystem, trotzdem ist es oftmals wenigstens nicht sofort die gesamte Trägermenge des Abschlusses. Gegebenenfalls kann das Erzeugendensystem weiter verkürzt werden.

Gemäß Satz 2.8 kann man durch die Untersuchung einer einzigen algebraischen Struktur auf Effektivität und Beantwortung der Frage nach der Entscheidbarkeit der Kerne ihrer starken Homomorphismen die Effektivität einer ganzen Klasse algebraischer Strukturen, nämlich aller starken homomorphen Bilder der Ausgangsalgebra, behandeln. Rückschlüsse auf die homomorphen Bilder sind allerdings nur dann möglich, wenn die Ausgangsstruktur effektiv ist. Nach Auffindung eines möglichst kleinen Erzeugendensystems des untersuchten algebraischen Systems $\mathcal{A}$, ist es sinnvoll, nach einem effektiven, algebraischen System $\mathcal{B}$ zu fragen, welches $\mathcal{A}$ als homomorphes Bild bezüglich eines starken Homomorphismus hat. Außerdem wird verlangt, daß sich die Standardbeschreibungsvorschrift von $\mathcal{A}$ in eine Beschreibungsvorschrift durch Repräsentanten aus $\mathcal{B}$ übersetzen läßt. Gibt es solch ein $\mathcal{B}$, so sind die weiteren Effektivitätsuntersuchungen zur Frage nach der Entscheidbarkeit des Kerns des Homomorphismus äquivalent. So kann man beispielsweise im Falle abstrakter Algebren $\mathcal{A}$ immer die absolut freie Algebra der entsprechenden Signatur als $\mathcal{B}$ wählen. Findet man ein geeignetes $\mathcal{B}$, für welches jede starke Kongruenzrelation entscheidbar ist, so ist man natürlich fertig. Muß aber die Entscheidbarkeit der betreffenden starken Kongruenzrelation im Einzelfall nachgewiesen werden, so stellt sich die Frage, ob es vielleicht eine algebraische Struktur $\mathcal{C}$ gibt, die homomorphes Bild von $\mathcal{B}$ ist und die $\mathcal{A}$ als homomorphes Bild hat. Dann ist es günstiger, mit $\mathcal{C}$ anstelle von $\mathcal{B}$ weiterzuarbeiten. In der Richtung dieses Vorgehens liegt auch die Methode, den Homomorphismus in Teilabbildungen zu zerlegen und jede davon einzeln zu untersuchen.

Für den Rest dieser Arbeit vereinbaren wir die Ausdehnung des für Funktionen über den natürlichen Zahlen eingeführten Berechenbarkeitsbegriffs auf

beliebige Strukturen $\mathcal{A}$ abstrakter Objekte. Die Aussagen sind dann immer relativ zu einer a priori gegebenen Standardbeschreibungsvorschrift $b : \Omega^* \to A$ zu verstehen. Insbesondere erfordert die Berechenbarkeit einer beliebigen Funktion über der Struktur $\mathcal{A}$ immer die Existenz einer Gödelisierung der Trägermenge A bezüglich der Beschreibungsvorschrift b.

2.3 Algebraische Simplifikation

$\mathcal{A}$ sei eine algebraische Struktur und R eine Kongruenzrelation auf $\mathcal{A}$. Weiterhin seien $\prec$ eine Halbordnung über der Trägermenge A von $\mathcal{A}$ und $S : A \to A$ eine totale, berechenbare Funktion mit den Eigenschaften: $(S(a), a) \in R$ und $S(a) \preceq a$ für alle $a \in A$. Dann wird S ein *algebraischer Simplifikator* der Faktorstruktur $\mathcal{A}/\mathcal{R}$ bezüglich $\prec$ genannt. Einen der Beziehung $S(a) = S(b) \iff (a, b) \in R$ genügenden Simplifikator S nennen wir *kanonisch*.

Besitzt $\mathcal{A}$ eine binäre Operation $\circ$, so daß $(A, \circ)$ eine Gruppe ist, dann wird ein Simplifikator S mit $S(a) = e \iff (a, e) \in R$, wobei $e \in A$ das bezüglich $\circ$ neutrale Element ist, ein bezüglich $\circ$ *normaler Simplifikator* genannt. Im Falle einer additiv geschriebenen Gruppe, d.h. $\circ = +$ und $e = 0$, sprechen wir auch von einem *Nullsimplifikator*.

Für eine beliebige totale, berechenbare Funktion $T : A \to A$ mit $T(a) = T(b) \iff (a, b) \in R$ definiert $a \prec_T b :\iff a = T(b)$ eine Halbordnung auf der Trägermenge A und T ist ein kanonischer Simplifikator von $\mathcal{A}/\mathcal{R}$ bezüglich $\prec_T$. Da jede Simplifikationshalbordnung $\prec$, für welche T ein Simplifikator von $\mathcal{A}/\mathcal{R}$ bezüglich $\prec$ ist, die Halbordnung $\prec_T$ verfeinert, werden wir bei der Behandlung kanonischer Simplifikatoren oftmals auf die Angabe der Simplifikationshalbordnung verzichten.

Der folgende Satz spiegelt einen wesentlichen Zusammenhang zwischen Entscheidbarkeit und algebraischer Simplifikation wider. In Verbindung mit Satz 2.8 reduziert er den Effektivitätsnachweis einer Faktorstruktur einer effektiven Struktur auf das Auffinden eines kanonischen oder normalen Simplifikators.

Satz 2.9 ([BCL83]) *$\mathcal{A}$ sei eine effektive algebraische Struktur und $+$ eine zu $\mathcal{A}$ gehörige binäre Operation, so daß $(A, +)$ eine Gruppe bildet. Wie üblich bezeichne 0 das neutrale Element der Gruppe. Weiterhin sei $R \subseteq A \times A$ eine Kongruenzrelation von $\mathcal{A}$. Dann sind die folgenden Aussagen äquivalent:*

i) Die Relation R ist eine entscheidbare Menge.

ii) Es existiert ein kanonischer Simplifikator der Restklassenstruktur $\mathcal{A}/\mathcal{R}$.

iii) Es existieren eine Halbordnung $\prec$ und eine Funktion $Z : A \to A$, so daß Z ein Nullsimplifikator der Restklassenstruktur $\mathcal{A}/\mathcal{R}$ bezüglich $\prec$ ist.

Beweis:
i) $\Rightarrow$ ii) Sei $\nu : A \to \mathbb{N}$ eine Gödelisierung der Trägermenge A. Aufgrund der Entscheidbarkeit von R ist die durch $I(a) = \min\{i \in \mathbb{N} \mid (a, \nu^{-1}(i)) \in R\}$ definierte Funktion berechenbar und $S(a) = \nu^{-1}(I(a))$ beschreibt einen kanonischen Simplifikator für $\mathcal{A}/\mathcal{R}$.

ii) $\Rightarrow$ *iii)* Seien S ein kanonischer Simplifikator für $\mathcal{A}/\mathcal{R}$ und $\prec$ eine beliebige Halbordnung von A mit 0 als kleinstem Element. Dann beschreibt

$$Z(a) = \begin{cases} 0 & : \quad \text{falls } S(a) = S(0) \\ a & : \quad \text{sonst} \end{cases}$$

einen Nullsimplifikator von $\mathcal{A}/\mathcal{R}$ bezüglich $\prec$.

iii) $\Rightarrow$ *i)* Sei Z ein Nullsimplifikator von $\mathcal{A}/\mathcal{R}$. Für beliebige $a, b \in A$ gilt genau dann $(a, b) \in R$, wenn $Z(a - b) = 0$ erfüllt ist. $\square$

Kapitel 3

Algorithmische Probleme der Ringtheorie

3.1 Ringe, Ideale und Moduln

Die Begriffe der algebraischen Strukturen Halbgruppe, Monoid, Gruppe sowie die entsprechenden kommutativen oder abelschen Versionen werden als bekannt vorausgesetzt. Gleiches trifft auf die Definitionen ausgezeichneter Objekte, wie neutrales Element, Nullelement, Einselement, inverses Element oder Nullteiler inklusive der entsprechenden links- beziehungsweise rechtsseitigen Varianten zu. Existieren zu zwei Elementen a und b einer multiplikativ geschriebenen Halbgruppe H Elemente $c, d \in H$ mit $cad = b$, dann wird a ein *Teiler* von b und b ein *Vielfaches* von a genannt und die Schreibweise $a \mid b$ verwendet. Falls es zu $a, b \in H$ ein $c \in H$ mit $ca = b$ gibt, so schreiben wir $a \rfloor b$. Entsprechend weist $a \lfloor b$ auf die Existenz eines $d \in H$ mit $ad = b$ hin. In Anlehnung an die in der freien Worthalbgruppe übliche Begriffsbildung nennen wir a im Fall $a \rfloor b$ einen *Postfix* und im Fall $a \lfloor b$ einen *Präfix* von b. Für Monoide H gilt $a \rfloor b \vee a \lfloor b \Longrightarrow a \mid b$.

Allgemein versteht man unter einem *Ring* R eine abstrakte algebraische Struktur mit zwei binären Operationen $+$ und $*$, wobei R mit $+$ eine abelsche Gruppe ist und die Operationen den Distributivgesetzen

$$\begin{aligned} (a+b)*c &= a*c+b*c \\ c*(a+b) &= c*a+c*b \end{aligned}$$

genügen. Üblicherweise wird $+$ Addition und $*$ Multiplikation genannt und häufig wird das Multiplikationszeichen $*$ in Produktausdrücken weggelassen. Ist die Multiplikation sogar assoziativ, bildet also R mit $*$ eine Halbgruppe, so wird R ein assoziativer Ring genannt. Existiert darüberhinaus ein bezüglich der Multiplikation neutrales Element, d.h. R mit $*$ ist ein Monoid, so heißt R ein assoziativer Ring mit Einselement. Teilbarkeitsaussagen in assoziativen Ringen beziehen sich immer auf die multiplikative Halbgruppe.

An allen Stellen, wo wir nicht explizit etwas Gegenteiliges betonen, werden wir in dieser Arbeit unter einem Ring immer einen assoziativen Ring mit

Einselement verstehen. Eine Teilmenge $I \subseteq R$ wird ein *Linksideal* von R genannt, wenn I mit $+$ eine Untergruppe von $(R, +)$ ist und die Multiplikation eines Elements von I von links mit einem beliebigen Ringelement nicht aus I hinausführt, d.h. $R * I \subseteq I$. Analog definiert man *Rechtsideale*. Ist I sowohl Links- als auch Rechtsideal, so nennen wir es auch ein zweiseitiges Ideal oder kurz ein *Ideal*. Sei $F \subseteq R$ eine Menge von Ringelementen. Die Menge (F) aller endlichen Summen[1] $g_1 f_1 h_1 + \ldots + g_m f_m h_m$ mit $g_i, h_i \in R$ und $f_i \in F$ bildet das kleinste F umfassende Ideal von R. (F) wird das von F erzeugte Ideal genannt und alternativ auch mit $R(F)R$ bezeichnet. Entsprechend wird eine Teilmenge $F \subseteq I$ eines Ideals im Falle $I = (F)$ ein *Erzeugendensystem* von I genannt. Unter Verwendung der Nebenbedingungen $h_i = 1$ $(i = 1, \ldots, m)$ beziehungsweise $g_i = 1$ $(i = 1, \ldots, m)$ gelangen wir zum von F erzeugten Links- und Rechtsideal. Falls jede echt aufsteigende Kette von Linksidealen eines Ringes R endlich ist, so nennen wir R *linksnoethersch*. Analog erklären wir den Begriff eines *rechtsnoetherschen* Ringes. Ist R sowohl links- als auch rechtsnoethersch, so bezeichnen wir R als *noetherschen Ring*. Eine weitere mögliche aufsteigende Kettenbedingung zur Auszeichnung von Ringen wäre, zu verlangen, daß jede echt aufsteigende Kette zweiseitiger Ideale endlich sein muß. Diese Forderung ist schwächer als jede der drei vorher aufgeführten Bedingungen, da jede Kette zweiseitiger Ideale auch eine Kette von Links- beziehungsweise Rechtsidealen ist. Die aufsteigenden Kettenbedingungen für ein- beziehungsweise zweiseitige Ideale sind jeweils dazu äquivalent, daß jedes entsprechendseitige Ideal des Ringes R ein endliches Erzeugendensystem besitzt.

Seien S und R Ringe sowie $\varphi : R \to S$ ein Ringhomomorphismus. Dann bildet die Menge $ker(\varphi) := \{a \in R \mid \varphi(a) = 0\}$ ein Ideal von R. $ker(\varphi)$ wird der *Kern* von φ genannt. In Kapitel 2.1.2 hatten wir bereits den Begriff des Kerns eines Σ-Homomorphismus als die Menge aller Paare bildgleicher Elemente eingeführt. Aufgrund der einem Ring zugrundeliegenden additiven Gruppenstruktur wird diese binäre Relation bereits vollständig dadurch charakterisiert, daß man die Menge aller mit 0 bildgleichen Elemente angibt. Das rechtfertigt die Verwendung des oben eingeführten und in der Ringtheorie gebräuchlichen Kernbegriffs. Es ist wohlbekannt, daß die Ideale von R genau die möglichen vollständigen Urbilder des Nullelements des Zielrings S, d.h. die möglichen Kerne, unter einem Ringhomomorphismus $\varphi : R \to S$ sind.

Ein Ring R wird *effektiv* genannt, wenn er bezüglich einer Standardbeschreibungsvorschrift mit den Ringoperationen $+, -, *$ und den Konstanten $1, 0$ eine effektive algebraische Struktur bildet.

Neben Ringen sind in dieser Arbeit auch unitäre R-Moduln von Interesse. Unter einem *unitären R-Linksmodul M* über einem Ring R mit Einselement verstehen wir eine additiv geschriebene abelsche Gruppe M auf der zusätzlich eine den Eigenschaften

$$\begin{aligned} (a+b) \cdot m &= a \cdot m + b \cdot m \\ a \cdot (m+n) &= a \cdot m + a \cdot n \\ (a * b) \cdot m &= a \cdot (b \cdot m) \end{aligned}$$

[1] Im Fall $m = 0$ ist die folgende Summe per definitionem gleich 0.

$$1 \cdot m \quad = \quad m$$

für alle $a, b \in R$ und $m, n \in M$ genügende Linksvervielfachung $\cdot : R \times M \to R$ erklärt ist. Analog definiert man einen unitären R-Rechtsmodul M, indem man R als Rechtsoperatorenbereich mit sinngemäß geltenden Bedingungen auf M wirken läßt. Ist M sowohl unitärer R-Links- als auch unitärer R-Rechtsmodul, so nennen wir M auch einen unitären *R-Bimodul*. Jeder Ring R kann in natürlicher Weise auch als unitärer R-Links, R-Rechts- und R-Bimodul aufgefaßt werden.

Läßt man auch Ringe R zu, die nicht notwendigerweise ein Einselement besitzen und verzichtet auf die letzte der obigen an die Vervielfachung gestellten Bedingungen, so spricht man gewöhnlich von einseitigen beziehungsweise zweiseitigen R-Moduln. Für diese Arbeit vereinbaren wir, daß wir unter einem R-Modul stets einen unitären R-Modul verstehen. Außerdem werden wir abkürzend auf die Angabe des Operatorenbereichs R verzichten, falls er aus dem Kontext heraus klar ist. In den meisten Fällen ist es unumgänglich, die Seitigkeit eines R-Moduls explizit anzugeben. Gilt jedoch für den R-Bimodul M die Beziehung $\forall r \in R \, \forall m \in M \; : \; r \cdot m = m \cdot r$, so spielt die Seitigkeit keine Rolle und wir nennen M einfach einen R-Modul. Falls Mißverständnisse ausgeschlossen sind, dann werden wir, wie bereits in einigen vorangegangenen Bemerkungen geschehen, auch in allgemeinen, gleichzeitig für R-Links-, R-Rechts- und R-Bimoduln zutreffenden Aussagen abkürzend von R-Moduln sprechen.

Die Untersuchung von R-Moduln im Rahmen der universellen Algebra erfordert den Übergang zu heterogenen Algebren. Solange man die Ringelemente nicht selbst als Modulelemente zuläßt, kann man sich auf den Fall einer Familie endlich vieler paarweise disjunkter Trägermengen beschränken. Die zugehörige Theorie unterscheidet sich nur unwesentlich von der in Abschnitt 2.1.2 dargestellten Theorie der homogenen universellen Algebra.

An die Stelle der ein- beziehungsweise zweiseitigen Ideale eines Ringes treten ein- beziehungsweise zweiseitige R-Untermoduln. Der Kern eines Homomorphismus wird unter Ausnutzung der Gruppenstruktur von M wieder als vollständiges Urbild des Nullelements definiert. Die R-Linksuntermoduln eines R-Linksmoduls M sind gerade die möglichen Kerne eines R-Linksmodulhomomorphismus von M in einen zweiten R-Linksmodul. Analoges gilt im rechtsseitigen und im zweiseitigen Fall. Der Begriff des Erzeugendensystems eines Untermoduls wird in naheliegender Weise definiert. Ist jeder Links-, Rechts-, Biuntermodul von M endlich erzeugt, so spricht man in Analogie zum Ringfall von einem noetherschen Links-, Rechts- oder Bimodul. Ist R ein effektiver Ring, M eine effektive abelsche Gruppe und sind die entsprechenden Vervielfachungen berechenbar, so nennen wir M einen effektiven R-Links-, R-Rechtsbeziehungsweise R-Bimodul.

3.2 Das Idealenthaltenseinsproblem

Vorausgesetzt R ist ein effektiver Ring und $\varphi : R \to S$ ein Epimorphismus, dann ist das homomorphe Bild S gemäß Satz 2.8 genau dann ein effektiver Ring, wenn die durch die Bildgleichheit definierte Kongruenzrelation $ker_u(\varphi) \subseteq R \times R$ entscheidbar ist. Gemäß Satz 2.9 ist diese Entscheidbarkeitsfrage zur Existenz

eines kanonischen Simplifikators von $R/ker_u(\varphi)$ äquivalent, was wiederum zur Existenz eines Nullsimplifikators von $R/ker_u(\varphi)$ und zur Entscheidbarkeit des Ideals $ker(\varphi) \subseteq R$ äquivalent ist. Die Frage nach der Existenz eines Algorithmus, welcher bei beliebig vorgegebenem Ideal $I \subseteq R$ für jedes Ringelement $a \in R$ in endlich vielen Schritten feststellt, ob $a \in I$ gilt oder nicht, wird das *Idealenthaltenseinsproblem* des Ringes R genannt. Die Untersuchung des Idealenthaltenseinsproblems bedarf zunächst einmal einer Festlegung darüber, wann ein Ideal I als gegeben angesehen werden soll, und wir vereinbaren, daß das durch ein Erzeugendensystem des Ideals zu erfolgen hat.

Das Ideal I sei durch ein Erzeugendensystem F gegeben. Unter einem *Divisionsalgorithmus* modulo F verstehen wir eine Vorschrift, welche in endlicher Zeit zu gegebenem $a \in R$ Elemente $g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a} \in R$ und $f_1, \ldots, f_k \in F$ ermittelt, so daß $\hat{0} = 0$ gilt, $\hat{a}$ nur von der Restklasse $a + I$ abhängt und die Gleichung

$$a = \sum_{i=1}^{k} g_i f_i h_i + \hat{a} \tag{3.1}$$

erfüllt ist. Falls es einen Divisionsalgorithmus modulo F gibt, dann ist die durch $\sigma(a) = \hat{a}$ definierte Funktion $\sigma : R \to R$ offensichtlich ein kanonischer Simplifikator des Faktorrings R/I. Folglich impliziert die Existenz eines Divisionsalgorithmus modulo des Erzeugendensystems F die Entscheidbarkeit des Ideals I.

Auf den ersten Blick erscheint die Forderung nach der Existenz eines Divisionsalgorithmus schärfer als die nach der Entscheidbarkeit des Ideals. Es läßt sich jedoch nachweisen, daß beide Eigenschaften zueinander äquivalent sind.

Seien R ein effektiver Ring und $I \subseteq R$ ein entscheidbares Ideal. Wir gehen davon aus, daß I durch ein rekursiv aufzählbares Erzeugendensystem F, z.B. $F = I$, gegeben ist. $\nu : R \to \mathbb{N}$ sei eine Gödelisierung von R mit der Eigenschaft $\nu(0) = 0$. Aufgrund der Entscheidbarkeit von I ist die Funktion $\sigma : R \to R$ mit

$$\sigma(a) := \nu^{-1}\left(\min\{i \mid \nu^{-1}(i) - a \in I\}\right)$$

berechenbar. Insbesondere handelt es sich sogar um einen kanonischen Simplifikator von R/I. Da F rekursiv aufzählbar ist, existiert eine berechenbare Funktion $\varphi_F : \mathbb{N} \to R$ mit $im(\varphi_F) = F$. Die Menge $(\mathbb{N}^3)^*$ aller endlichen Folgen von Tripeln natürlicher Zahlen ist rekursiv aufzählbar. Sei also $t : \mathbb{N} \to (\mathbb{N}^3)^*$ eine berechenbare, surjektive Funktion. Jeder Folge $w = (i_1, j_1, l_1)(i_2, j_2, l_2) \cdots (i_k, j_k, l_k) \in (\mathbb{N}^3)^*$ läßt sich durch die Vorschrift $T(w) := \sum_{h=1}^{k} \nu^{-1}(i_h)\varphi_F(j_h)\nu^{-1}(l_h)$ ein Element von R zuordnen. Die Funktion T ist berechenbar und die Hintereinanderausführung $t \circ T$ der beiden Funktionen t und T ist total und zählt das Ideal I rekursiv auf. Die bisher eingeführten berechenbaren Funktionen erlauben es schließlich, einen Divisionsalgorithmus modulo F anzugeben:

Aufruf: $(g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a}, f_1, \ldots, f_k) :=$ DIVIDE(a, F)
Eingaben: $a \in R$,
F vermöge φ_F rekursiv aufzählbares Erzeugendensystem des Ideals I
Ausgaben: $g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a} \in R$, $f_1, \ldots, f_k \in F$, so daß (3.1) erfüllt ist.

$\hat{a} := \sigma(a)$
$r := 0$
while $T(t(r)) + \hat{a} \neq a$ **do** $r := r + 1$
return$(\nu^{-1}(i_1), \ldots, \nu^{-1}(i_k), \nu^{-1}(l_1), \ldots, \nu^{-1}(l_k), \hat{a}, \varphi_F(j_1), \ldots, \varphi_F(j_k))$,
wobei $t(r) = (i_1, j_1, l_1) \cdots (i_k, j_k, l_k)$

Die Korrektheit des Algorithmus folgt unmittelbar aus den vorangegangenen Ausführungen. Wegen $im(t \circ T) = I$ und $a - \hat{a} \in I$ gibt es ein $r_0 \in \mathbb{N}$ mit $T(t(r_0)) = a - \hat{a}$. Aufgrund von $dom(t \circ T) = \mathbb{N}$ ist jeder vorhergehende Schleifendurchlauf mit $r < r_0$ effektiv ausführbar und die **while**-Schleife wird spätestens nach r_0 Durchläufen verlassen. Damit ist bewiesen, daß der Algorithmus bei beliebiger Eingabe a nach endlicher Zeit anhält. Zusammenfassend stellen wir fest:

Satz 3.1 *Sei R ein effektiver Ring und $F \subseteq R$ eine rekursiv aufzählbare Teilmenge von R. Dann ist das von F erzeugte Ideal I von R genau dann eine entscheidbare Teilmenge von R, wenn es einen Divisionsalgorithmus modulo F gibt.*

Der Beweis des Satzes wurde bereits erbracht.

Wir haben uns bisher auf den Fall zweiseitiger Ideale beschränkt. Ein Ring R läßt sich als ein R-Linksmodul auffassen. Die Linksideale von R sind gerade die R-Linksuntermoduln von R und als solche auch die Kerne der von R ausgehenden R-Linksmodulhomomorphismen. Analoge Aussagen gelten für die entsprechenden rechtsseitigen Begriffe. Die Untersuchung der Entscheidbarkeit von einseitigen Idealen ist eng mit der Frage nach der Effektivität einseitiger Faktormoduln von R verbunden. Das legt es nahe, entsprechende Untersuchungen möglichst im Kontext beliebiger endlich erzeugter R-Linksmoduln anzusiedeln. Auf völlig analoge Weise zu den vorangegangenen Untersuchungen kann man auch im Falle ein- oder zweiseitiger R-Moduln die Äquivalenz des Enthaltenseinsproblems zur Existenz von Divisionsalgorithmen modulo rekursiv aufzählbarer Modulerzeugendensysteme nachweisen. Selbstverständlich ist in den zugehörigen Divisionsalgorithmen die entsprechende Seitigkeit dadurch zu berücksichtigen, daß gegebenenfalls alle Faktoren g_i beziehungsweise h_i gleich 1 sind.

Kommen wir noch einmal auf Algorithmus DIVIDE zurück. Abänderung der ersten Anweisung von $\hat{a} := \sigma(a)$ zu $\hat{a} := 0$ und der letzten Anweisung zu **return**(1) führt auf einen die Funktion

$$\tau_I(a) = \begin{cases} 1 & : \quad a \in I \\ \perp & : \quad \text{sonst} \end{cases}$$

berechnenden Algorithmus. Daran erkennt man, daß das Enthaltenseinsproblem eines effektiven Ringes stets wenigstens semientscheidbar ist.

Außer dem allgemeinen Idealenthaltenseinsproblem eines Ringes werden wir im weiteren auch auf einige spezielle Idealenthaltenseinsprobleme Bezug nehmen, was mit Einschränkungen an die zur Angabe eines Ideals zugelassenen Erzeugendensysteme verbunden sein wird. Wenn wir von der Entscheidbarkeit des *Idealenthaltenseinsproblems endlich erzeugter Ideale* sprechen, so impliziert

dies, daß die Beschreibung der Ideale nur durch endliche Erzeugendensysteme erfolgen darf. Insbesondere ist mit dem *Idealenthaltenseinsproblem eines noetherschen Ringes* immer das Idealenthaltenseinsproblem endlich erzeugter Ideale gemeint. Auf diesen Sachverhalt wird hier explizit hingewiesen, da die Existenz endlicher Erzeugendensysteme keineswegs absichert, daß ein solches auch effektiv aus einem beliebig vorgegebenen Erzeugendensystem extrahiert werden kann. Ist der Ring nicht noethersch, so kann sich das Idealenthaltenseinsproblem endlich erzeugter Ideale nur auf die Teilklasse der endlich erzeugten Ideale beziehen. Setzt man also das allgemeine Idealenthaltenseinsproblem mit dem Idealenthaltenseinsproblem endlich erzeugter Ideale in Beziehung, so bedeutet die Entscheidbarkeit des letzteren die Entscheidbarkeit des allgemeinen Problems relativ zur Berechenbarkeit eines endlichen Erzeugendensystems.

In ähnlicher Weise beschränkt sich das *Idealenthaltenseinsproblem eines graduierten Ringes* immer auf das Enthaltensein homogener Elemente in durch homogene Erzeugendensysteme gegebenen Idealen.

Man sieht leicht, daß die Entscheidbarkeit der speziellen Idealenthaltenseinsprobleme wiederum zur Existenz von Divisionsalgorithmen mit entsprechend eingeschränkten Eingabespezifikationen äquivalent ist.

An dieser Stelle erlauben wir uns einen Vorgriff auf die in Abschnitt 4.4 noch einzuführenden Bezeichnungen. Im Falle des Idealenthaltenseinsproblems graduierter Ringe werden die Anforderungen an den Divisionsalgorithmus dahingehend verschärft, daß jeder in Gleichung (3.1) auftretende Summand $g_i f_i h_i$ homogen vom Grad $\deg_\Gamma(a)$ sein muß. Ist ein beliebiger Divisionsalgorithmus für homogene Elemente modulo homogener Ideale gegeben, so ist es trivial, daraus einen die obigen Zusatzforderungen erfüllenden zu konstruieren. Man spaltet jeden Summanden in seine homogenen Bestandteile auf und läßt von den entstehenden homogenen Summanden diejenigen weg, deren Grad nicht mit dem von a übereinstimmt. Es gibt graduierte Ringe, deren Idealenthaltenseinsproblem als graduierter Ring entscheidbar ist, während ihr allgemeines Idealenthaltenseinsproblem als Ring unentscheidbar ist. Eine analoge Aussage trifft für endlich erzeugte Ideale zu. Ein wohlbekanntes Beispiel dafür ist der Ring $\mathbb{Q}\langle X_1, \ldots, X_n\rangle$, welcher sich durch Ringadjunktion des freien nichtkommutativen von $X_1, \ldots, X_n$ erzeugten Monoids zum Körper $\mathbb{Q}$ der rationalen Zahlen ergibt. Die Unentscheidbarkeit seines Idealenthaltenseinsproblems folgt aus der Unentscheidbarkeit des Wortproblems der freien Worthalbgruppe. Betrachtet man jedoch die gewöhnliche $\mathbb{N}$-Graduierung von $\mathbb{Q}\langle X_1, \ldots, X_n\rangle$, welche jedem Wort seine Länge als Grad zuweist, so ist das Enthaltenseinsproblem jedes bezüglich dieser Graduierung homogenen Ideals entscheidbar.

Das Grundprinzip der in dieser Arbeit dargestellten Algorithmen besteht in der Reduktion auf gleichartige Probleme für endlich erzeugte homogene Ideale der entsprechenden Seitigkeit. Im assoziierten graduierten Ring wird sich die Behandlung des einseitigen Falls stets als einfacher als die des zweiseitigen erweisen. Dadurch kann leicht der Eindruck entstehen, daß die Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter zweiseitiger Ideale die des Enthaltenseinsproblems endlich erzeugter einseitiger Ideale nach sich zieht. Dem ist aber nicht so, denn neben der Berechenbarkeit der Elementarschritte muß auch die Abbruchbedingung der Algorithmen beachtet werden.

Die Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter einseitiger Ideale impliziert nicht notwendigerweise die für zweiseitige Ideale. Ein Gegenbeispiel sind die freien $\mathbb{K}$-Algebren (siehe [Mo86]). Umgekehrt zieht auch die Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter zweiseitiger Ideale nicht die für einseitige Ideale nach sich. Gegenbeispiele dafür findet man unter den Ringen, deren assoziierter graduierter Ring die aufsteigende Kettenbedingung für zweiseitige Ideale nicht aber die für einseitige Ideale erfüllt (siehe [Mo88b]).

Aufgrund der Beziehung

$$f \in N + L \subseteq M \Longleftrightarrow f + N \in (L + N)/N \subseteq M/N \tag{3.2}$$

für beliebige R-(Links-, Rechts-) Bimoduln M, Elemente $f \in R$ und (Links-, Rechts-) Biuntermoduln N und L von M überträgt sich die Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter (Links-,Rechts-) Biuntermoduln eines R-(Links-, Rechts-) Bimoduls M auf beliebige Faktormoduln nach einem endlich erzeugten (Links-, Rechts-) Biuntermodul von M.

Während Mora bei der Untersuchung zweiseitiger Ideale in Restklassenringen nichtkommutativer Ringe ausschließlich von diesem Sachverhalt Gebrauch machte (siehe [Mo88a] und [Mo88b]), wurde in [Ap92] ein anderes Vorgehen gewählt. Zum einen stand dort die Untersuchung einseitiger Ideale in Restklassenringen nach zweiseitigen Idealen im Vordergrund. Auch wenn M noethersch ist und damit jeder seiner Unterbimoduln auch als einseitiger Untermodul endlich erzeugt ist, so ist es im allgemeinen dennoch nicht gesichert, daß ein endliches Erzeugendensystem eines Bimoduls N auf algorithmischem Wege in ein endliches Erzeugendensystem des einseitigen Moduls N transformiert werden kann. Die in [Ap92] betrachtete Klasse von Algebren stellt eine Verallgemeinerung der Algebren von auflösbarem Typ (siehe [KW90]) dar. Während die Übertragung der Gröbnertheorie einseitiger Ideale von den in [ApL85] untersuchten Einhüllenden von Liealgebren und Weylalgebren auf den allgemeineren Fall der Algebren von auflösbarem Typ sehr geradlinig verläuft, erfordert die erstmalig in [KW90] vorgenommene Einbeziehung zweiseitiger Ideale prinzipiell neue Methoden. In der konkreten Situation ist jede Gröbnerbasis eines zweiseitigen Ideals I bereits Links- beziehungsweise Rechtsidealerzeugendensystem von I. Gleiches trifft auch auf die in [Ap92] vorgenommene nochmalige Verallgemeinerung zu. Somit steht in beiden Situationen eine berechenbare Transformation endlicher zweiseitiger in endliche einseitige Erzeugendensysteme zur Verfügung. Die in [Ap92] untersuchte Klasse von Algebren ist jedoch reichhaltiger als nur der Abschluß der Klasse der Algebren von auflösbarem Typ gegenüber Restklassenringbildung. Falls das Enthaltenseinsproblem des Faktormoduls M/N entscheidbar ist, so trifft für M keineswegs mit Notwendigkeit das Gleiche zu. Insbesondere läßt sich die Untersuchung der in [Ap92] betrachteten Algebren nicht einfach auf eine bekannte Klasse von Algebren, zum Beispiel freie nichtkommutative $\mathbb{K}$-Algebren, und Beziehung (3.2) zurückführen. Deshalb und auch aus Sicht der Effizienz der Entscheidungsalgorithmen ist es in vielen Fällen ratsam, nach direkt im Restklassenring (oder allgemeiner im Faktormodul) angesiedelten Algorithmen zu suchen. Dennoch sollte darauf

hingewiesen werden, daß Beziehung (3.2) eine entscheidende Bedeutung bei der Suche nach direkten Algorithmen zukommt.

3.3 Das Syzygienproblem

Einführend wollen wir das Syzygienproblem eines R-Linksmoduls M als die Frage nach der algorithmischen Lösbarkeit einer homogenen, linearen Gleichung $\sum_{i=1}^{m} H_i f_i = 0$ in den Variablen H_i mit Koeffizienten $f_i \in M$ charakterisieren. Ein Lösungstupel $(H_1, \ldots, H_m) \in R^m$ wird eine Linkssyzygie der Elemente $f_1, \ldots, f_m$ genannt. Der Lösungsraum läßt sich in natürlicher Weise selbst zu einem R-Linksmodul machen. Man nennt ihn daher auch Linkssyzygienmodul. Obgleich die Lösungstupel selbstverständlich von der Reihenfolge der Elemente f_i abhängen und auch eine Wiederholung $f_i = f_j$, $i \neq j$, nicht unbedingt ausgeschlossen werden sollte, ist es aus Gründen, die wir hier nicht erörtern wollen, günstig, den Linkssyzygienmodul dem von $F = \{f_1, \ldots, f_m\}$ erzeugten Untermodul N von M zuzuordnen. Dementsprechend sind die Bezeichnungen $LSyz(N)$ oder auch $LSyz(F)$ gebräuchlich. Die Anordnung der Elemente von F läßt sich durch eine bijektive Zuordnung von Unbestimmten e_f zu $f \in F$ ersetzen. Um Komplikationen zu vermeiden, werden wir ein Erzeugendensystem F von N im Zusammenhang mit Syzygienberechnungen immer als geordnetes Tupel auffassen. Im weiteren werden wir den Begriff des Syzygienmoduls präzisieren und auf den Bimodulfall ausdehnen.

3.3.1 Syzygien eines R-Linksmoduls

Sei M ein R-Linksmodul und $F \subset M$ eine Teilmenge davon. Wir ordnen jedem Element $f \in F$ eine Unbestimmte e_f zu und bezeichnen den von $E = \{e_f \mid f \in F\}$ frei erzeugten R-Linksmodul mit $R^{|F|}$. Der Kern des durch $S\left(\sum_{f\in F} h_f e_f\right) = \sum_{f\in F} h_f f$ definierten R-Linksmodulhomomorphismus $S : R^{|F|} \to M$ wird der *(erste) Linkssyzygienmodul* von F genannt und mit $LSyz(F)$ bezeichnet. Aus der Definition ist unmittelbar ersichtlich, daß $LSyz(F)$ ebenfalls ein R-Linksmodul ist. Sei B ein Erzeugendensystem von $LSyz(F)$ als Untermodul von $R^{|F|}$. Auf die gleiche Weise wie vorhin gelangen wir zum Linkssyzygienmodul $LSyz(B)$ von B. Dieser heißt ein zweiter Linkssyzygienmodul von F. Sukzessives Fortsetzen der Vorgehensweise führt zu höheren Linkssyzygienmoduln von F. Bereits beim zweiten Linkssyzygienmodul besteht eine Abhängigkeit von der Wahl des Erzeugendensystems B für den vorangegangenen ersten Linkssyzygienmodul von F. Läßt man die gleiche Freiheit bei der Auswahl des Erzeugendensystems F zu, so kann man $LSyz(F)$ auch als einen ersten Linkssyzygienmodul des von F erzeugten Linksuntermoduls N von M ansehen. Betrachten wir nun eine sogenannte *Linkssyzygienkette* von N, d.h. eine Reihe aufeinanderfolgender Linkssyzygienmoduln von N. Tritt in der Linkssyzygienkette irgendwann ein Nullmodul auf, so nennen wir das Anfangsstück der von Null verschiedenen Linkssyzygienmoduln eine *freie Auflösung* von N. Obgleich Linksyzygienmoduln und Linkssyzygienkette eines R-Linksmoduls nicht eindeutig bestimmt sind, so besitzen sie doch eine Reihe invarianter Eigen-

schaften. Deren Bedeutung ist für den Inhalt dieser Arbeit nachrangig und wir werden daher nicht darauf eingehen. Der interessierte Leser wird beispielsweise auf [Ei68] und [Ren76] verwiesen.

Entsprechend lassen sich erste und höhere *Rechtssyzygienmoduln* und Rechtssyzygienketten von R-Rechtsuntermoduln einführen.

Seien R ein effektiver Ring, M ein effektiver R-Linksmodul und F eine endliche Teilmenge von M. Dann ist $R^{|F|}$ ein effektiver R-Linksmodul und der Linkssyzygienmodul $LSyz(F)$ ist eine entscheidbare Teilmenge davon.

Unter dem *Linkssyzygienproblem* von M verstehen wir die Frage nach der Existenz und der Berechenbarkeit eines endlichen Erzeugendensystems des Linksmoduls $LSyz(F)$ für jede endliche Teilmenge $F \subset M$. Gibt es einen Algorithmus, der zu einer vorgegebenen endlichen Menge $F \subset M$ stets ein endliches Erzeugendensystem des Linkssyzygienmoduls $LSyz(F)$ berechnet, so sagen wir: das Linkssyzygienproblem von M ist lösbar. Für noethersche Ringe R kann wenigstens die Frage nach der Existenz eines endlichen Erzeugendensystems generell positiv beantwortet werden:

Bemerkung 3.2 *Ein endlich erzeugter R-Linksmodul über einem noetherschen Ring R ist noethersch.*

Es reicht aus, einen von einer endlichen Menge E frei erzeugten Linksmodul M zu betrachten. Sei N ein Linksuntermodul von M. Für fest vorgegebenes $e \in E$ bezeichnen wir die Menge aller Elemente von R, die in wenigstens einem Element von N als Koeffizient von e auftreten, mit I_e. Für jedes $e \in E$ ist I_e ein Linksideal von R und als solches endlich erzeugt. Wir halten ein $e \in E$ fest und wählen zu jedem Element a eines endlichen Erzeugendensystems von I_e ein Element von N aus, dessen Koeffizient von e gleich a ist. Die Menge dieser Elemente erzeugt gemeinsam mit all den Elementen von N, in denen e nicht auftritt, den gesamten Linkmodul N. Die e nicht enthaltenden Elemente von N bilden einen Linksuntermodul des von $E\backslash\{e\}$ frei erzeugten R-Linksmoduls und durch vollständige Induktion über die Anzahl der Elemente von E folgt die Existenz eines endlichen Erzeugendensystems von N. □

3.3.2 Syzygien eines R-Bimoduls

Sei U der vom Einselement erzeugte Unterring von R und $U \subseteq Q \subseteq R$ ein beliebiger Zwischenring. Faßt man den linken Faktor als R-Links- und Q-Rechtsmodul und den rechten Faktor als Q-Links- und R-Rechtsmodul auf, so kann das Tensorprodukt $R \otimes_Q R$ mit auf natürliche Weise definierten Links- und Rechtsvervielfachungen als unitärer R-Bimodul aufgefaßt werden. Wir fixieren ein nicht zu R gehöriges Symbol e und vereinbaren die Schreibweise aeb für den Elementartensor $a \otimes b$. Während $R \otimes_U R$ freier unitärer R-Bimodul mit freiem Erzeugendensystem $\{e\}$ ist, gilt im anderen Randfall die Isomorphie $R \otimes_R R \cong R$. Mit $(R \otimes_Q R)^m$ bezeichnen wir die direkte Summe $\bigoplus_{i=1}^{m} (R \otimes_Q R)_i$ von m Exemplaren des Tensorprodukts $R \otimes_Q R$. Indem wir für jeden direkten Summanden eine Unbestimmte e_i einführen, läßt sich die oben vereinbarte Schreibweise auf die direkte Summe fortsetzen.

Sei M ein unitärer R-Bimodul, $F \subset M$ eine endliche Teilmenge von M und N der von F erzeugte R-Unterbimodul. Wir führen für jedes Element $f \in F$ eine Unbestimmte e_f ein und bezeichnen den von $E = \{e_f \mid f \in F\}$ frei erzeugten unitären R-Bimodul mit $(R \otimes_U R)^{|F|}$. Der Kern $ker(S)$ des durch die Vorschrift $S\left(\sum_{j=1}^{k} a_j e_{f_{i_j}} b_j\right) = \sum_{j=1}^{k} a_j f_{i_j} b_j$ definierten R-Bimodulhomomorphismus $S : (R \otimes_U R)^{|F|} \to M$ wird *Syzygienmodul* von F genannt und mit $Syz(F)$ bezeichnet.

Sei R ein effektiver Ring, M und $R \otimes_U R$ seien effektive R-Bimoduln und F sei eine endliche Teilmenge von M. Dann ist auch $(R \otimes_U R)^{|F|}$ ein effektiver R-Bimodul und $Syz(F)$ ist eine entscheidbare Teilmenge davon. Der Bimodul $(R \otimes_U R)^{|F|}$ ist selbst für noethersche R-Bimoduln M über einem noetherschen Ring R und endliche Mengen $F \subset M$ im allgemeinen nicht noethersch. Daher kann das Syzygienproblem im Sinne der Berechenbarkeit endlicher Erzeugendensysteme von Syzygienmoduln bereits aufgrund deren Nichtexistenz unlösbar sein. Wenden wir uns nun einem abgeschwächten Syzygienproblem zu. Sei T eine Funktion, die jeder endlichen Menge $F \subset M$ eine Teilmenge $T(F) \subseteq Syz(F)$ ihres Syzygienmoduls zuordnet. Dann verstehen wir unter der Lösbarkeit des *T-Syzygienproblems* von M, daß zu jeder endlichen Teilmenge $F \subset M$ eine endliche Menge H existiert und berechnet werden kann, für welche $H \cup T(F)$ ein Erzeugendensystem von $Syz(F)$ ist. Ein solches H nennen wir ein *T-Erzeugendensystem* von $Syz(F)$. Die Wahl der Bezeichnung T für die obige Funktion soll auf *triviale Syzygien* von F hindeuten. Als Motivation für das T-Syzygienproblem stehen Moras triviale Syzygien

$$Triv(F) = \{gae_f - e_g af \mid f, g \in F, a \in R\} \tag{3.3}$$

endlicher Teilmengen $F \subset R$ im Hintergrund (siehe [Mo88a]).

Offensichtlich ist die Frage nach einem endlichen T-Erzeugendensystem des Syzygienmoduls $Syz(F)$ äquivalent zur Frage nach einem endlichen Erzeugendensystem des Faktormoduls $Syz(F)/R \cdot T(F) \cdot R$. Wir zeigen einen Weg auf, wie man zuweilen durch Ausnutzen der Feinstruktur von M a priori triviale Syzygien ausfaktorisieren kann.

Für einen Zwischenring $U \subseteq Q \subseteq R$ bezeichne ι_Q den durch $e_f \mapsto e_f$ erklärten natürlichen Homomorphismus $\iota_Q : (R \otimes_U R)^{|F|} \longrightarrow (R \otimes_Q R)^{|F|}$. Dann kann die Lösung des T-Syzygienproblems für jedes T mit $ker(\iota_Q) \subseteq T(F) \subseteq Syz(F)$ für alle endlichen Teilmengen $F \subset M$ auf die Untersuchung der Faktormoduln $Syz(F)/ker(\iota_Q) \subseteq (R \otimes_U R)^{|F|}/ker(\iota_Q) \cong (R \otimes_Q R)^{|F|}$ reduziert werden. Sei $Z(M)$ die Menge $\{a \in R \mid \forall m \in M : am = ma\}$ aller derjenigen Ringelemente, die mit allen Modulelementen kommutieren. Durch einfaches Nachrechnen überzeugt man sich leicht, daß $Z(M)$ zusammen mit den entsprechend eingeschränkten Operationen von R für jeden beliebigen unitären R-Bimodul M einen das Einselement enthaltenden Unterring von R bildet. Im Spezialfall $M = R$ ist $Z(M)$ kommutativ und wird das Zentrum des Ringes R genannt. Für jede endliche Teilmenge F des R-Bimoduls M und jeden Zwischenring $U \subseteq Q \subseteq Z(M)$ gilt $ker(\iota_Q) \subseteq Syz(F)$. Die Nützlichkeit dieser Feststellungen wird am Beispiel eines Bimoduls M über einem kommutativen Ring R mit $Z(M) = R$ deutlich. Es wird sich erweisen, daß dort die Elemen-

te von $\ker(\iota_R)$ als trivial angesehen werden können. Damit gelangt man zu der in der kommutativen Algebra erwarteten Äquivalenz der Untersuchung der Syzygienprobleme ein- und zweiseitiger Untermoduln von M.

3.3.3 Endliche Moduldurchschnitte und Syzygien von Faktormoduln

Zwischen der Lösbarkeit des Syzygienproblems und der Berechenbarkeit des Durchschnitts endlich vieler Untermoduln besteht ein enger Zusammenhang. In einer Formulierung für Polynomideale findet man ihn beispielsweise in [GTZ88]. Basierend auf der gleichen Idee lassen sich Syzygienmoduln von Untermoduln eines Faktormoduls berechnen.

Sei M ein R-Linksmodul mit lösbarem Linkssyzygienproblem für endlich erzeugte Linksuntermoduln. Dann ist der Durchschnitt endlich vieler endlich erzeugter Linksuntermoduln berechenbar und das Linkssyzygienproblem endlich erzeugter Linksuntermoduln eines Faktorlinksmoduls von M nach einem beliebigen endlich erzeugten Linksuntermodul von M ist lösbar.

Seien N der von $H = \{h_1, \ldots, h_n\} \subset M$ und L der von $F = \{f_1, \ldots, f_m\} \subset M$ erzeugte Linksuntermodul von M. Weiterhin sei B ein beliebiges endliches Erzeugendensystem des Linkssyzygienmoduls $LSyz(F \cup H)$ der Linksmodulsumme $N + L$. Dann erzeugen

$$\{s_{f_1} f_1 + \cdots + s_{f_m} f_m \mid s_{f_1} e_{f_1} + \cdots + s_{f_m} e_{f_m} + s_{h_1} e_{h_1} + \cdots + s_{h_n} e_{h_n} \in B\}$$

den Linksmoduldurchschnitt $N \cap L$ und

$$\{(s_{f_1} + N) e_{f_1+N} + \cdots + (s_{f_m} + N) e_{f_m+N} \mid s_{f_1} e_{f_1} + \cdots + s_{f_m} e_{f_m} + s_{h_1} e_{h_1} + \cdots + s_{h_n} e_{h_n} \in B\}$$

den Linkssyzygienmodul $LSyz(F + N)$ des Linksuntermoduls $(L + N)/N \subseteq M/N$.

Beide Beziehungen lassen sich völlig geradlinig auf Rechts- und Bimoduln M sowie entsprechendseitige Untermoduln übertragen.

3.4 Das Unterringenthaltenseinsproblem

Sei R ein Ring und $F \subseteq R$ eine Teilmenge des Ringes. In Abschnitt 2.1.2 hatten wir erklärt, wie eine nichtleere Teilmenge der Trägermenge einer algebraischen Struktur eine algebraische Unterstruktur des gleichen Typs erzeugt. In diesem Sinne ist der (bezüglich der Mengeninklusion) kleinste, F umfassende Unterring $U(F)$ von R der von F erzeugte Unterring von R. Aus Sicht der universellen Algebra ist die Behandlung von Unterringen in gewisser Weise sogar natürlicher als die von Idealen, denn der im Zusammenhang mit Kernen von Homomorphismen auftauchende Idealbegriff erlangt erst in Gruppenstrukturen Bedeutung. Ähnlich dem Idealenthaltenseinsproblem können wir die Frage stellen, ob ein gegebenes Element $a \in R$ dem von F erzeugten Unterring angehört. Dies ist genau dann der Fall, wenn a Summe endlich vieler Produkte der Gestalt $f_1 \cdots f_k$

von Elementen $f_i \in F$ $(i = 1, \ldots, k)$ ist.[2] Die Frage der Entscheidbarkeit des Unterringenthaltenseinsproblems ist nicht Gegenstand dieser Arbeit, aber wir weisen darauf hin, daß es sich in einigen Fällen mit ähnlichen Methoden wie in der Theorie der Gröbnerbasen von Idealen behandeln läßt (siehe z.B. [RS88], [SS88] und [Swe88]).

[2]Per definitionem wollen wir jedes Produkt mit $k = 0$ als 1 ansehen. Betrachtet man nur Produkte mit $k \geq 1$, so gelangt man zu einer Unterstruktur von R als Ring, in welchem kein Einselement gefordert ist. Unseren Ringkonventionen entsprechend müssen wir daher $k = 0$ zulassen.

Kapitel 4

Graduierte Strukturen

Im weiteren konzentrieren wir uns auf die Suche nach Divisionsalgorithmen modulo endlichen Erzeugendensystemen von Idealen. Oftmals besteht das Schlüsselproblem in der vorherigen Aufbereitung der Idealbasis, um dann einen besonders einfachen Divisionsalgorithmus anwenden zu können. Ein mögliches Ziel der Vorbereitung besteht darin, bei vorgegebener Simplifikationshalbordnung $\prec_R$ für jedes ein- beziehungsweise zweiseitige Ideal I ein derartiges endliches Erzeugendensystem F von I auszuzeichnen, so daß es Gleichung (3.1) erfüllende Objekte gibt, für die in der Folge

$$a, a - g_1 f_1 h_1, \ldots, a - \sum_{i=1}^{k} g_i f_i h_i = \hat{a}$$

niemals ein Element vor einem bezüglich $\prec_R$ größeren auftritt. Im Idealfall streben wir eine monoton fallende Folge an. Man beachte, daß bereits bei der schwächeren, die Unvergleichbarkeit zulassenden Forderung ein derartiges F selbst in noetherschen Ringen nicht notwendigerweise für jedes Ideal zu existieren braucht. Aber man kann zumindest für eine große Klasse von Ringen bei Verwendung geeigneter Simplifikationshalbordnungen die Existenz eines entsprechenden Aufbereitungsalgorithmus nachweisen.

Ein seit langem bekanntes Beispiel für einen derartigen Aufbereitungsalgorithmus ist der Euklidische Algorithmus in effektiven Euklidischen Ringen. Ein anderes Beispiel ist der Gaußsche Algorithmus, welcher in endlichdimensionalen Vektorräumen über effektiven Körpern zum Einsatz kommt. Vektorräume und Untervektorräume fügen sich als Moduln über Körpern in die bisherigen Betrachtungen ein. In die Reihe dieser Beispiele gehört aber auch der Buchbergeralgorithmus in Polynomringen in endlich vielen Unbestimmten über einem effektiven Körper, welcher die beiden vorher genannten Algorithmen als Spezialfälle umfaßt. In den letzten zwei Jahrzehnten wurde Buchbergers Algorithmus von verschiedenen Autoren auf zahlreiche andere Klassen von Ringen verallgemeinert. Nachdem viele Jahre lang immer wieder neue, mehr oder weniger große Klassen von Ringen von Grund auf untersucht wurden, entwickelten Robbiano und Mora Ende der 80-iger Jahre das sehr umfassende, viele der vorherigen Ansätze subsummierende Konzept der graduierten Strukturen (siehe [Rob86] und [Mo88a]). Moras Verdienst bestand dabei vor allem in der Verallgemeine-

rung der Robbianoschen Theorie auf nichtkommutative Ringe. Die Robbiano-Morasche Methode liefert eine relative Berechenbarkeit bezüglich der Effektivität der Grundstrukturen und einiger weiterer Funktionen. Die ursprünglich notwendigen Untersuchungen zur Übertragung des Buchbergerschen Algorithmus schrumpften damit auf die Berechenbarkeitsnachweise gewisser Grundfunktionen zusammen.

In diesem Kapitel werden wir das allgemeine Konzept graduierter Strukturen auf der Grundlage der Moraschen Arbeit [Mo88a] darlegen.

4.1 Geordnete Monoide

Ein *geordnetes Monoid* ist eine algebraische Struktur $(\Gamma, \circ, \prec)$ mit einer binären Operation $\circ$ und einer linearen Ordnung $\prec$, wobei Γ mit $\circ$ ein Monoid, das heißt eine Halbgruppe mit neutralem Element ϵ, bildet und $\circ$ monoton bezüglich $\prec$ ist. In dieser Arbeit verlangen wir immer die Irreflexivität von $\prec$ und die strenge Monotonie in dem Sinne, daß für alle Monoidelemente $a, b, c \in \Gamma$ aus der Beziehung $a \prec b$ die Relationen $a \circ c \prec b \circ c$ und $c \circ a \prec c \circ b$ folgen. In der Literatur findet man zuweilen auch eine schwächere, auf dem reflexiven Abschluß von $\prec$ beruhende Monotoniebedingung. Man sieht sofort, daß in jedem bezüglich einer streng monotonen Ordnung geordnetem Monoid die linke und die rechte Kürzungsregel gelten, das heißt:

$$\forall a, b, c \in \Gamma \ : \ c \circ a = c \circ b \vee a \circ c = b \circ c \Rightarrow a = b \quad . \tag{4.1}$$

Wir nennen Γ ein *effektives geordnetes Monoid*, falls es mit der Operation $\circ$, der Konstanten ϵ und der Ordnungsrelation $\prec$ eine effektive algebraische Struktur bildet. Bei der Behandlung graduierter Strukturen werden wir stets geordnete Monoide betrachten, ohne daß wir an jeder Stelle explizit auf die Ordnung hinweisen werden. Wenn wir in diesem Zusammenhang kurz von einem effektivem Monoid sprechen, so bezieht sich die Effektivität immer auf die algebraische Struktur, die neben den Monoidoperationen auch die Ordnung beinhaltet. Entsprechend verwenden wir die Begriffe der *geordneten Halbgruppe* und der *geordneten Gruppe*. Jede geordnete Halbgruppe Γ läßt sich durch Hinzunahme eines Elementes $-\infty$ zu einer geordneten Halbgruppe $\hat{\Gamma} = \Gamma \cup \{-\infty\}$ erweitern, wobei $-\infty$ kleinstes Element von $\hat{\Gamma}$ bezüglich $\prec$ und gleichzeitig absorbierendes Element bezüglich $\circ$ ist.

Eine nichtleere Teilmenge $M \subseteq \Gamma$ mit $\Gamma \circ M \subseteq \Gamma$ wird ein *Monoidlinksideal* von Γ genannt. Entsprechend nennt man M ein *Monoidrechtsideal* wenn $M \circ \Gamma \subseteq \Gamma$ gilt und ein (zweiseitiges) *Monoidideal* falls M sowohl Monoidlinks- als auch Monoidrechtsideal ist. $Y \subseteq M$ heißt Erzeugendensystem des Monoidideals M, wenn $\Gamma \circ Y \circ \Gamma = M$ gilt.

Falls ein geordnetes Monoid Γ ein kleinstes Element ω besitzt, so muß dies das neutrale Element ϵ von Γ sein, denn angenommen $\omega \prec \epsilon$, so $\omega^2 = \omega \circ \omega \prec \omega \circ \epsilon = \omega$ im Widerspruch zur Minimalität von ω. In einem geordneten Monoid mit kleinstem Element ist ϵ das einzige invertierbare Element, denn sei $\gamma \in \Gamma$ invertierbar, dann führt Multiplikation von $\epsilon \preceq \gamma$ mit dem Inversen γ^{-1} auf die Ungleichung $\gamma^{-1} \preceq \epsilon$, was aufgrund der Minimalität von ϵ die Gleichheit

$\gamma = \gamma^{-1} = \epsilon$ nach sich zieht. Analog überlegt man sich, daß es sich im Falle der Existenz eines größten Elementes von Γ auch nur um das neutrale Element ϵ handeln kann und daß auch dann ϵ einziges invertierbares Element sein muß. In jedem wohlgeordneten Monoid Γ gilt für alle $\gamma, \omega, \omega' \in \Gamma$ die Beziehung

$$\gamma \preceq \omega \circ \gamma \circ \omega', \tag{4.2}$$

denn andernfalls hätte die Menge $\{\omega^i \circ \gamma \circ \omega'^i \mid i \in \mathbb{N}\}$ wegen $\omega \circ \gamma \circ \omega' \prec \gamma \Rightarrow \omega^{k+1} \circ \gamma \circ \omega'^{k+1} \prec \omega^k \circ \gamma \circ \omega'^k$ kein kleinstes Element.

Auf ähnliche Weise sieht man, daß das minimale Erzeugendensystem eines beliebigen ein- oder zweiseitigen Monoidideals M eines wohlgeordneten Monoids Γ eindeutig bestimmt ist. Denn seien X und Y zwei minimale Erzeugendensysteme von M. Dann gibt es zu jedem $x \in X$ Elemente $y \in Y$ und $x' \in X$ mit $ayb = x$ und $y = a'x'b'$, also $aa'x'b'b = x$, was wegen der Minimalität von X die Gleichheit $x = x'$ und aus Ordnungsgründen die Gültigkeit von $a = b = a' = b' = \epsilon$ zur Folge hat. Daraus folgt $X \subseteq Y$ und wegen der Minimalität von Y muß die Gleichheit gelten.

Da in einem wohlgeordnetem Monoid Γ nur das Element ϵ invertierbar ist, bildet die Menge $\Gamma\backslash\{\epsilon\}$ ein Monoidideal von Γ. X ist genau dann ein minimales Erzeugendensystem des Monoidideals $\Gamma\backslash\{\epsilon\}$, wenn X ein minimales Erzeugendensystem des Monoids Γ ist. Daher ist auch das Monoiderzeugendensystem eindeutig bestimmt. Darüberhinaus wird $\Gamma\backslash\{\epsilon\}$ bereits als Monoidlinks- beziehungsweise Monoidrechtsideal von X erzeugt.

Für Ordnungen $\prec$ von Γ mit der Eigenschaft, daß jede nach unten beschränkte Teilmenge von Γ wohlgeordnet ist, führen wir die Bezeichnung *beschränkte Wohlordnung*[1] ein. Die Eigenschaft, beschränkte Wohlordnung zu sein, ist äquivalent dazu, daß zu jeder unendlichen Folge $\gamma_1 \succ \gamma_2 \succ \cdots$ und jedem $\gamma \in \Gamma$ ein $n_0(\gamma)$ mit $\gamma_n \prec \gamma$ für alle $n \geq n_0(\gamma)$ existiert. Offensichtlich ist jede Wohlordnung erst recht eine beschränkte Wohlordnung. Ist die beschränkte Wohlordnung $\prec$ dagegen keine Wohlordnung, so ist Γ nach unten unbeschränkt, Γ besitzt also kein kleinstes Element.

Einen wichtigen Spezialfall stellt die Klasse der Monoide dar, in denen Dicksons Lemma (siehe [Di13]) gilt. Im Fall eines kommutativen Monoids Γ sagt Dicksons Lemma aus, daß für jede unendliche Folge $\gamma_1, \gamma_2, \ldots$ von Elementen aus Γ Indizes i und j mit $i < j$ und $\gamma_i \mid \gamma_j$ existieren. Für nichtkommutative Monoide Γ spaltete sich die Bedingung bezüglich der Seitigkeit auf. An die Stelle der Teilerrelation tritt im linksseitigen Fall die Postfix- und im rechtsseitigen Fall die Präfixrelation. Im zweiseitigen Fall gibt es zwei natürliche Verallgemeinerungen, nämlich erstens: die Teilbarkeitsrelation zu verwenden oder zweitens: zu verlangen, daß sowohl die linksseitige als auch die rechtsseitige Bedingung erfüllt sind. Die beschriebenen Varianten Dicksons Lemma entsprechen den aufsteigenden Kettenbedingungen in Ringen. Wir nennen das Monoid Γ *linksnoethersch*, wenn Γ Dicksons Lemma in der Postfix-Variante erfüllt. Gilt für Γ die Präfix-Variante Dicksons Lemma, so heißt Γ *rechtsnoethersch*. Ein Monoid Γ wird *noethersch* genannt, falls es sowohl links- als auch rechtsnoethersch ist.

[1] Mora nennt diese Ordnungen *inf-limited* (siehe [Mo88a]).

In einem noetherschen Monoid ist jedes Monoidideal beliebiger Seitigkeit endlich erzeugt. Man überlegt sich leicht, daß jede unendliche Folge $\gamma_1, \gamma_2, \ldots$ von Elementen eines noetherschen Monoids Γ eine unendliche Teilfolge $\gamma_{i_1}, \gamma_{i_2}, \ldots$, $i_1 < i_2 < \ldots$, besitzt, welche für alle $j < k$ die Bedingung $\gamma_{i_j} \mid \gamma_{i_k}$ erfüllt. Zum Beweis konstruiert man zuerst eine Teilfolge $\gamma_{j_1}, \gamma_{j_2}, \ldots$ mit $\gamma_{j_1} \mid \gamma_{j_k}$ für alle $k > 1$. Besitzt γ_1 unendlich viele Vielfache unter den γ_i, dann bilden diese Vielfachen bereits eine solche Teilfolge. Andernfalls entfernen wir die endlich vielen Vielfachen von γ_1 und fahren mit der unendlichen Restfolge der verbleibenden Glieder fort. k_i sei der kleinste Index eines Elementes welches beim i-ten Durchlauf entfernt wurde, insbesondere $k_1 = 1$. Nach Konstruktion gilt für alle $i < j$ die Beziehung $\gamma_{k_i} \nmid \gamma_{k_j}$. Da Γ als noethersch vorausgesetzt war, muß die Folge der k_i nach endlich vielen Schritten abbrechen, was die Existenz der Teilfolge $\gamma_{j_1}, \gamma_{j_2}, \ldots$ nach sich zieht. Man setzt $i_1 = j_1$ und fährt mit $\gamma_{j_2}, \gamma_{j_3}, \ldots$ wie oben fort. Im Ergebnis dieses Prozesses entsteht Glied für Glied die behauptete unendliche Teilfolge $\gamma_{i_1}, \gamma_{i_2}, \ldots$. Anstelle der Teilbarkeit kann ebenso die Präfix- oder Postfixrelation gefordert werden.

Eine Verallgemeinerung des Hilbertschen Basissatzes (vgl. [vW67]) zeigt einen engen Zusammenhang zwischen noetherschen Monoiden und noetherschen Ringen auf. Für jeden noetherschen Ring Q ist der *Monoidring* $Q\langle\Gamma\rangle$, dessen additive Gruppe die direkte Summe $\bigoplus_{\gamma\in\Gamma} Q\gamma$ ist und dessen Multiplikation durch $\gamma\omega = \gamma \circ \omega$ sowie $\gamma c = c\gamma$ für alle $\gamma, \omega \in \Gamma$ und alle $c \in Q$ festgelegt wird, genau dann noethersch, wenn Γ noethersch ist. Analoges gilt im linksseitigen, rechtsseitigen und im schwachen zweiseitigen Fall.

Unter dem *Teilbarkeitsproblem* eines Monoids Γ verstehen wir die Frage, ob zu beliebig vorgegebenen $\gamma, \omega \in \Gamma$ entschieden werden kann, ob es Elemente $\gamma', \gamma'' \in \Gamma$ mit $\gamma' \circ \gamma \circ \gamma'' = \omega$ gibt. Das Teilbarkeitsproblem ist die geradlinige Übertragung des Idealenthaltenseinsproblems von Ringen auf den Monoididealfall. Im Falle der Entscheidbarkeit des Teilbarkeitsproblems kann man, ähnlich zur Situation bei Ringen, einen Divisionsalgorithmus angeben, der bei Vorliegen der Teilbarkeit passende Kofaktoren γ' und γ'' durch sukzessives Durchprobieren aller Paare von Elementen von Γ ermittelt und andernfalls $FALSE$ ausgibt. Eine Verschärfung des Teilbarkeitsproblems besteht im Auffinden aller möglichen Kofaktorpaare (γ', γ''). Analog kann man das *Präfix-* beziehungsweise *Postfixproblem* des Monoids Γ einführen.

Jedes Element $\gamma \in \Gamma\backslash\{\epsilon\}$ eines noetherschen wohlgeordneten Monoids Γ besitzt nur endlich viele Zerlegungen in irreduzible Faktoren. Dabei nennen wir ein Element $\gamma \in \Gamma$ *irreduzibel*, wenn es von ϵ verschieden ist und keine Elemente $\gamma', \gamma'' \neq \epsilon$ mit $\gamma = \gamma' \circ \gamma''$ existieren. Jedes Element des minimalen Erzeugendensystems X von Γ ist irreduzibel, denn die Existenz einer Zerlegung würde der Minimalität von X oder der Wohlordnungseigenschaft von $\prec$ widersprechen. Ein noethersches wohlgeordnetes Monoid ist immer endlich erzeugt, daher kann ein beliebiges $\gamma \in \Gamma$ nur endlich viele Elemente von X als Präfix haben. Aufgrund der Gültigkeit der Kürzungsregel gehört zu jedem Präfix X_j ein eindeutig bestimmter Postfix γ' von γ mit $\gamma = X_j \circ \gamma'$. Die Existenz unendlich vieler Faktorzerlegungen würde die Existenz einer unendlichen Folge $\gamma_1, \gamma_2, \ldots$ paarweise verschiedener Monoidelemente mit $\gamma_{i+1} \rfloor \gamma_i$ für alle $i = 1, 2, \ldots$ nach sich ziehen, was in einem wohlgeordneten noetherschen Monoid unmöglich ist.

Die Frage nach der Endlichkeit und Berechenbarkeit der Menge aller möglichen Zerlegungen eines Monoidelements in irreduzible Faktoren nennen wir das *Faktorisierungsproblem* des Monoids Γ.

Der oben geführte Endlichkeitsnachweis der Menge aller irreduziblen Faktorzerlegungen eines beliebigen Elements eines wohlgeordneten noetherschen Monoids Γ ist konstruktiv und man erkennt gleichzeitig daraus, daß die Lösung des Faktorisierungsproblems auf die Effektivität von Γ und die Entscheidbarkeit des Präfixproblems reduziert werden kann. Mehr noch, neben der Effektivität ist es sogar nur erforderlich, daß für beliebiges $X_i \in X$ und $\gamma \in \Gamma$ entschieden werden kann, ob X_i Präfix von γ ist. Mit dem Faktorisierungsproblem werden gleichzeitig eine Reihe weiterer Probleme algorithmisch lösbar. Neben der Entscheidbarkeit von Teilbarkeits-, Präfix- und Postfixproblem ergibt sich für beliebige $\gamma, \omega \in \Gamma$ die Endlichkeit und Berechenbarkeit der Menge $quot(\gamma, \omega) = \{(\gamma', \gamma'') \in \Gamma \times \Gamma \mid \gamma' \circ \gamma \circ \gamma' = \omega\}$. Ein Monoidelement γ ist genau dann Teiler von ω, wenn $quot(\gamma, \omega) \neq \emptyset$ gilt. In diesem Sinne hat die Berechenbarkeit von *quot* die algorithmische Lösbarkeit eines strengeren Teilbarkeitsproblems zur Folge. Weiterhin ist γ genau dann Präfix von ω, wenn ein $(\epsilon, \gamma'') \in quot(\gamma, \omega)$ existiert, dieses Element ist dann sogar eindeutig bestimmt. Entsprechendes gilt für die Postfixrelation. Die Menge

$$mgV(\gamma, \gamma') = \{\omega \,:\, \gamma \mid \omega \wedge \gamma' \mid \omega \wedge \big(\forall \omega' \neq \omega \,:\, \omega' \mid \omega \longrightarrow \gamma \nmid \omega' \vee \gamma' \nmid \omega'\big)\}$$

aller *minimalen gemeinsamen Vielfachen* zweier beliebiger Elemente $\gamma, \gamma' \in \Gamma$ eines noetherschen Monoids ist stets endlich. Ersetzt man die Teilerbeziehung durch die Präfix- beziehungsweise Postfixrelation, so gelangt man zu den Mengen aller *minimalen gemeinsamen Links-* $(mgLV(\gamma, \gamma'))$ und aller *minimalen gemeinsamen Rechtsvielfachen* $(mgRV(\gamma, \gamma'))$ von γ und γ'.

In den in dieser Arbeit angeführten Beispielen werden vor allem zwei Typen von Monoiden zur Anwendung kommen. Sei $X = \{X_1, \ldots, X_n\}$ eine endliche Menge von paarweise verschiedenen Objekten. Mit $T(X) = T(X_1, \ldots, X_n)$ bezeichnen wir das von X frei erzeugte kommutative Monoid. $T(X)$ ist isomorph zum additiven Monoid $\mathbb{N}^n$ der n-Tupel natürlicher Zahlen. Außerdem verwenden wir das von X frei erzeugte nichtkommutative Monoid $S(X) = S(X_1, \ldots, X_n)$, welches zur von X frei erzeugten Worthalbgruppe $\langle X \rangle$ (mit leerem Wort) isomorph ist.

Die Monoidstruktur ist in beiden Fällen wohlbekannt und bedarf sicher keiner weiteren Erklärung. Zu den möglichen Monoidordnungen erscheinen jedoch einige Worte angebracht. Für die abelschen Monoide $\mathbb{N}^n$ findet man eine vollständige Klassifikation der mit der Monoidstruktur verträglichen Ordnungen in [Rob85], die wesentlichen Resultate gehen auf [Er56] zurück. Die Klassifikation basiert auf Beschreibungen der Monoidordnungen durch reelle Matrizen. Wir beschränken uns hier auf die Darlegung der wesentlichsten Sachverhalte, für die Beweise und weiteren Zusammenhänge wird auf [Rob85] verwiesen.

Ordnet man jeder Variablen X_k, $k = 1, \ldots, n$, eine reelle Zahl g_k zu, so definiert

$$(i_1, \ldots, i_n) \sqsubset (j_1, \ldots, j_n) \Longleftrightarrow \sum_{k=1}^{n} g_k i_k < \sum_{k=1}^{n} g_k j_k \tag{4.3}$$

eine additionsverträgliche Halbordnung von $\mathbb{N}^n$. Wir nennen g_k das *Gewicht* von X_k und bezeichnen die Monoidhalbordnung $\sqsubset$ als eine *gewichtete Gradordnung* von $\mathbb{N}^n$.

Sind $\prec_1$ und $\prec_2$ zwei beliebige additionsverträgliche Halbordnungen von $\mathbb{N}^n$, dann kann man $\prec_1$ durch $\prec_2$ zu einer ebenfalls additionsverträglichen Halbordnung $\prec$ von $\mathbb{N}^n$ verfeinern, indem man für beliebige $u, v \in \mathbb{N}^n$ definiert:

$$u \prec v \iff u \prec_1 v \vee (u \# v \wedge u \prec_2 v) \quad . \tag{4.4}$$

Dabei bezeichnet die Schreibweise $u\#v$ die Unvergleichbarkeit von u und v in der Halbordnung $\prec_1$, d.h. $u \neq v$, $u \not\prec_1 v$ und $v \not\prec_1 u$. Seien $\sqsubset_1, \ldots, \sqsubset_m$ gewichtete Gradordnungen, wobei die Variable X_j bezüglich $\sqsubset_i$ für $1 \leq i \leq m$ und $1 \leq j \leq n$ das Gewicht $g_{i,j}$ aufweist. Dann beschreibt die $m \times n$-Matrix $\mathfrak{A} = (g_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$ vermöge

$$u \prec_{\mathfrak{A}} v \iff \mathfrak{A}u^T <_{lex} \mathfrak{A}v^T \quad , \tag{4.5}$$

wobei $<_{lex}$ die lexikographische Ordnung der m-Tupel reeller Zahlen ist, eine Monoidhalbordnung $\prec_{\mathfrak{A}}$ von $\mathbb{N}^n$. Zum ersten ist $\prec_{\mathfrak{A}}$ eine Verfeinerung von $\sqsubset_1$ und zum weiteren auch eine Verfeinerung jeder der sukzessiven Verfeinerungen von $\sqsubset_1$ durch $\sqsubset_2, \ldots, \sqsubset_k$, $2 \leq k < m$, gemäß (4.4). Weiter gilt, daß sich jede (lineare) Monoidordnung $\prec$ von $\mathbb{N}^n$ durch eine Folge von höchstens n gewichteten Gradordnungen $\sqsubset_1, \ldots, \sqsubset_m$ im Sinne von (4.5) darstellen läßt. Ohne Beschränkung der Allgemeinheit können wir annehmen, daß der Zeilenrang von $\mathfrak{A}$ gleich m, also maximal, ist. Andernfalls wäre wenigstens eine der beschreibenden gewichteten Gradordnungen überflüssig und könnte weggelassen werden.

Zu jeder Ordnung $\prec$ gibt es unendlich viele beschreibende Matrizen der obigen Art, insbesondere ist nur die erste gewichtete Gradordnung $\sqsubset_1$ durch $\prec$ eindeutig bestimmt. In [CMP95] werden Normalformdarstellungen für die Matrizen aufgezeigt. Da jedoch alle in dieser Arbeit benötigten Eigenschaften von der konkreten Auswahl der beschreibenden Matrix unabhängig sind, werden wir keine Normalformen benötigen und auf ihre Beschreibung verzichten.

Bemerkung 4.1 *Sei $\mathfrak{A} = (g_{i,j})$ eine reelle $m \times n$-Matrix des Ranges m, so daß die vermöge (4.5) definierte Monoidhalbordnung $\prec_{\mathfrak{A}}$ linear ist. Es gilt:*

i) $\prec_{\mathfrak{A}}$ ist genau dann eine Wohlordnung, wenn das am weitesten oben stehende Nichtnullelement jeder Spalte von $\mathfrak{A}$ positiv ist.

ii) Falls $\mathbb{N}^n$ ein bezüglich $\prec_{\mathfrak{A}}$ maximales Element besitzt, dann ist $\prec_{\mathfrak{A}}$ genau dann eine beschränkte Wohlordnung, wenn alle Einträge der ersten Zeile von $\mathfrak{A}$, das heißt alle zur ersten gewichteten Gradordnung gehörigen Gewichte, negativ sind.

Beweis: *i)* Wäre z.B. das am weitesten oben stehende Gewicht der j-ten Spalte negativ, so besäße die Menge der Exponentenvektoren aller Potenzen von X_j kein kleinstes Element.

Erfüllt $\mathfrak{A}$ die gestellten Forderungen, so zeigt man mittels vollständiger Induktion über n, daß jede streng monoton fallende Folge von Exponentenvektoren endlich ist.

ii) Wie oben gezeigt wurde, muß der Nullvektor ϵ das größte Element von $\mathbb{N}^n$ sein. Hätte eine Variable in der ersten Zeile von $\mathfrak{A}$ ein positives Gewicht, so wäre ϵ nicht maximal. Nehmen wir an, es gäbe eine Variable X_j mit dem Gewicht 0 in der ersten Zeile von $\mathfrak{A}$. Aufgrund des Maximalrangs von $\mathfrak{A}$ hat wenigstens eine der anderen Variablen, sagen wir X_i, ein von Null verschiedenes, also negatives, Gewicht. Der erste von Null verschiedene Eintrag in der j-ten Spalte muß negativ sein, sonst wäre der Exponentenvektor von X_j größer als ϵ. Folglich fällt die Folge der Exponentenvektoren aufsteigender Potenzen von X_j streng monoton, ohne dabei jemals den Exponentenvektor von X_i zu unterschreiten. Das steht im Widerspruch zur beschränkten Wohlordnungseigenschaft.

Seien alle Einträge der ersten Zeile von $\mathfrak{A}$ negativ. Für eine beliebige bezüglich $\prec_{\mathfrak{A}}$ streng monoton fallende Folge von Exponentenvektoren unterschreitet die Folge der Skalarprodukte mit der ersten Zeile von $\mathfrak{A}$ jede vorgegebene ganze Zahl. Folglich ist $\prec_{\mathfrak{A}}$ eine beschränkte Wohlordnung. □

Für eine Reihe von Anwendungen ist es notwendig, Monoidwohlordnungen vom Ordnungstyp ω einzusetzen. Die Begriffsbildung erfolgt in Anlehnung an die Kleinerordnung der natürlichen Zahlen[2]. Eine lineare Ordnung $(M, \prec)$ heißt vom *Ordnungstyp* ω, wenn die Teilmenge $\{a \in M \mid a \prec m\}$ für jedes vorgegebene $m \in M$ endlich ist. Diese Forderung ist dazu äquivalent, daß $(M, \prec)$ Wohlordnung und $(M, \succ)$ beschränkte Wohlordnung ist, wobei $\succ$ in der üblichen Weise durch $a \succ b \iff b \prec a$ definiert wird. Ist M ein Monoid und $\prec$ eine Monoidordnung, so ist auch $\succ$ eine Monoidordnung. Sei $M = T(X)$ und die Matrix $\mathfrak{A}$ beschreibe die Monoidordnung $\prec$, dann beschreibt $-\mathfrak{A}$ die Monoidordnung $\succ$. Bemerkung 4.1 gibt somit auch Aufschluß über die Darstellung einer Ordnung vom Ordnungstyp ω. Diese zeichnen sich gerade dadurch aus, daß sie lineare Verfeinerungen gewichteter Gradordnungen mit durchweg positiven Gewichten sind.

Wir kommen nun zum Fall freier Worthalbgruppen. Sei $\tau : \langle X \rangle \to \mathbb{N}^n$ der natürliche Homomorphismus, der jedem Wort über dem Alphabet $X = \{X_1, \ldots, X_n\}$ den Vektor der Anzahl der Vorkommen der Buchstaben $X_1, \ldots, X_n$ zuordnet. Weiterhin sei $\prec$ eine Monoidordnung von $\mathbb{N}^n$. Dann definiert

$$u \sqsubset v \iff \tau(u) \prec \tau(v) \vee (\tau(u) = \tau(v) \wedge u \sqsubset_{lex} v)$$

eine Monoidordnung von $\langle X \rangle$. Dabei ist $\sqsubset_{lex}$ eine lexikographische Ordnung der Wörter über X. Natürlich läßt sich nicht jede Monoidordnung von $\langle X \rangle$ auf diese Weise darstellen, unsere Untersuchungen werden sich aber auf diesen Typ beschränken. Der Schnitt von τ, der jedem Vektor $u \in \mathbb{N}^n$ gerade das Wort $X_{k_1} X_{k_2} \cdots X_{k_m}$ zuordnet, welches $\tau\,(X_{k_1} X_{k_2} \cdots X_{k_m}) = u$ und $k_1 \leq k_2 \leq \ldots \leq k_m$ erfüllt, ist eine injektive Abbildung von $\mathbb{N}^n$ in $\langle X \rangle$. Zusammen mit den natürlichen Isomorphismen zwischen $T(X)$ und $\mathbb{N}^n$ sowie $S(X)$ und $\langle X \rangle$ liefert dieser Schnitt eine Einbettung der Menge $T(X)$ in die Menge $S(X)$. In diesem Sinne werden wir $T(X)$ in Zukunft als Teilmenge von $S(X)$ ansehen.

[2]Insbesondere in der Mengenlehre und einigen anderen Grenzgebieten zwischen Mathematik und theoretischer Informatik wird die Menge der natürlichen Zahlen mit dem Symbol ω bezeichnet.

Selbstverständlich handelt es sich dabei um eine reine Mengeninklusion und keineswegs um eine Untermonoidbeziehung.

4.2 Gefilterte Ringe

Seien Γ eine geordnetes Monoid mit neutralem Element ϵ, $\hat{\Gamma} = \Gamma \cup \{-\infty\}$ und R ein Ring. Eine Familie $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ bestehend aus additiven Untergruppen von R die für alle $\gamma, \gamma' \in \Gamma$ den Bedingungen

$$\begin{array}{rcll} \bigcup \mathfrak{F} & = & R & , \\ \gamma \preceq \gamma' & \Longleftrightarrow & \mathcal{F}_\gamma \subseteq \mathcal{F}_{\gamma'} & \text{und} \\ \mathcal{F}_\gamma \mathcal{F}_{\gamma'} & \subseteq & \mathcal{F}_{\gamma\circ\gamma'} & \end{array} \tag{4.6}$$

genügen, wird eine Γ-*Filtrierung*[3] von R genannt. $(R, \Gamma, \mathfrak{F})$ heißt eine *gefilterte Ringstruktur* und R ein *gefilterter Ring*. R wird *effektiver gefilterter Ring* genannt, falls R ein effektiver Ring, Γ ein effektives geordnetes Monoid und jede Untergruppe $\mathcal{F}_\gamma$ eine entscheidbare Teilmenge von R ist.

Eine Funktion $\varphi : R \to \hat{\Gamma}$ wird eine Γ-*Pseudobewertung* (oder kurz eine Pseudobewertung) des Ringes R genannt, falls sie für alle $a, b \in R$ und alle invertierbaren Elemente $e \in R$ den Bedingungen:

$$\begin{array}{rcl} \varphi(a) = -\infty & \Longleftrightarrow & a = 0 \\ \varphi(a+b) & \preceq & \max(\varphi(a), \varphi(b)) \\ \varphi(ab) & \preceq & \varphi(a) \circ \varphi(b) \\ \varphi(e) & = & \epsilon \end{array} \tag{4.7}$$

genügt. Γ heißt das *Wertemonoid* der Pseudobewertung φ und (R, φ) wird als *pseudobewerteter Ring* bezeichnet. Gilt für alle $a, b \in R$ sogar die Gleichheit $\varphi(ab) = \varphi(a) \circ \varphi(b)$, so nennt man φ eine *Bewertung* und (R, φ) einen *bewerteten Ring*. Wenn φ aus dem Kontext heraus klar ist, werden wir abkürzend R als (pseudo-) bewerteten Ring bezeichnen. Wegen $\varphi(-a) \preceq \varphi(-1) \circ \varphi(a) = \varphi(a) = \varphi(-(-a)) \preceq \varphi(-a)$ und $\varphi(b) = \varphi((a+b)-a) \preceq \max(\varphi(a+b), \varphi(-a))$ genügt jede Pseudobewertung φ für alle $a, b \in R$ den Relationen

i) $\varphi(a) = \varphi(-a)$ und

ii) $\varphi(a) \prec \varphi(b) \Rightarrow \varphi(a+b) = \varphi(b)$.

Für jedes $\gamma \in \Gamma$ beschreibt $\mathcal{F}_\gamma^\varphi = \{a \in R \mid \varphi(a) \preceq \gamma\}$ eine Untergruppe der additiven Gruppe von R. Die Familie $\mathfrak{F}^\varphi = (\mathcal{F}_\gamma^\varphi)_{\gamma\in\Gamma}$ ist eine Filtrierung von R, diese werden wir die von der Pseudobewertung φ induzierte Filtrierung nennen. Sind R ein effektiver Ring, Γ ein effektives geordnetes Monoid und $\varphi : R \to \hat{\Gamma}$ eine berechenbare Pseudobewertung, dann ist R mit der durch φ induzierten Filtrierung ein effektiver gefilterter Ring.

[3] Man kann den Begriff der Filtrierung auch ohne die erste der drei Bedingungen einführen. Den Bezeichnungen von [Ei89] folgend, handelt es sich bei dem hier betrachteten Filtrierungsbegriff nur um den Spezialfall *erschöpfender* Filtrierungen.

4.3 Gefilterte Moduln und Gröbnerfiltrierungen

Seien $(R,\Gamma,\mathfrak{F})$ eine gefilterte Ringstruktur und M ein R-Linksmodul. Analog zu Ringen führen wir den Begriff einer Γ-*Filtrierung* des R-Linksmoduls M als eine Familie $\mathfrak{F}^M = \left(\mathcal{F}^M_\gamma\right)_{\gamma\in\Gamma}$ additiver Untergruppen von M mit den Eigenschaften

$$\begin{array}{lcl} \bigcup \mathfrak{F}^M & = & M \quad , \\ \gamma \preceq \gamma' & \Longleftrightarrow & \mathcal{F}^M_\gamma \subseteq \mathcal{F}^M_{\gamma'}, \\ \mathcal{F}_\gamma \mathcal{F}^M_{\gamma'} & \subseteq & \mathcal{F}^M_{\gamma\circ\gamma'} \end{array} \tag{4.8}$$

ein. Wir nennen $(M,\Gamma,\mathfrak{F}^M)$ eine *gefilterte* $(R,\Gamma,\mathfrak{F})$-*Linksmodulstruktur* und M einen *gefilterten* R-*Linksmodul*. Ersetzt man in (4.8) die dritte Bedingung durch

$$\mathcal{F}^M_{\gamma'} \mathcal{F}_\gamma \subseteq \mathcal{F}^M_{\gamma\circ\gamma'} \quad ,$$

so gelangt man zu den Begriffen der *gefilterten* $(R,\Gamma,\mathfrak{F})$-*Rechtsmodulstruktur* $(M,\Gamma,\mathfrak{F}^M)$ und des *gefilterten* R-*Rechtsmoduls* M.

Seien $(R,\Gamma,\mathfrak{F}_l)$ und $(R,\Gamma,\mathfrak{F}_r)$ zwei gefilterte Ringstrukturen von R und M ein R-Bimodul. Ist das Tripel $(M,\Gamma,\mathfrak{F}^M)$ sowohl gefilterte $(R,\Gamma,\mathfrak{F}_l)$-Linksmodulstruktur als auch gefilterte $(R,\Gamma,\mathfrak{F}_r)$-Rechtsmodulstruktur, so nennen wir es eine *gefilterte* $(R,\Gamma,\mathfrak{F}_l,\mathfrak{F}_r)$-*Bimodulstruktur* und M einen gefilterten R-Bimodul[4]. Auf die gleiche Weise kann man ausgehend von gegebenen Γ-Filtrierungen der Ringe R und S auch Γ-Filtrierungen einer Struktur M, welche R-Links- und S-Rechtsmodul ist, definieren. Wichtig ist dabei nur, daß den Filtrierungen aller beteiligten Strukturen das gleiche geordnete Monoid Γ zugrundeliegt.

Jede Γ-Filtrierung eines Ringes R ist gleichzeitig auch eine Γ-Filtrierung von R als R-Links-, R-Rechts- und R-Bimodul. Die Klasse der Modulfiltrierungen eines Ringes R ist im allgemeinen reichhaltiger als die Klasse seiner Ringfiltrierungen.

Definition 4.2 *Seien M ein R-Linksmodul, $(\Omega,\circ_\Omega,\prec_\Omega)$ und $(\Gamma,\circ_\Gamma,\prec_\Gamma)$ zwei geordnete Monoide und $(M,\Omega,\mathfrak{F}^{\Omega,M})$ eine Ω-Filtrierung sowie $(M,\Gamma,\mathfrak{F}^{\Gamma,M})$ eine Γ-Filtrierung von M.*

Falls es einen im schwachen Sinne ordnungsverträglichen Monoidepimorphismus $\tau:\Omega\to\Gamma$ gibt

$$(d.h.\ \forall\omega,\omega'\in\Omega\ :\ \omega\preceq_\Omega\omega' \Longrightarrow \tau(\omega)\preceq_\Gamma\tau(\omega') \quad), \tag{4.9}$$

so daß für alle $\gamma\in\Gamma$ die Gleichheit

$$\mathcal{F}^{\Gamma,M}_\gamma = \bigcup_{\omega\in\tau^{-1}(\gamma)} \mathcal{F}^{\Omega,M}_\omega$$

erfüllt ist, so nennen wir $(M,\Omega,\mathfrak{F}^{\Omega,M})$ eine Verfeinerung *von $(M,\Gamma,\mathfrak{F}^{\Gamma,M})$.*

[4]Sind die Bestimmungstücke der hier definierten Strukturen aus dem Kontext heraus klar, dann werden wir ihre Angabe verkürzen oder ganz darauf verzichten. So verwenden wir beispielsweise anstelle des Begriffs "gefilterte $(R,\Gamma,\mathfrak{F}_l,\mathfrak{F}_r)$-Bimodulstruktur" die Abkürzung "gefilterte R-Bimodulstruktur" oder noch kürzer "gefilterte Modulstruktur".

Ring- und Bimodulfiltrierungen sind als Spezialfall bereits erfaßt. Verfeinerungen von Rechtsmodulfiltrierungen erklärt man analog. Durch einfaches Nachrechnen überzeugt man sich von der Gültigkeit von

$$\forall \omega \in \Omega \; : \; \bigcup_{\gamma \prec \tau(\omega)} \mathcal{F}_\gamma^{\Gamma,M} \subseteq \mathcal{F}_\omega^{\Omega,M} \subseteq \mathcal{F}_{\tau(\omega)}^{\Gamma,M} \tag{4.10}$$

für eine beliebige Verfeinerung $(M, \Omega, \mathfrak{F}^{\Omega,M})$ von $(M, \Gamma, \mathfrak{F}^{\Gamma,M})$. Gilt in (4.10) für wenigstens ein $\omega \in \Omega$ auf keiner Seite die Gleichheit, so sprechen wir von einer *echten* Verfeinerung.

Sei $I \subseteq R$ ein ein- oder zweiseitiges Ideal des gefilterten Ringes R. Dann induziert $\mathfrak{F}$ durch $\mathcal{F}_\gamma^I = \mathcal{F}_\gamma \cap I$ in natürlicher Weise eine Filtrierung $\mathfrak{F}^I = \left(\mathcal{F}_\gamma^I\right)_{\gamma \in \Gamma}$ auf dem Unterring I von R. Daneben gibt es eine Klasse weiterer Γ-Filtrierungen, welche durch $\mathfrak{F}$ auf dem entsprechendseitigen R-Modul I induziert werden.

Sei I ein zweiseitiges Ideal von R und H ein Erzeugendensystem von I. Jedes Element $f \in I$ besitzt Darstellungen der Gestalt

$$f = \sum_{i=1}^{k} a_i h_i b_i \quad , \tag{4.11}$$

wobei $a_1, \ldots, a_k, b_1, \ldots, b_k \in R$ und $h_1, \ldots, h_k \in H$. Falls Monoidelemente $\gamma_1, \ldots, \gamma_k, \omega_1, \ldots, \omega_k, \tau_1, \ldots, \tau_k \in \Gamma$ existieren, so daß für alle $i = 1, \ldots, k$ die Beziehungen $a_i \in \mathcal{F}_{\gamma_i}$, $b_i \in \mathcal{F}_{\omega_i}$ und $h_i \in \mathcal{F}_{\tau_i}$ sowie $\gamma_i \circ \tau_i \circ \omega_i \preceq \gamma$ gelten, so wird die obige Darstellung eine γ-*Darstellung* von f bezüglich H genannt. Die Teilmenge $\mathcal{F}_\gamma^{(H)}$ aller Elemente von I, die eine γ-Darstellung bezüglich H besitzen, bildet eine additive Untergruppe von I. Darüberhinaus überzeugt man sich leicht davon, daß die Familie $\mathfrak{F}^{(H)} = \left(\mathcal{F}_\gamma^{(H)}\right)_{\gamma \in \Gamma}$ auch den Bedingungen (4.8) einer R-Linksmodulfiltrierung genügt. Ebenso handelt es sich um eine R-Rechtsmodul- sowie eine R-Bimodulfiltrierung. $\mathfrak{F}^{(H)}$ wird als die durch $\mathfrak{F}$ und das Erzeugendensystem H definierte *Gröbnerfiltrierung* des R-Bimoduls I bezeichnet.

Betrachten wir nun den Fall einseitiger Ideale I. Verlangt man in (4.11), daß alle b_i oder alle a_i gleich 1 sein müssen, so gelangt man zu der durch $\mathfrak{F}$ und H definierten Gröbnerfiltrierung $\mathfrak{F}^{(H)}$ des von H erzeugten Links- beziehungsweise Rechtsideals I.

Für jedes ein- oder zweiseitige Ideal $I \subseteq R$ und jedes Erzeugendensystem H von I gilt $\mathcal{F}_\gamma^{(H)} \subseteq \mathcal{F}_\gamma^I$ für alle $\gamma \in \Gamma$. Es besteht ein enger Zusammenhang zwischen den Gröbnerfiltrierungen und den in Kapitel 5 einzuführenden Gröbnerbasen. Insbesondere wird sich der Extremfall $\mathfrak{F}^I = \mathfrak{F}^{(H)}$ als zur Gröbnerbasiseigenschaft von H äquivalent erweisen (siehe Satz 5.4).

4.4 Graduierte Ringe

Seien Γ ein (nicht notwendigerweise geordnetes) Monoid, R ein Ring und $\mathfrak{R} = (R_\gamma)_{\gamma \in \Gamma}$ eine Familie additiver Untergruppen von R. Die Familie $\mathfrak{R}$ sei so

beschaffen, daß R als additive Gruppe direkte Summe der Untergruppen aus $\mathfrak{R}$ ist (d.h. $R = \bigoplus_{\gamma\in\Gamma} R_\gamma$) und daß bezüglich der Ringmultiplikation für alle $\gamma, \gamma' \in \Gamma$ die Inklusion

$$R_\gamma R_{\gamma'} \subseteq R_{\gamma\circ\gamma'} \tag{4.12}$$

erfüllt ist. Aus der Direktheit der Summe und Gleichung (4.12) folgt sofort $1 \in R_\epsilon$, wobei ϵ das neutrale Element des Monoids Γ ist. Wir definieren die *Gradfunktion* $\deg_\Gamma : \bigcup_{\gamma\in\Gamma} R_\gamma \to \hat{\Gamma}$ vermöge $\deg_\Gamma(0) = -\infty$ und $\deg_\Gamma(a) = \gamma$ für $0 \neq a \in R_\gamma$. Ein Element $a \in R$ heißt *homogen* vom Grad γ, falls $a \in R_\gamma$ gilt. Entsprechend dieser Definition ist 0 homogen von jedem Grad $\gamma \in \Gamma$, die Gradfunktion ordnet der Null jedoch formal das nicht zu Γ gehörige Element $-\infty$ zu.

Gibt es zu R eine Familie $\mathfrak{R}$ der oben beschriebenen Art, so nennen wir R einen Γ-*graduierten Ring*[5]. Aus der Definition eines graduierten Rings folgt unmittelbar, daß jedes Element $a \in R$ eine (bis auf die Reihenfolge der Summanden) eindeutige Zerlegung $a = a_{\gamma_1} + \cdots + a_{\gamma_k}$ in homogene Bestandteile besitzt, wobei für jedes $i = 1, \ldots, k$ die Beziehung $a_{\gamma_i} \in R_{\gamma_i} \setminus \{0\}$ gilt und die γ_i paarweise verschieden sind. Ein Ideal I von R wird *homogen* (oder *graduiert*) genannt, falls für alle $a \in I$ bereits jeder homogene Bestandteil a_{γ_i} von a zu I gehört. Es ist leicht einzusehen, daß ein Ideal von R genau dann homogen ist, wenn es ein Erzeugendensystem besitzt, welches nur aus homogenen Elementen besteht.

Seien R und S zwei Ringe und $\varphi : R \to S$ ein Ringhomomorphismus. Sind R und S außerdem Γ-graduierte Ringe und ist φ gradverträglich, das heißt für jedes homogene Element $a \in R$ vom Grad $\gamma \in \Gamma$ muß auch $\varphi(a)$ homogen vom Grad γ sein, dann nennen wir φ einen Homomorphismus der Γ-graduierten Ringe R und S.

Wenn wir in dieser Arbeit eine Gleichung in den Variablen $X_1, \ldots, X_n$ über einem graduierten Ring G als homogen bezeichnen, so bezieht sich das nicht auf die Gleichheit der Variablengrade aller Summanden, sondern eine derartige Gleichung wird *homogen* vom Grad γ genannt, falls jede Variable X_i nur homogene Elemente von einem vorgegebenen Grad γ_i annehmen darf und darüberhinaus die zulässigen Werte eines Summanden der Gleichung stets homogen vom Gesamtgrad γ sind.

Wir nennen R einen *effektiven graduierten Ring*, wenn R ein effektiver Ring und $\deg_\Gamma$ eine berechenbare Funktion sind und es eine berechenbare Funktion gibt, die die Elemente von R in ihre homogenen Bestandteile zerlegt.

4.5 Der assoziierte graduierte Ring

Seien Γ ein durch $\prec$ geordnetes Monoid mit neutralem Element ϵ, $\varphi : R \to \hat{\Gamma}$ eine Pseudobewertung und $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ die von φ induzierte Filtrierung von R. Wir setzen formal $\mathcal{F}_{-\infty} = \hat{\mathcal{F}}_{-\infty} = \{0\}$. Man überzeugt sich leicht davon,

[5]Wenn Γ aus dem Kontext heraus klar ist, wird häufig auf seine Angabe verzichtet.

daß die Vereinigung

$$\hat{\mathcal{F}}_\gamma = \bigcup_{\hat{\Gamma} \ni \gamma' \prec \gamma} \mathcal{F}_{\gamma'}$$

für jedes $\gamma \in \Gamma$ eine Untergruppe von $\mathcal{F}_\gamma$ ist. Die Faktorgruppen der additiven Gruppen $\mathcal{F}_\gamma$ nach ihren Untergruppen $\hat{\mathcal{F}}_\gamma$ werden wir mit

$$R_\gamma = \mathcal{F}_\gamma / \hat{\mathcal{F}}_\gamma \qquad (\gamma \in \Gamma)$$

bezeichnen. Vermöge

$$[a]_{\hat{\mathcal{F}}_\gamma} [b]_{\hat{\mathcal{F}}_\omega} := [ab]_{\hat{\mathcal{F}}_{\gamma \circ \omega}} \tag{4.13}$$

wird für beliebige Elemente $a \in \mathcal{F}_\gamma$ und $b \in \mathcal{F}_\omega$ eine multiplikative Verknüpfung der Restklassen $[a]_{\hat{\mathcal{F}}_\gamma} \in R_\gamma$ und $[b]_{\hat{\mathcal{F}}_\omega} \in R_\omega$ erklärt. Wegen (4.6) ist die rechte Seite der Gleichung wohldefiniert. Diese Verknüpfung homogener Elemente läßt sich auf eindeutige Weise zu einer assoziativen Ringmultiplikation auf der direkten Summe $G = \bigoplus_{\gamma \in \Gamma} R_\gamma$ fortsetzen und der dabei entstehende Ring G hat $[1]_{\hat{\mathcal{F}}_\epsilon}$ zum Einselement und ist Γ-graduiert. G wird *assoziierter graduierter Ring* des gefilterten Rings R genannt.

Zwischen dem gefilterten Ring R und seinem assoziierten graduierten Ring G besteht vermöge $\mathrm{in}(a) = [a]_{\hat{\mathcal{F}}_{\varphi(a)}}$ eine natürliche Abbildung $\mathrm{in} : R \to G$, welche jedem Element $a \in R$ ein homogenes Element $\mathrm{in}(a)$ vom Grade $\deg_\Gamma \mathrm{in}(a) = \varphi(a)$ zuordnet. Der Bildbereich der Funktion in ist gerade die Menge $\bigcup_{\gamma \in \Gamma} R_\gamma$ aller homogenen Elemente von G und das vollständige Urbild des Nullelementes von G besteht nur aus dem Nullelement von R. Wir nennen in die *Initialabbildung* von R und $\mathrm{in}(a)$ den *Initialterm* von a. Die Initialabbildung wird durch $\mathrm{in}(F) = \{ \mathrm{in}(f) \mid f \in F \}$ auf beliebige Teilmengen $F \subseteq R$ ausgedehnt. Das von $\mathrm{in}(F)$ erzeugte zweiseitige Ideal von G nennen wir das *Initialideal* von F und bezeichnen es mit $\mathrm{In}(F)$. Analog führen wir die Begriffe *Links-* ($\mathrm{LIn}(F)$) und *Rechtsinitialideal* ($\mathrm{RIn}(F)$) für das von $\mathrm{in}(F)$ erzeugte Links- beziehungsweise Rechtsideal des Ringes G ein.

In Anlehnung an [Ap92] nennen wir das Quadrupel $(R, \Gamma, \prec, \varphi)$ eine *graduierte Ringstruktur* (oder auch kurz *graduierte Struktur*). Im Gegensatz dazu bezeichnen Robbiano und Mora das Quintupel $(R, \Gamma, \varphi, G, \mathrm{in})$ als graduierte Struktur. Der Unterschied in der Auswahl der Bestimmungsstücke ist rein technischer Natur. Aufgrund der Redundanz der Information haben wir hier auf die Aufnahme des assoziierten graduierten Ringes und der Initialabbildung in das Tupel verzichtet. Gemäß unserer Konventionen ist die Ordnung $\prec$ bereits Bestandteil des geordneten Monoids Γ und brauchte daher eigentlich, ähnlich wie bei Robbiano oder Mora, nicht noch einmal explizit hervorgehoben zu werden. Das Loslösen der Ordnungs- von der Monoidbezeichnung erweist sich jedoch beim Variieren der Ordnung als vorteilhaft.

Kapitel 5

Gröbnerbasen in graduierten Strukturen

In der Vergangenheit hat sich der Begriff der Gröbnerbasis für solche Situationen durchgesetzt, in denen die Ordnung $\prec$ des Monoids Γ eine Wohlordnung ist. In diesem Fall bestimmt die Basis eine konfluente, noethersche Reduktionsrelation. Wenn man die Forderung nach der Wohlordnungseigenschaft von $\prec$ fallenläßt, so ist die Reduktionsrelation nicht mehr notwendigerweise noethersch. In derartigen Situationen ist der Terminus der Standardbasis gebräuchlicher.

Gibt es für den Ring R ein wohlgeordnetes Monoid Γ und eine Pseudobewertung $\varphi : R \to \hat{\Gamma}$, so kann man das Idealenthaltenseinsproblem grob gesprochen relativ zur Effektivität des durch φ gefilterten Ringes R, des assoziierten graduierten Ringes G und des geordneten Monoids Γ sowie der Lösbarkeit homogener, linearer Gleichungen im assoziierten graduierten Ring G lösen. Die Entwicklung von Gröbnerbasistheorien in gefilterten Ringen dieser Art nimmt einen breiten Raum in der Literatur ein. Darunter sind Arbeiten zu Polynomringen über Körpern (siehe [Bu65],[Bu85]), freien nichtkommutativen $\mathbb{K}$-Algebren (siehe [Ber78], [Mo86]), Einhüllenden von Liealgebren (siehe [ApL85], [ApL88]), Algebren von auflösbarem Typ (siehe [KW90]) und G-Algebren (siehe [Ap88], [Ap92]), um nur einige Beispiele zu nennen. Der in voller Allgemeinheit durch Robbiano und Mora entwickelte Kalkül wurde für den Spezialfall bewerteter Ringe unabhängig auch von Beckmann und Stückrad untersucht (siehe [BS90]).

Unsere Darstellung orientiert sich an Moras Arbeit [Mo88a]. Eine Reihe von Ergebnissen wird dabei einer Präzisierung unterzogen, insbesondere wird die Syzygientheorie des zweiseitigen Falls ausgebaut. Bei der praktischen Untersuchung von Idealen graduierter Strukturen mit kommutativem Bewertungsmonoid beschränkt sich Mora auf die Behandlung von Linksidealen. Auf diese Weise werden zweiseitige Syzygien vermieden und das Nichtnoetherschsein der zweiseitigen Syzygienmoduln umgangen. Dadurch fällt aber beispielsweise der Kandri-Rody/Weispfenningsche Ansatz (siehe [KW90]) zur Behandlung zweiseitiger Ideale aus dem Rahmen und es wird eine separate, nicht auf Syzygien fußende Behandlung erforderlich. Betrachtet man die obigen zweiseitigen Ideale entsprechend ihrer tatsächlichen Natur als zweiseitig, so findet sich die Kandri-Rody/Weispfenningsche Idee in natürlicher Weise in den Syzygien wieder. Der

Begriff der Trivialität einer Syzygie wird neu gefaßt und der Morasche Ansatz freier Bimoduln zur Behandlung zweiseitiger Syzygien durch die Ausführungen aus Kapitel 3 präzisiert. Dadurch gelangt man unter anderem zu der sehr schönen Eigenschaft, daß ein- und zweiseitige Ideale kommutativer Ringe gleich behandelt werden dürfen. Auch wird eine kleine Ungenauigkeit Moras beseitigt, denn Syzygien der Gestalt $ce - ec$, wobei c dem Zentrum des Ringes angehört und e ein erzeugendes Element des Moduls ist, blieben in [Mo88a] unberücksichtigt.

Darüberhinaus behandeln wir die bisher noch nicht in dieser Allgemeinheit untersuchten Fragestellungen reduzierter Gröbnerbasen in graduierten Strukturen und der Verallgemeinerbarkeit der Theorie auf ein- und zweiseitige Moduln. Außerdem werden wir nach Bedingungen fragen, unter denen Gröbnerbasen algorithmisch konstruiert werden können. Dabei werden große Klassen der bisher in der Literatur untersuchten Algebren und Ringe umfaßt. Weiterhin gelangt man zu wesentlich allgemeineren Situationen und erhält insbesondere die Möglichkeit, die klassischen Fälle zu kombinieren.

5.1 Ringe mit verallgemeinerten Gröbnerbasen

Es folgt eine Auflistung von Ringen, auf die sich die Theorie der Gröbnerbasen verallgemeinern läßt und die eine Filtrierung bezüglich eines wohlgeordneten Wertemonoids besitzen.

Polynomringe über Körpern Sei $R = \mathbb{K}[X_1, \ldots, X_n]$ der Polynomring über dem Körper $\mathbb{K}$ in den Unbestimmten $X = \{X_1, \ldots, X_n\}$. Weiterhin seien $\Gamma = T(X)$ das von X frei erzeugte kommutative Monoid und $\prec$ eine beliebige Monoidwohlordnung[1]. Die Pseudobewertung φ ordne jedem von Null verschiedenen Polynom f sein führendes Potenzprodukt $\mathrm{lpp}(f)$, das heißt das bezüglich $\prec$ größte in f mit von Null verschiedenem Koeffizienten vorkommende Potenzprodukt, zu. Der assoziierte graduierte Ring der graduierten Struktur ist isomorph zu R, die homogenen Ideale sind gerade die Monomideale. Sowohl Syzygienmodulberechnung als auch Entscheidbarkeit des Idealenthaltenseinsproblems sind für Monomideale wohlbekannt und sehr einfach ausführbar.

Freie $\mathbb{K}$-Algebren Sei $R = \mathbb{K}\langle X_1, \ldots, X_n\rangle$ die von $X = \{X_1, \ldots, X_n\}$ frei erzeugte $\mathbb{K}$-Algebra über dem Körper $\mathbb{K}$. Als Wertemonoid wählen wir das von X frei erzeugte nichtkommutative Monoid $\Gamma = S(X)$ mit einer zugehörigen Monoidwohlordnung $\prec$. $S(X)$ ist $\mathbb{K}$-Vektorraumbasis von R. Jedes Element $f \in R\backslash\{0\}$ kann daher auf eindeutige Weise als endliche Linearkombination von Elementen aus $S(X)$ dargestellt werden. Die Pseudobewertung φ weist jedem von Null verschiedenen Element $f \in R$ das bezüglich $\prec$ größte Basiselement aus $S(X)$ zu, welches mit Nichtnullkoeffizient in der Summendarstellung von f auftritt. Der assoziierte graduierte Ring ist isomorph zu R und die homogenen Ideale sind monomial. Die Entscheidbarkeit des Idealenthaltenseinsproblems homogener Ideale kann auf das Teilwortproblem für die freie Worthalbgruppe

[1] Für eine Charakterisierung derartiger Ordnungen verweisen wir auf Bemerkung 4.1 *i)*.

zurückgeführt werden. Die Lösung des Syzygienproblems beruht auf Bergmans Diamond-Lemma (siehe [Ber78]).

Algebren von auflösbarem Typ Analog zu den Polynomringen kann man Algebren von auflösbarem Typ behandeln (siehe [KW90]). Diese beispielsweise die Polynomringe und die Einhüllenden von Liealgebren umfassende Klasse von $\mathbb{K}$-Algebren zeichnet sich dadurch aus, daß jede derartige Algebra ein freies kommutatives Monoid $T(X)$ als $\mathbb{K}$-Vektorraumbasis hat. Man spricht daher auch von Poincaré-Birkhoff-Witt-Algebren. Eine Algebra R von auflösbarem Typ ist eine Faktoralgebra der Gestalt $R = \mathbb{K}\langle X_1, \ldots, X_n\rangle / J$. Das zweiseitige Ideal J hat ein Erzeugendensystem

$$\{X_i X_j + c_{i,j} X_j X_i + p_{i,j} \mid 1 \leq j < i \leq n, 0 \neq c_{i,j} \in \mathbb{K}, p_{i,j} \in \mathit{Span}(T(X))\}$$

und erfüllt $J \cap \mathit{Span}(T(X)) = \{0\}$. Dabei bezeichnet $\mathit{Span}(T(X))$ den von $T(X) \subseteq S(X)$ aufgespannten $\mathbb{K}$-Untervektorraum von $\mathbb{K}\langle X\rangle$, wobei die Mengeneinbettung $T(X) \subseteq S(X)$ in dem am Ende von Abschnitt 4.1 vereinbarten Sinne zu verstehen ist. Weiterhin muß es eine Monoidwohlordnung $\prec$ von $T(X)$ geben, so daß für alle $1 \leq j < i \leq n$ und alle in $p_{i,j}$ vorkommenden Terme t die Relation $t \prec X_j X_i$ gilt. Wir definieren die Abbildung φ, indem wir jedem Element $f \in R\backslash\{0\}$ den bezüglich $\prec$ größten Term zuordnen, der in seiner Darstellung als $T(X)$-Linearkombination mit Nichtnullkoeffizient vorkommt. Als Wertemonoid dient $(T(X), \prec)$. Gilt für alle $1 \leq j < i \leq n$ die Gleichheit $c_{i,j} = -1$, wie zum Beispiel im Fall von Polynomringen oder Einhüllenden von Liealgebren, dann ist der assoziierte graduierte Ring isomorph zum Polynomring $\mathbb{K}[X_1, \ldots, X_n]$. Andernfalls gilt auf jeden Fall noch, daß der assoziierte graduierte Ring, wie auch R selbst, nullteilerfrei und als $\mathbb{K}$-Vektorraum zum Polynomring isomorph ist. Aber es gibt dann auch $u, v \in T(X)$, so daß sich die Produkte uv und vu in einem Faktor aus $\mathbb{K}$ unterscheiden. Bei den weiteren Untersuchungen bringt das jedoch keine wesentlichen Probleme mit sich.

G-Algebren Abschließend wollen wir noch den in [Ap92] untersuchten Fall der G-Algebren betrachten. G-Algebren sind Verallgemeinerungen der Algebren von auflösbarem Typ, wobei die Forderung $J \cap \mathit{Span}(T(X)) = \{0\}$ fallengelassen wird. Dadurch wird $T(X)$ ein im allgemeinen linear abhängiges Erzeugendensystem der G-Algebra betrachtet als $\mathbb{K}$-Vektorraum. Dennoch kann man φ und $(\Gamma, \prec)$ auf die gleiche Weise definieren, wie wir es zuvor für Algebren von auflösbarem Typ getan haben. Erstmalig in unserer Beispielserie haben wir es mit einem nicht notwendigerweise bewerteten Ring zu tun. Infolgedessen geht die Nullteilerfreiheit des assoziierten graduierten Rings verloren. Das Idealenthaltenseinsproblem homogener Ideale des assoziierten graduierten Rings kann analog dem monomialer Polynomideale behandelt werden. Das Vorhandensein von Nullteilern hat Einfluß auf das Syzygienproblem homogener Ideale, eine Lösung findet man in [Ap88].

5.2 Gröbnerbasen von Idealen

In diesem Abschnitt betrachten wir eine graduierte Ringstruktur $(R, \Gamma, \prec, \varphi)$ mit einer Wohlordnung $\prec$. Mit G bezeichnen wir den zugehörigen assoziierten graduierten Ring von R und mit $\mathrm{in} : R \to G$ die Initialabbildung. $\mathrm{in}^* : G \to R$ sei eine beliebige Abbildung, die bezüglich der homogenen Elemente von G ein Schnitt von in ist, das heißt, für jedes homogene Element $a \in G$ gilt die Gleichheit $\mathrm{in}(\mathrm{in}^*(a)) = a$. In Zunkunft werden wir in^* kurz einen Schnitt von in nennen. Die Pseudobewertung φ induziert vermöge

$$a \prec_R b :\Longleftrightarrow \varphi(a) \prec \varphi(b) \tag{5.1}$$

eine partielle Ordnung $\prec_R$ auf dem Ring R. Aufgrund der Wohlordnungseigenschaft von $\prec$ besitzt jede nicht leere Teilmenge von R bezüglich $\prec_R$ minimale Elemente, $\prec_R$ ist also eine noethersche Halbordnung. $\prec_R$ wird uns als Simplifikationshalbordnung für Restklassenringe von R dienen. Im allgemeinen besitzt eine Restklasse modulo eines gegebenen Ideals I wohl minimale, aber kein kleinstes Element bezüglich $\prec_R$. In solch einem Falle kann es keinen kanonischen Simplifikator von R/I bezüglich $\prec_R$ geben. Die Restklasse I hat stets 0 als kleinstes Element, was wenigstens die Chancen auf einen Nullsimplifikator bezüglich $\prec_R$ erhält. Weiterhin läßt sich $\prec_R$ im Falle der Existenz eines Nullsimplifikators so verfeinern, daß es einen kanonischen Simplifikator bezüglich der Verfeinerung gibt.

Wir schwächen die Forderungen an die Divisionsformel (3.1) dahingehend ab, daß anstelle von $\hat{a} = \hat{b} \Longleftrightarrow a - b \in I$ nur noch $\hat{a} = 0 \Longleftrightarrow a \in I$ verlangt wird. Falls es uns gelingt, einen Algorithmus zur Berechnung der Bestandteile solch einer abgeschwächten Divisionsformel zu finden, so liefert $a \mapsto \hat{a}$ einen Nullsimplifikator für R/I bezüglich $\prec_R$.

Bei der Konstruktion derartiger schwacher Divisionsalgorithmen nutzen wir die durch φ gefilterte Struktur von R aus, indem wir nach Erzeugendensystemen F fragen, für die in der Folge der Zwischensummen

$$a, a - g_1 f_1 h_1, \ldots, \hat{a} = a - \sum_{i=1}^{k} g_i f_i h_i \tag{5.2}$$

niemals ein Element vor einem in der Halbordnung $\prec_R$ größeren Element auftritt. Zusätzlich fordern wir die Gültigkeit von

$$\varphi(g_i) \circ \varphi(f_i) \circ \varphi(h_i) \preceq \varphi(a) \quad (i = 1, \ldots, k) \; . \tag{5.3}$$

Für Bewertungen φ folgt die Gültigkeit von (5.3) bereits aus Bedingung (5.2). Im allgemeinen Fall bewirkt (5.3) jedoch eine echte Einschränkung der zulässigen Folgen. Sei $L = \{1 \leq i \leq k \mid \varphi(g_i) \circ \varphi(f_i) \circ \varphi(h_i) = \varphi(a)\}$ die Menge aller Indizes an denen in (5.3) die Gleichheit gilt. Liegt für F ein Nullsimplifikator mit den geforderten Eigenschaften vor, so ist die Menge L für kein von Null verschiedenes Element a des von F erzeugten Ideals I leer und das Element

$$H := \mathrm{in}(a) - \sum_{i \in L} \mathrm{in}(g_i)\, \mathrm{in}(f_i)\, \mathrm{in}(h_i)$$

ist homogen vom Grade $\varphi(a)$. Außerdem sind die Elemente $a - \sum_{i\in L} g_i f_i h_i$ und $\hat{a}$ der abelschen Gruppe $\mathcal{F}_{\varphi(a)}$ modulo der Untergruppe $\hat{\mathcal{F}}_{\varphi(a)}$ zueinander kongruent und wegen $\hat{a} = 0$ folgt schließlich $H = [0]_{\hat{\mathcal{F}}_{\varphi(a)}} = 0$.

Damit der Rest modulo des Erzeugendensystems F von I einen Nullsimplifikator liefern kann, muß demnach notwendigerweise die Bedingung $\mathrm{In}(I) \subseteq \mathrm{In}(F)$, was offensichtlich äquivalent zur Gleichheit $\mathrm{In}(I) = \mathrm{In}(F)$ ist, gelten. Betrachten wir nun den umgekehrten Fall und nehmen an, uns ist ein $\mathrm{In}(I) = \mathrm{In}(F)$ erfüllendes, endliches Erzeugendensystem F von I gegeben. Wir geben einen relativ zur Effektivität des gefilterten Ringes R, zur Effektivität des graduierten Ringes G, zur Berechenbarkeit der Funktionen in und in^* sowie zur Entscheidbarkeit des Idealenthaltenseinsproblems des graduierten Ringes G berechenbaren schwachen Divisionsalgorithmus modulo F an, welcher einen Nullsimplifikator für R/I bezüglich $\prec_R$ liefert.

Aufruf: $(g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a}, j_1, \ldots, j_k) := \textsc{Div}_R(a, F)$
Eingaben: $a \in R$
$F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Ideals I, wobei $\mathrm{In}(I) = \mathrm{In}(F)$
Ausgaben: $g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a} \in R$, $1 \le j_1, \ldots, j_k \le m$, so daß (5.2), (5.3) und $a = \sum_{i=1}^{k} g_i f_{j_i} h_i + \hat{a}$ erfüllt sind und $\hat{a} = 0$ oder $\mathrm{in}(\hat{a}) \notin \mathrm{In}(F)$ gilt.

$\hat{a} := a$, $k := 0$
$(p_1, \ldots, p_l, q_1, \ldots, q_l, A, r_1, \ldots, r_l) := \textsc{Divide}_G(\mathrm{in}(\hat{a}), \mathrm{in}(F))$
while $A = 0$ **do**
  $g_{k+i} := \mathrm{in}^*(p_i)$, $h_{k+i} := \mathrm{in}^*(q_i)$, $j_{k+i} := r_i \quad (i = 1, \ldots, l)$
  $\hat{a} := \hat{a} - \sum_{i=1}^{l} g_{k+i} f_{j_{k+i}} h_{k+i}$
  k:=k+l
  $(p_1, \ldots, p_l, q_1, \ldots, q_l, A, r_1, \ldots, r_l) := \textsc{Divide}_G(\mathrm{in}(\hat{a}), \mathrm{in}(F))$
return$(g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a}, j_1, \ldots, j_k)$

Dabei genügt die innerhalb von $\textsc{Div}_R$ gerufene Funktion $\textsc{Divide}_G$ der Spezifikation:
Aufruf: $(p_1, \ldots, p_l, q_1, \ldots, q_l, A, r_1, \ldots, r_l) := \textsc{Divide}_G(a, H)$
Eingaben: a homogenes Element von G
$H = \{h_1, \ldots, h_m\}$ endliche Menge homogener Elemente von G.
Ausgaben: $p_1, \ldots, p_l, q_1, \ldots, q_l, A \in G$ homogene Elemente, $1 \le r_1, \ldots, r_l \le m$, so daß $\deg_\Gamma(p_i) \circ \deg_\Gamma(h_{r_i}) \circ \deg_\Gamma(q_i) = \deg_\Gamma(a)$, $a = \sum_{i=1}^{l} p_i h_{r_i} q_i + A$ und $A = 0 \iff a \in G(H)G$

Beweis der Korrektheit und Termination von $\textsc{Div}_R$:
Ist G ein effektiver graduierter Ring mit entscheidbarem Idealenthaltenseinsproblem, so existiert eine den Spezifikationen von $\textsc{Divide}_G$ genügende berechenbare Funktion. Die Effektivität von R und die Berechenbarkeit der Funktionen in und in^* sichern ab, daß auch alle anderen Anweisungen von $\textsc{Div}_R$ algorithmisch ausführbar sind. Weiterhin überzeugt man sich schnell davon, daß die Abarbeitung der Anweisungsfolge bei Eingabe (F, a) im Falle der Termination ein korrektes Ergebnis liefert. Bei jedem Durchlauf der **while**-Schleife verkleinert

sich der Grad von $\mathrm{in}(\hat{a})$. Aufgrund der Wohlordnungseigenschaft von $\prec$ kann die Schleife daher nur endlich oft durchlaufen werden und somit ist schließlich auch die Termination nachgewiesen. □

Wir führen einen Algorithmus $\textsc{Divide}_R$ mit der gleichen Anweisungsfolge wie $\textsc{Div}_R$ und der allgemeineren Spezifikation

Aufruf: $(g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a}, j_1, \ldots, j_k) := \textsc{Divide}_R(a, F)$
Eingaben: $a \in R$,
$F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Ideals I
Ausgaben: $g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a} \in R$, $1 \leq j_1, \ldots, j_k \leq m$, so daß (5.2), (5.3) und $a = \sum_{i=1}^{k} g_i f_{j_i} h_i + \hat{a}$ erfüllt sind und $\hat{a} = 0$ oder $\mathrm{in}(\hat{a}) \notin \mathrm{In}(F)$ gilt.

ein. Korrektheits- und Terminationsbeweis für $\textsc{Divide}_R$ verlaufen in völliger Analogie zu $\textsc{Div}_R$. Die durch $\textsc{Divide}_R$ vermittelte Abbildung $a \mapsto \hat{a}$ ist genau dann ein Nullsimplifikator für R/I bezüglich $\prec_R$, wenn $\mathrm{In}(F) = \mathrm{In}(I)$ gilt. Die vorangegangenen Untersuchungen belegen die Bedeutung von Erzeugendensystemen F eines Ideals I mit der Eigenschaft $\mathrm{In}(F) = \mathrm{In}(I)$ für die Entscheidbarkeit des Idealenthaltenseinsproblems pseudobewerteter Ringe. Wir definieren:

Definition 5.1 *Sei I ein zweiseitiges (Links-, Rechts-) Ideal des Ringes R. Ein Erzeugendensystem F von I wird eine* Gröbnerbasis von I bezüglich $(R, \Gamma, \prec, \varphi)$ *genannt, falls die Menge* $\mathrm{in}(F)$ *das zweiseitige (Links-, Rechts-) Initialideal von I erzeugt, d.h.* $\mathrm{In}(F) = \mathrm{In}(I)$ ($\mathrm{LIn}(F) = \mathrm{LIn}(I)$, $\mathrm{RIn}(F) = \mathrm{RIn}(I)$).

Die Existenz von Gröbnerbasen ist trivial, denn mit Sicherheit ist immer $F = I$ geeignet. Bisher stellt die obige Definition zwei Forderungen an F: die Menge muß I erzeugen und darüberhinaus müssen ihre Initialterme das Initialideal erzeugen. Der folgende Satz belegt, daß die zweite Forderung bereits allein ausreicht, um eine Teilmenge von I als Gröbnerbasis auszuzeichnen.

Satz 5.2 *Sei I ein zweiseitiges (Links-, Rechts-) Ideal von R und $F \subseteq I$ eine Teilmenge mit der Eigenschaft, daß* $\mathrm{in}(F)$ *das zweiseitige (Links-, Rechts-) Initialideal* $\mathrm{In}(I)$ *(* $\mathrm{LIn}(I)$, $\mathrm{RIn}(I)$*) von I erzeugt. Dann ist F ein Erzeugendensystem von I.*

Beweis: Wir betrachten den Fall eines Linksideals I. Das von F erzeugte Linksideal J von R ist trivialerweise in I enthalten. Angenommen, die Menge $I \backslash J$ ist nicht leer, dann existiert ein bezüglich $\prec_R$ minimales Element a dieser Menge. Nach Voraussetzung läßt sich der Initialterm von a als homogene Linkskombination der Initialterme der Elemente von F darstellen, d.h. es existieren homogene Elemente $h_f \in G$ mit $\mathrm{in}(a) = \sum_{f \in F} h_f \, \mathrm{in}(f)$ und $\deg_\Gamma(h_f) \circ \varphi(f) = \varphi(a)$ für alle $f \in F$ mit $h_f \neq 0$. Wir wählen beliebige Elemente $b_f \in R$ mit $\mathrm{in}(b_f) = h_f$. Offensichtlich gilt $a' = a - \sum_{f \in F} b_f f \in I \backslash J$ und $\varphi(a') \prec \varphi(a)$ im Widerspruch zur Konstruktion von a. Folglich ist $I \backslash J$ leer und F erzeugt I.

Im Fall eines zweiseitigen oder eines Rechtsideals I verläuft der Beweis völlig analog. □

Folgerung 5.3 *Erfüllt der assoziierte graduierte Ring G die aufsteigende Kettenbedingung für Links-, Rechts- beziehungsweise zweiseitige Ideale, so trifft gleiches auch auf den gefilterten Ring R zu und jedes Ideal der entsprechenden Seitigkeit von R besitzt eine endliche Gröbnerbasis.*

Der Beweis ist offensichtlich, denn nach dem obigen Satz zieht die Existenz eines endlichen Erzeugendensystems des Initialideals von I die Existenz eines solchen für I selbst nach sich, wobei letzteres sogar Gröbnerbasis ist.

An dieser Stelle sei bemerkt, daß bei Betrachtung von graduierten Strukturen bezüglich nicht wohlgeordneter Monoide im allgemeinen weder Satz noch Folgerung übertragbar sind.

Fassen wir die bisher erzielten Resultate zusammen: Ist $(R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur, wobei $\prec$ Wohlordnung ist, der gefilterte Ring R und sein assoziierter graduierter Ring G effektiv sind, die Initialabbildung in und ein zugehöriger Schnitt in^* berechenbare Funktionen sind und das Idealenthaltenseinsproblem des graduierten Rings G entscheidbar ist, dann ist das Idealenthaltenseinsproblem für durch endliche Gröbnerbasen gegebene Ideale von R entscheidbar.

Wenngleich wir nachgewiesen haben, daß jedes Ideal von R, dessen Initialideal endlich erzeugt ist, eine endliche Gröbnerbasis besitzt, so stellt doch die Forderung, Ideale durch endliche Gröbnerbasen angeben zu müssen, erst einmal eine erhebliche Einschränkung dar. Ist der assoziierte graduierte Ring G noethersch, so gibt es eine Funktion $\textsc{Groebner} : Fin(R) \to Fin(R)$, die jeder endlichen Teilmenge $F \subset R$ eine das gleiche Ideal erzeugende endliche Gröbnerbasis $\textsc{Groebner}(F) \subset R$ zuordnet. Diese Funktion Groebner ist relativ zu einer Gröbnerbasistestfunktion $\textsc{GbTest} : Fin(R) \to R$ berechenbar.

Aufruf: $H := \textsc{Groebner}(F)$
Eingaben: $F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Ideals I.
Ausgaben: $H = \{h_1, \ldots, h_l\}$ Gröbnerbasis von I.

$H := F$
$a := \textsc{GbTest}(H)$
while $a \neq 0$ **do**
    $H := H \cup \{a\}$
    $a := \textsc{GbTest}(H)$
return(H)

Aufruf: $a := \textsc{GbTest}(F)$
Eingaben: $F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Ideals I.
Ausgaben: $a \in I$, wobei $a = 0$ falls F Gröbnerbasis von I ist und
$\mathrm{in}(a) \notin \mathrm{In}(F)$ sonst.

Die Korrektheit des Algorithmus Groebner folgt unmittelbar aus der Spezifikation von GbTest. Bei jedem Durchlauf der **while**-Schleife wird das Initialideal $\mathrm{In}(H)$ echt größer, was aufgrund des Noetherschseins von G nur endlich

oft passieren kann. Damit ist die Termination nachgewiesen. Die Hauptschwierigkeit besteht schließlich im Finden einer berechenbaren Funktion GbTest, welche den obigen Spezifikationen genügt. Betrachten wir dazu die folgende Anweisungsfolge:

$S :=$ Nontriv(in(F))
while $S \neq \emptyset$ **do**
    Wähle $s \in S$, $S := S \backslash \{s\}$
    $(g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a}, j_1, \ldots, j_k) :=$ Divide$_R$(Lift(s), F)
    if $\hat{a} \neq 0$ **then return**($\hat{a}$)
return(0)

Jede homogene zweiseitige Syzygie s von in(F) vom Grad γ hat die Gestalt $s = \sum_{j=1}^{k} h_j e_{i_j} g_j$, wobei $\sum h_j \text{ in}(f_{i_j}) g_j = 0$ gilt, $h_1, \ldots, h_k, g_1, \ldots, g_k$ homogene Elemente von G und f_{i_j} Elemente von F sind sowie $\deg_\Gamma(h_j) \circ \varphi(f_{i_j}) \circ \deg_\Gamma(g_j) = \gamma$ für alle $j = 1, \ldots, k$ erfüllt ist. Die Funktion Lift weist der Syzygie s vermöge

$$\text{Lift}(s) = \text{Lift}\left(\sum_{j=1}^{k} h_j e_{i_j} g_j\right) = \sum_{j=1}^{k} \text{in}^*(h_j) f_{i_j} \text{ in}^*(g_j)$$

ein Element von R zu. Die gerufene Funktion Nontriv genügt der Spezifikation

Aufruf: $S :=$ Nontriv(H)
Eingaben: $H = \{h_1, \ldots, h_m\}$ Menge[2] homogener Elemente von G.
Ausgaben: S endliche Menge homogener Syzygien,
wobei $S \cup \text{Triv}(H)$ den Syzygienmodul $Syz(H)$ erzeugt.

Triv ist eine Funktion, die jeder endlichen Menge $H = \{h_1, \ldots, h_m\}$ homogener Elemente von G eine Menge homogener Syzygien zuordnet. Die Menge Triv(H) braucht nicht notwendigerweise endlich zu sein, es wird auch nicht die Berechenbarkeit von Triv gefordert. Wichtig ist nur, daß die Mengen $S =$ Nontriv(H) und Triv(H) die folgende Kompatibilitätsbedingung erfüllen. Eine Syzygie $s \in \text{Triv}(H)$ hat in dem Sinne trivial zu sein, daß für beliebige Elemente $F = \{f_1, \ldots, f_m\}$ mit in$(f_i) = h_i$, $i = 1, \ldots, m$, aus der Gültigkeit von Lift$(s') \in \hat{\mathcal{F}}^{(F)}_{\deg_\Gamma(s')}$ für alle $s' \in$ Nontriv(H) auch die Gültigkeit von Lift$(s) \in \hat{\mathcal{F}}^{(F)}_{\deg_\Gamma(s)}$ folgt. Die Mengen $\hat{\mathcal{F}}^{(F)}_{\gamma}$ beziehen sich auf die durch F definierte Gröbnerfiltrierung von I. In jedem Fall sind Moras Syzygien der Menge $Triv(H) = \{h_i w e_j - e_i w h_j \mid 1 \leq i, j \leq m \wedge w \in G \text{ homogen}\}$ trivial, denn jedes $s = h_i w e_j - e_i w h_j \in Triv(H)$ erfüllt die Bedingungen $f_i \text{ in}^*(w) f_j - f_i \text{ in}^*(w) f_j = 0$, $\varphi(\text{in}^*(w h_j) - \text{in}^*(w) f_j) \prec \deg_\Gamma(w) \circ \deg_\Gamma h_j$ und $\varphi(\text{in}^*(h_i w) - f_i \text{ in}^*(w)) \prec \deg_\Gamma(h_i) \circ \deg_\Gamma(w)$ und somit auch Lift$(s) \in \hat{\mathcal{F}}^{(F)}_{\deg_\Gamma(s)}$. Die Moraschen Syzygien weisen die Besonderheit auf, daß ihre Trivialität gar keinen Bezug auf die Syzygien aus Nontriv(H) benötigt. Ebenso

[2] Wir erinnern an die auf Seite 40 getroffene Vereinbarung und weisen darauf hin, daß H genau genommen als geordnetes Tupel aufgefaßt wird.

verhält es sich bei einer weiteren Klasse trivialer Syzygien. Per definitionem ist der Syzygienmodul $Syz(H)$ ein Untermodul des G-Bimoduls $(G \otimes_U G)^{|H|}$, wobei das Tensorprodukt über den vom Einselement erzeugten Unterring U von G gebildet wird. Sei $Z(R) \subseteq R$ das Zentrum von R. Dann erzeugen die Initialterme der Elemente von $Z(R)$ einen Unterring $Q \subseteq Z(G)$ des Zentrums von G. Der Kern $ker(\iota_Q)$ des durch $e_i \mapsto e_i$ erklärten natürlichen Homomorphismus $\iota_Q : (G \otimes_U G)^{|H|} \to (G \otimes_Q G)^{|H|}$ ist ein homogener Untermodul des Syzygienmoduls $Syz(H)$. $ker(\iota_Q)$ wird von allen Elementen der Bauart $\alpha e_i - e_i \alpha$ mit $\alpha \in \text{ in}(Z(R))$ erzeugt. Jedes dieser Elemente erfüllt offensichtlich die Anforderungen einer trivialen Syzygie und anstelle des Syzygienmoduls $Syz(H)$ kann auf den Faktormodul $Syz(H)/ker(\iota_Q)$ Bezug genommen werden. Insbesondere bewirkt dieses Vorgehen die erwartete Äquivalenz der Algorithmen zur Behandlung zwei- und einseitiger Ideale eines kommutativen Ringes R.

Darüberhinaus kann man auch jede aufgrund eines Kriteriums überflüssige Syzygie (siehe [Bu85]) als trivial ansehen. In diesem Sinne ist der Ausschluß trivialer Syzygien auch im einseitigen Fall sinnvoll. Aber während es sich in den in der Literatur betrachteten einseitigen Fällen immer nur um endliche Mengen trivialer Syzygien handelt, deren Aussonderung rein technischer Natur ist, gibt es interessante zweiseitige Fälle mit unendlichen Mengen trivialer Syzygien, deren a priori Ausschluß grundlegende Bedeutung für die Termination des Algorithmus besitzt.

Dem Korrektheitsbeweis des Gröbnerbasistestalgorithmus stellen wir den im Abschnitt über Gröbnergraduierungen bereits angedeuteten Satz voran.

Satz 5.4 *Sei I ein zweiseitiges (Links-, Rechts-) Ideal von R und $H \subseteq I$ ein Erzeugendensystem davon. Sei $\mathfrak{F}^I$ die Filtrierung von I, welche sich durch Einschränkung der durch φ auf R definierten Filtrierung $\mathfrak{F}$ ergibt. Weiterhin sei $\mathfrak{F}^{(H)}$ die durch $\mathfrak{F}$ und H definierte Gröbnerfiltrierung des zweiseitigen (Links-, Rechts-) R-Moduls I. H ist genau dann eine Gröbnerbasis von I, wenn $\mathfrak{F}^I = \mathfrak{F}^{(H)}$ gilt.*

Beweis: Wir beschränken uns auf den Fall eines zweiseitigen Ideals I. Im einseitigen Fall vereinfacht sich der Beweis etwas und verläuft ansonsten völlig analog.

($\Longrightarrow$) Sei H eine Gröbnerbasis von I. Dann liefert Algorithmus DIVIDE$_R$ angewandt auf $a \in I$ und H eine $\varphi(a)$-Darstellung von a bezüglich H und es folgt $\mathfrak{F}^I = \mathfrak{F}^{(H)}$.

($\Longleftarrow$) Setzen wir nun die Gleichheit $\mathfrak{F}^I = \mathfrak{F}^{(H)}$ voraus. Sei $a \in I$ beliebig. Wegen $a \in \mathcal{F}^{(H)}_{\varphi(a)}$ existieren Elemente $b_i, c_i \in R$ und $h_i \in H$, so daß $a = \sum_{i=1}^{k} b_i h_i c_i$ eine $\varphi(a)$-Darstellung von a bezüglich H ist. Aus den Eigenschaften einer γ-Darstellung ergibt sich $\varphi(b_i) \circ \varphi(h_i) \circ \varphi(c_i) \preceq \varphi(a)$ und o.B.d.A. können wir annehmen, daß dabei genau für $i = 1, \ldots, l$ die Gleichheit vorliegt. Es folgt

$$\varphi\left(a - \sum_{i=1}^{l} b_i h_i c_i\right) \prec \varphi(a)$$

und durch Übergang zu den Restklassen modulo der Untergruppe $\hat{\mathcal{F}}_{\varphi(a)}$ gelangen wir zu:

$$0 = \left[a - \sum_{i=1}^{l} b_i h_i c_i \right]_{\hat{\mathcal{F}}_{\varphi(a)}} = \mathrm{in}(a) - \sum_{i=1}^{l} \mathrm{in}(b_i)\,\mathrm{in}(h_i)\,\mathrm{in}(c_i) \quad ,$$

womit schließlich $\mathrm{In}(I) \subseteq \mathrm{In}(H)$ nachgewiesen ist, also ist H eine Gröbnerbasis von I. □

Korrektheitsbeweis für Algorithmus GbTest: Angenommen, die Abarbeitung von GbTest stoppt mit Ausgabe des von Null verschiedenen Rests a der Division von Lift(s) modulo F. Es gilt Lift$(s), a \in I$ und $\mathrm{in}(a) \notin \mathrm{In}(F)$. Folglich ist F keine Gröbnerbasis und das Resultat entspricht der Spezifikation von GbTest.

Halte die Abarbeitung von GbTest bei Eingabe F mit dem Resultat 0 an. Sei $\mathfrak{F}^{(F)}$ die Gröbnerfiltrierung von I bezüglich des Erzeugendensystems F. Wie üblich bezeichnen wir die Untergruppe $\bigcup_{\gamma' \prec \gamma} \mathcal{F}^{(F)}_{\gamma'}$ von $\mathcal{F}^{(F)}_{\gamma}$ für jedes $\gamma \in \Gamma$ mit $\hat{\mathcal{F}}^{(F)}_{\gamma}$.

Angenommen, F ist keine Gröbnerbasis von I. Dann gibt es nach Satz 5.4 ein $\gamma \in \Gamma$ mit $\mathcal{F}^{(F)}_{\gamma} \subsetneqq \mathcal{F}^{I}_{\gamma}$. Sei $h \in \mathcal{F}^{I}_{\gamma} \backslash \mathcal{F}^{(F)}_{\gamma}$ und τ minimal mit der Eigenschaft $h \in \mathcal{F}^{(F)}_{\tau}$. Wir betrachten eine beliebige τ-Darstellung $h = \sum_{j=1}^{k} a_j f_{i_j} b_j$, wobei $a_j, b_j \in R$ und $f_{i_j} \in F$, von h bezüglich F. O.B.d.A. gelte genau für $j = 1, \ldots, l$ die Gleichheit $\varphi(a_j) \circ \varphi(f_{i_j}) \circ \varphi(b_j) = \tau$. Es folgt $\sum_{j=1}^{l} \mathrm{in}(a_j)\,\mathrm{in}(f_{i_j})\,\mathrm{in}(b_j) = 0$, was bedeutet, daß $t := \sum_{j=1}^{l} \mathrm{in}(a_j) e_{i_j} \mathrm{in}(b_j)$ eine homogene Syzygie von $\mathrm{in}(F)$ vom Grad τ ist. Demnach existieren homogene Syzygien $s_1, \ldots, s_n \in S$ und homogene Elemente $p_1, \ldots, p_n, q_1, \ldots, q_n \in G$ mit $\deg_\Gamma(p_i) \circ \deg_\Gamma(s_i) \circ \deg_\Gamma(q_i) = \tau$ für alle $i = 1, \ldots, n$, so daß $t = \sum_{i=1}^{n} p_i s_i q_i$ gilt. Betrachten wir nun das Element

$$h' := h - \sum_{i=1}^{n} \mathrm{in}^*(p_i)\mathrm{Lift}(s_i)\,\mathrm{in}^*(q_i) \in I \quad .$$

Zum einen erkennt man die Enthaltenseinsrelation $h' \in \hat{\mathcal{F}}^{(F)}_{\tau}$ und zum anderen garantiert Algorithmus GbTest die Beziehung Lift$(s_i) \in \hat{\mathcal{F}}^{(F)}_{\deg_\Gamma(s_i)}$ für jede der Syzygien s_i. Damit erhalten wir $h \in \hat{\mathcal{F}}^{(F)}_{\tau}$. Das steht im Widerspruch zur vorausgesetzten Minimalität von τ. Folglich gilt die Gleichheit $\mathfrak{F}^I = \mathfrak{F}^{(F)}$ und nach Satz 5.4 ist F eine Gröbnerbasis von I. □

Terminationsdiskussion für Algorithmus GbTest: Die Abarbeitung hält nur dann immer an, wenn es eine Funktion gibt, die zu beliebigem endlichem $\mathrm{in}(F)$ in endlicher Zeit eine endliche Menge S berechnet. Im Falle der Berechenbarkeit einer rekursiv aufzählbaren Menge S würde wenigstens noch die Semientscheidbarkeit der Frage nach dem Nichtvorliegen einer Gröbnerbasis erzielt. □

Zusammenfassend haben wir folgendes gezeigt:

Satz 5.5 *Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit Wohlordnung $\prec$ und noetherschem assoziierten graduierten Ring G. Dann ist das Idealenthaltenseinsproblem des noetherschen Rings R relativ zur Effektivität des gefilterten Rings R und des graduierten Rings G, zur Berechenbarkeit der Funktionen* in *und* in^**, zur Entscheidbarkeit des Idealenthaltenseinsproblems endlich erzeugter homogener Ideale des graduierten Rings G und der algorithmischen Lösbarkeit des* TRIV*-Syzygienproblems endlich erzeugter homogener Ideale von G berechenbar.*

Dann nennen wir $\mathfrak{R}$ aufgrund des obigen Satzes eine *effektive graduierte Gröbnerstruktur* (oder auch kurz effektive Gröbnerstruktur), wenn sie folgende Eigenschaften hat:

i) $(\Gamma, \prec)$ ist effektives wohlgeordnetes Monoid,

ii) R ist effektiver Γ-gefilterter Ring,

iii) G ist effektiver Γ-graduierter Ring und noethersch,

iv) die Funktionen in und in^* sind berechenbar,

v) das Idealenthaltenseinsproblem des noetherschen graduierten Rings G ist entscheidbar und

vi) es existiert eine Funktion TRIV, die jeder endlichen Menge homogener Elemente von G eine Menge trivialer Syzygien zuordnet, so daß das TRIV-Syzygienproblem des noetherschen graduierten Rings G lösbar ist.

Ersetzt man *v)* und *vi)* durch die entsprechenden Bedingungen für homogene Links- beziehungsweise Rechtsideale, dann gelangt man zu den Begriffen der *effektiven (graduierten) Linksgröbnerstruktur* und der *effektiven (graduierten) Rechtsgröbnerstruktur.*

Bei der Darstellung der Algorithmen haben wir uns ganz auf den Fall zweiseitiger Ideale konzentriert. Die Algorithmen können nahezu unverändert auf einseitige Ideale übertragen werden. Es ist nur notwendig, DIVIDE_R dahingehend abzuändern, daß die entsprechende Division DIVIDE_G modulo einseitiger homogener Ideale des assoziierten graduierten Rings zum Einsatz kommt. GBTEST muß dann die modifizierte Funktion DIVIDE_R benutzen und für S ein endliches Erzeugendensystem des entsprechenden einseitigen Syzygienmoduls berechnen. Auf triviale Syzygien kann ganz verzichtet werden. Es gilt:

Satz 5.6 *Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine effektive graduierte (Links-) Rechtsgröbnerstruktur. Dann ist das Enthaltenseinsproblem endlich erzeugter (Links-) Rechtsideale von R entscheidbar.*

In den beiden vorangegangenen Sätzen war jeweils vorausgesetzt worden, daß der assoziierte graduierte Ring noethersch sein soll und diese Eigenschaft überträgt sich dann auch auf R. In den meisten in der Literatur untersuchten Situationen ist diese Forderung erfüllt. Eine Ausnahme stellt Moras Theorie freier $\mathbb{K}$-Algebren dar. Im Fall eines nicht notwendigerweise noetherschen assoziierten graduierten Rings kann wenigstens noch die Semientscheidbarkeit des

Enthaltenseinsproblems endlich erzeugter ein- oder zweiseitiger Ideale gezeigt werden. Ist R selbst ein in geeigneter Weise graduierter Ring, so ist darüberhinaus das Enthaltenseinsproblem endlich erzeugter ein- oder zweiseitiger homogener Ideale entscheidbar. Einen leicht auf die hier betrachtete Situation übertragbaren Beweis dieser Aussagen werden wir später für Satz 5.31 im Kontext der Gröbnerbasen von R-Bimoduln führen. Dort wäre eine Beschränkung auf noethersche assoziierte graduierte Bimoduln viel zu streng.

Sei $s = \sum_{j=1}^{l} u_j e_{i_j} v_j$ eine homogene Syzygie von $\mathrm{in}(F)$. Betrachten wir nun die Division von $\textsc{Lift}(s)$ modulo F mit Hilfe von Algorithmus $\textsc{Divide}_R$. Dabei erhalten wir eine Darstellung

$$\textsc{Lift}(s) = \sum_{j=1}^{l} \mathrm{in}^*(u_j) f_{i_j} \mathrm{in}^*(v_j) = \sum_{p=1}^{k} g_p f_{q_p} h_p + \hat{a} \; .$$

Im Falle $\hat{a} = 0$ können wir daraus die Syzygie

$$\textsc{LiftSyz}(s) = \sum_{j=1}^{l} \mathrm{in}^*(u_j) e_{f_{i_j}} \mathrm{in}^*(v_j) - \sum_{p=1}^{k} g_p e_{f_{q_p}} h_p \in Syz(F) \qquad (5.4)$$

ablesen.

Satz 5.7 *Sei I das von $F = \{f_1, \ldots, f_m\}$ erzeugte Ideal von R und sei S ein homogenes Erzeugendensystem des Syzygienmoduls $Syz(\mathrm{in}(F))$ des Initialideals von F. F ist genau dann eine Gröbnerbasis von I, wenn es zu jeder Syzygie $s = \sum_{j=1}^{l} u_j e_{i_j} v_j \in S$ eine Syzygie $t(s) = \sum_{j=1}^{k} h_j e_{f_{i_j}} g_j \in Syz(F)$ mit $k \geq n$ und der Eigenschaft $\mathrm{in}(h_j) = u_j$ und $\mathrm{in}(g_j) = v_j$ für alle $1 \leq j \leq l$ sowie $\varphi(h_j) \circ \varphi(f_{i_j}) \circ \varphi(g_j) \prec \deg_\Gamma(s)$ für alle $l < j \leq k$ gibt. Im Falle ihrer Existenz erzeugt die Menge $\{t(s) \mid s \in S\}$ den Syzygienmodul $Syz(F)$ von F.*

Beweis: Seien F eine Gröbnerbasis von I und S ein Erzeugendensystem von $Syz(\mathrm{in}(F))$. Dann läßt $\textsc{Lift}(s)$ für alle $s \in S$ bei Division modulo F mittels $\textsc{Divide}_R$ den Rest 0 und die in (5.4) definierte Syzygie $\textsc{LiftSyz}(s)$ genügt den an $t(s)$ gestellten Bedingungen.

Nehmen wir nun an, daß zu jedem $s \in S$ ein $t(s) \in Syz(F)$ mit den geforderten Eigenschaften existiert. Dann läßt sich jede γ-Darstellung eines Elementes $a \in I$ mit Hilfe dieser Syzygien in eine $\varphi(a)$-Darstellung von a umwandeln. Folglich ist F nach Satz 5.4 eine Gröbnerbasis.

Die Syzygien von F entsprechen genau den γ-Darstellungen des Nullelements modulo F und Anwendung der obigen Überlegung auf den Spezialfall $a = 0$ zeigt schließlich, daß $\{t(s) \mid s \in S\}$ den Syzygienmodul $Syz(F)$ erzeugt. □

Sei $T(F) = \{\textsc{LiftSyz}(s) \mid s \in \textsc{Triv}(\mathrm{in}(F))\}$. Dann ist unter den Voraussetzungen von Satz 5.5 das T-Syzygienproblem relativ zu den gleichen Berechenbarkeitsanforderungen wie bei der Gröbnerbasisberechnung algorithmisch lösbar.

Ist F eine Gröbnerbasis, so kann man die neben $T(F)$ noch fehlenden nichttrivialen Syzygien zur Erzeugung von $Syz(F)$ als Nebenprodukt des Gröbnerbasistests berechnen, indem man die dabei auftretenden Syzygien $\textsc{LiftSyz}(s)$

aufsammelt. Kommen wir nun zum Fall, daß das Erzeugendensystem F noch keine Gröbnerbasis ist. Wir starten Algorithmus GROEBNER und jeder erfolglose Aufruf der Gröbnerbasistestfunktion liefert eine Darstellung des ausgegebenen Idealelements als Kombination der Eingabebasis. Sammelt man die Transformationsgleichungen während der Ausführung von GROEBNER auf und transformiert damit das letztendlich berechnete Erzeugendensystem des Syzygienmoduls der Gröbnerbasis, so erhält man ein Erzeugendensystem des Syzygienmoduls von F. Diese Methode zur Syzygienmodulberechnung geht auf Zacharias zurück (siehe [Za78]).

Analoge Aussagen zu Satz 5.7 und den sich daran anschließenden konstruktiven Betrachtungen gelten auch für einseitige Ideale. Der Beweis verwendet genau dieselben Ideen, nur daß er sich an manchen Stellen noch vereinfacht, insbesondere dann, wenn im zweiseitigen Fall triviale Syzygien auftauchen.

Wir kommen zu einem wohlbekannten, allerdings in diesem allgemeinen Kontext nach Kenntnis des Autors bisher an keiner Stelle formulierten Zusammenhang zwischen Gröbnerbasen bezüglich unterschiedlicher Filtrierungen.

Satz 5.8 *Seien $(R, \Gamma, \prec_\Gamma, \varphi_\Gamma)$ und $(R, \Omega, \prec_\Omega, \varphi_\Omega)$ zwei zum Ring R gehörige graduierte Strukturen, so daß es einen schwach ordnungsverträglichen (d.h. Bedingung (4.9) erfüllenden) Monoidepimorphismus $\tau : \Omega \to \Gamma$ mit $\varphi_\Gamma = \varphi_\Omega \circ \tau$ gibt*[3]*.*

Sei I ein ein- oder zweiseitiges Ideal von R und F eine Gröbnerbasis von I bezüglich $(R, \Omega, \prec_\Omega, \varphi_\Omega)$. Dann ist F auch Gröbnerbasis von I bezüglich $(R, \Gamma, \prec_\Gamma, \varphi_\Gamma)$.

Beweis: Wir betrachten den Fall eines zweiseitigen Ideals I, im einseitigen Fall verläuft der Beweis analog. Zur Unterscheidbarkeit werden die zu einer der graduierten Strukturen gehörigen Bestimmungsstücke jeweils mit dem Monoid indiziert.

Angenommen, es gilt $\mathrm{In}_\Gamma(I) \not\subseteq \mathrm{In}_\Gamma(F)$. Sei $g \in I$ ein Element mit bezüglich $\prec_\Omega$ minimalem $\varphi_\Omega(g)$, für welches

$$\mathrm{in}_\Gamma(g) \notin \mathrm{In}_\Gamma(F) \tag{5.5}$$

gilt. Aus der vorausgesetzten Gröbnerbasiseigenschaft können wir $\mathrm{in}_\Omega(g) \in \mathrm{In}_\Omega(F)$ ableiten, also existieren $f_1, \ldots, f_k \in F$ und $h_1, \ldots, h_k, h'_1, \ldots, h'_k \in R$ mit

$$\begin{aligned} \varphi_\Omega(g) &= \varphi_\Omega(h_i) \circ \varphi_\Omega(f_i) \circ \varphi_\Omega(h'_i)\ , 1 \le i \le k, \quad \text{und} \\ \mathrm{in}_\Omega(g) &= \sum_{i=1}^{k} \mathrm{in}_\Omega(h_i)\ \mathrm{in}_\Omega(f_i)\ \mathrm{in}_\Omega(h'_i) \quad . \end{aligned} \tag{5.6}$$

Daraus ergibt sich

$$\varphi_\Omega\left(g - \sum_{i=1}^{k} h_i f_i h'_i\right) \prec_\Omega \varphi_\Omega(g) \quad . \tag{5.7}$$

[3] Insbesondere ist die durch φ_Ω induzierte Ω-Filtrierung von R eine Verfeinerung der durch φ_Γ induzierten Γ-Filtrierung von R.

Anwendung von τ auf (5.6) und (5.7) führt zu

$$\varphi_\Gamma(g) = \varphi_\Gamma(h_i) \circ \varphi_\Gamma(f_i) \circ \varphi_\Gamma(h_i') \text{ , } 1 \leq i \leq k, \text{ und} \tag{5.8}$$

$$\varphi_\Gamma \left(g - \sum_{i=1}^{k} h_i f_i h_i' \right) \preceq_\Gamma \varphi_\Gamma(g) \quad . \tag{5.9}$$

Wegen (5.5) muß in (5.9) die Gleichheit gelten. Das impliziert

$$\text{in}_\Gamma(g) = \text{in}_\Gamma \left(g - \sum_{i=1}^{k} h_i f_i h_i' \right) + \sum_{i=1}^{k} \text{in}_\Gamma(h_i) \, \text{in}_\Gamma(f_i) \, \text{in}_\Gamma(h_i') \quad . \tag{5.10}$$

Aufgrund von (5.7) gilt $\text{in}_\Gamma \left(g - \sum_{i=1}^{k} h_i f_i h_i' \right) \in \text{In}_\Gamma(F)$, was wegen (5.10) im Widerspruch zu (5.5) die Gültigkeit von $\text{in}_\Gamma(g) \in \text{In}_\Gamma(F)$ zur Folge hätte. Also folgt $\text{In}_\Gamma(I) = \text{In}_\Gamma(F)$. □

Das im Polynomfall verwendete Standardargument, daß für beliebige Teilmengen $H \subseteq R$ trivialerweise die Gleichheit $\text{In}_\Omega(\text{In}_\Gamma(H)) = \text{In}_\Omega(H)$ gilt, kann nicht übernommen werden, da der assoziierte graduierte Ring im allgemeinen nicht in den Ausgangsring einbettbar ist.

Bei Betrachtung des Satzes stellt sich die Frage, was passiert, wenn man anstelle von $\varphi_\Gamma = \varphi_\Omega \circ \tau$ nur fordert, daß die Ω-Filtrierung Verfeinerung der Γ-Filtrierung ist. Leider muß man feststellen, daß dann nicht mehr notwendigerweise eine Übertragung der Gröbnerbasiseigenschaft stattfindet. Für beliebige Verfeinerungen gelten die Beziehungen $\varphi_\Omega(g) \preceq_\Omega \varphi_\Omega(h) \Longrightarrow \varphi_\Gamma(g) \preceq_\Gamma \varphi_\Gamma(h)$ und $\varphi_\Gamma(g) \preceq_\Gamma \tau(\varphi_\Omega(g))$. Es gibt aber Verfeinerungen, die nicht die Bedingung

$$\varphi_\Omega(g) = \varphi_\Omega(h_i) \circ_\Omega \varphi_\Omega(f_i) \circ_\Omega \varphi_\Omega(h_i') \Longrightarrow \varphi_\Gamma(g) = \varphi_\Gamma(h_i) \circ_\Gamma \varphi_\Gamma(f_i) \circ_\Gamma \varphi_\Gamma(h_i') \tag{5.11}$$

erfüllen. In einigen Situationen kann es vorkommen, daß eine Ω-Gröbnerbasis nicht mehr notwendigerweise auch Γ-Gröbnerbasis ist. Hier ist ein solches Beispiel: $R = \mathbb{K}[X]$, $\Omega = T(X)$, $\prec_\Omega = \prec_{totdeg}$, $\varphi_\Omega =$ lpp, $\Gamma = \mathbb{N} \times \mathbb{N}$, $\prec_\Gamma = \prec_{lex}$,

$$\forall c \in \mathbb{K} \backslash \{0\} \ : \ \varphi_\Gamma(c) = (0,0) \quad \forall f \notin \mathbb{K} \ : \ \varphi_\Gamma(f) = (\deg(f), 1) \text{ und}$$

$$\forall u \in T(X) \ : \ \tau(u) = (\deg(u), \deg(u)) \quad .$$

Der assoziierte graduierte Ring in der Γ-Filtrierung ist als $\mathbb{K}$-Vektorraum isomorph zu R, die Multiplikation zweier beliebiger homogener Elemente vom Grad größer als $\epsilon = (0,0)$ ergibt in jedem Fall 0. Damit sind die Γ-Gröbnerbasen eines Polynomideals gerade seine $\mathbb{K}$-Vektorraumbasen. Dagegen handelt es sich bei den Ω-Gröbnerbasen um gewöhnliche Buchbergersche Gröbnerbasen bezüglich der totalen Gradordnung.

Man erkennt aber auch, daß die Voraussetzungen des Satzes auf Verfeinerungen mit der Eigenschaft (5.11) abgeschwächt werden können, ohne daß der Satz dabei seine Gültigkeit verliert.

Abschließend geben wir einen Zusammenhang an, welcher sich später bei der Konstruktion geeigneter R-Modulfiltrierungen als hilfreich erweisen wird. Auf den trivialen Beweis der Aussage wird verzichtet.

Bemerkung 5.9 *Seien $(R, \Gamma, \prec_\Gamma, \varphi_\Gamma)$ und $(R, \Omega, \prec_\Omega, \varphi_\Omega)$ zwei zum Ring R gehörige graduierte Strukturen, so daß es einen Monomorphismus $\tau : \Gamma \to \Omega$ geordneter Monoide mit der Eigenschaft $\varphi_\Omega = \varphi_\Gamma \circ \tau$ gibt.*

Dann ist der zur graduierten Struktur $(R, \Omega, \prec_\Omega, \varphi_\Omega)$ gehörige assoziierte graduierte Ring G_Ω in natürlicher Weise isomorph zum assoziierten graduierten Ring G_Γ der graduierten Struktur $(R, \Gamma, \prec_\Gamma, \varphi_\Gamma)$. Von Null verschiedene homogene Elemente vom Grad $\omega \in \Omega$ gehen bei diesem Isomorphismus in homogene Elemente vom Grad $\tau^{-1}(\omega)$ über und umgekehrt. Weiterhin stimmen die durch beide graduierten Strukturen definierten Initialabbildungen unter dem Isomorphismus überein und folglich ist $F \subset R$ genau dann eine Ω-Gröbnerbasis, wenn F eine Γ-Gröbnerbasis ist.

5.3 Reduzierte Gröbnerbasen und kanonische Simplifikation

Algorithmus DIVIDE$_R$ liefert nur einen Nullsimplifikator des Restklassenrings R/I und ist somit kein Divisionsalgorithmus im auf Seite 36 definierten strengen Sinne. Nach Satz 2.9 reicht das aber bereits für die Existenz eines kanonischen Simplifikators und folglich auch des auf Seite 36 vorgestellten echten Divisionsalgorithmus DIVIDE aus. Sowohl der im Beweis des Satzes konstruierte kanonische Simplifikator als auch Algorithmus DIVIDE sind allerdings von rein theoretischer Bedeutung. In einer Reihe von Spezialfällen lassen sich darüberhinaus echte Divisionsalgorithmen konstruieren, welche Bedingung (5.3) erfüllen und bei Anwendung auf eine Gröbnerbasis des Ideals I einen praktikablen kanonischen Simplifikator von R/I liefern. Während DIVIDE$_R$ auf der sogenannten Kopfreduktion beruht, bauen diese kanonischen Simplifikatoren auf der Totalreduktion auf. Neben den offensichtlichen theoretischen Vorzügen besitzen die kanonischen Simplifikatoren in dieser konkreten Situation auch Effizienzvorteile (siehe [G&91]). Außerdem beruht der Existenz- und Eindeutigkeitssatz reduzierter Gröbnerbasen auf den gleichen Grundideen wie die Totalreduktion (siehe [Bu85]). Das legt die Frage nach der Verallgemeinerbarkeit der Totalreduktion auf graduierte Strukturen nahe. Wir werden uns ganz auf die Betrachtung von zweiseitigen Idealen beschränken. Alle Ergebnisse lassen sich jedoch geradlinig auf den einfacheren Fall einseitiger Ideale übertragen.

Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine effektive graduierte Gröbnerstruktur. Weiterhin seien F eine beliebige endliche Teilmenge von R und I das von F erzeugte Ideal. Aufgrund der gemachten Annahmen sind die Funktionen GROEBNER und DIVIDE$_R$ berechenbar und die Zuordnung $a \mapsto \hat{a}$, wobei $\hat{a}$ der beim Aufruf von DIVIDE$_R(a,$ GROEBNER$(F))$ berechnete Rest ist, beschreibt einen Nullsimplifikator $Z_F : R \to R$ des Restklassenrings R/I. Nächstes Ziel ist es, eine berechenbare Funktion $\overline{\text{DIVIDE}}_R$ der Spezifikation

Aufruf: $(g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a}, j_1, \ldots, j_k) := \overline{\text{DIVIDE}}_R(a, F)$
Eingaben: $a \in R$,
$F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Ideals I
Ausgaben: $g_1, \ldots, g_k, h_1, \ldots, h_k, \hat{a} \in R$, $1 \le j_1, \ldots, j_k \le m$, wobei
$a = \sum_{i=1}^{k} g_i f_{j_i} h_i + \hat{a}$, $\varphi(g_i) \circ \varphi(f_{i_j}) \circ \varphi(h_i) \preceq \varphi(a)$ $(i = 1, \ldots, k)$,

$$\hat{a} = 0 \text{ oder } \mathrm{in}(\hat{a}) \notin \mathrm{In}(F) \text{ und aus } a - a' \in I \text{ folgt } \hat{a} = \widehat{a'}.$$

zu konstruieren. Falls eine derartige berechenbare Funktion existiert, so ist die Funktion $S_I : R \to R$, die jedem Element $a \in R$ ihren Divisionsrest $\hat{a}$ bei Anwendung von $\overline{\textsc{Divide}}_R(a, \textsc{Groebner}(F))$ zuordnet, ein kanonischer Simplifikator von R/I.

Seien $a, a' \in R$ zwei beliebige modulo I kongruente Elemente. Es muß

$$Z_F\left(Z_F(a) - Z_F(a')\right) = 0$$

gelten, was insbesondere die Enthaltenseinsrelation

$$\mathrm{in}\left(Z_F(a) - Z_F(a')\right) \in \mathrm{In}(I)$$

bedingt. Wegen $Z_F(a) \notin \mathrm{In}(I)$ und $Z_F(a') \notin \mathrm{In}(I)$ impliziert das

$$\varphi\left(Z_F(a)\right) = \varphi\left(Z_F(a')\right) \ , \tag{5.12}$$

ohne daß jedoch sofort notwendigerweise die Gleichheit $\mathrm{in}(Z_F(a)) = \mathrm{in}(Z_F(a'))$ vorzuliegen braucht. Anstelle der Konstruktion eines geeigneten Algorithmus $\overline{\textsc{Divide}}_R$ werden wir der Einfachheit halber nur einen Algorithmus für S_I angeben. Es ist leicht ersichtlich, wie aus diesem ein Algorithmus $\overline{\textsc{Divide}}_R$ gewonnen werden kann.

Vermöge $\mathrm{head}(a) = \mathrm{in}^*(\mathrm{in}(a))$ und $\mathrm{tail}(a) = a - \mathrm{head}(a)$ werden berechenbare Funktionen $\mathrm{head} : R \to R$ und $\mathrm{tail} : R \to R$ eingeführt. $\mathrm{head}(a)$ wird der *Kopf* und $\mathrm{tail}(a)$ der *Rest* des Ringelements a genannt. Nach Konstruktion gilt $\varphi(\mathrm{tail}(a)) \prec \varphi(a)$.

Wir betrachten die auf der Menge aller endlichen Teilmengen von $G \setminus \{0\}$, welche aus homogenen Elementen mit paarweise verschiedenen Γ-Graden bestehen, durch

$$\begin{aligned} \emptyset &\mapsto 0 \quad \text{und} \\ \{u_1, \ldots, u_m\} &\mapsto \sum_{i=1}^{m} \mathrm{in}^*(u_i) \end{aligned}$$

definierte Abbildung und werden uns davon überzeugen, daß es sich dabei um eine Bijektion handelt. Seien $U = \{u_1, \ldots, u_m\}$, $V = \{v_1, \ldots, v_n\}$ und $a \in R$ so, daß $U \mapsto a$ und $V \mapsto a$ gelten. Ohne Beschränkung der Allgemeinheit nehmen wir an, daß u_1 und v_1 die jeweils gradgrößten Elementen von U beziehungsweise V sind. Nach Definition der Abbildung gilt $a = \sum_{i=1}^{m} \mathrm{in}^*(u_i) = \sum_{i=1}^{n} \mathrm{in}^*(v_i)$ und damit folgt aus $\mathrm{in}(a) = \mathrm{in}\left(\sum_{i=1}^{m} \mathrm{in}^*(u_i)\right) = u_1$ und $\mathrm{in}(a) = \mathrm{in}\left(\sum_{i=1}^{n} \mathrm{in}^*(v_i)\right) = v_1$ die Gleichheit $u_1 = v_1$. Mittels vollständige Induktion über den Grad des Initialterms von a weist man schließlich die Injektivität der Abbildung nach. Sei nun $a \in R$ ein von Null verschiedenes Element, dann bricht die Folge $u_1 = \mathrm{in}(a), u_2 = \mathrm{in}(tail(a)), u_3 = \mathrm{in}(tail(tail(a))), \ldots$ aufgrund der Wohlordnungseigenschaft von $\prec$ nach endlich vielen, sagen wir m, Gliedern ab und die Menge der Glieder $\{u_1, u_2, \ldots, u_m\}$ wird bei der obigen Abbildung auf a abgebildet. Somit ist auch die Surjektivität bewiesen.

Wir stellen also fest: jedes von Null verschiedene Element $a \in R$ läßt sich in eindeutiger Weise als endliche Summe

$$a = \sum_{i=1}^{m} \text{in}^*(u_i) \tag{5.13}$$

darstellen, wobei die u_i von Null verschiedene homogene Elemente des assoziierten graduierten Rings G sind und der Bedingung $\deg_\Gamma(u_m) \prec \cdots \prec \deg_\Gamma(u_1)$ genügen. Die Menge $\{u_1, \ldots, u_m\}$ nennen wir den *Monomträger* von a und bezeichnen sie mit $\text{Mon}(a)$. Per definitionem ist die leere Menge Monomträger des Nullpolynoms. Der Begriff des Monomträgers lehnt sich an den aus Polynomringen bekannten Begriff des Trägers eines Polynoms an. Darunter versteht man die Menge der Potenzprodukte, die mit von Null verschiedenem Koeffizienten in dem Polynom vorkommen. Die natürliche Verallgemeinerung des Trägers besteht im Bilden der Menge der Γ-Grade der Elemente von $\text{Mon}(a)$. In Situationen, in denen der assoziierte graduierte Ring eine direkte Summe eindimensionaler Vektorräume R_γ über einem Körper $\mathbb{K} = R_\epsilon$ ist, gibt die Menge dieser Grade bereits Aufschluß über die Irreduzibilität des Polynoms modulo einer beliebigen Menge F. Darin spiegelt sich die wohlbekannte Tatsache wider, daß in dieser Situation die wesentlichen Berechnungen bei der Konstruktion von Gröbnerbasen nicht nur in den assoziierten graduierten Ring, sondern sogar in das Wertemonoid zurückgedrückt werden können. In der hier betrachteten Allgemeinheit ist das nicht möglich und die Verwendung des informationshaltigeren Begriffs des Monomträgers erweist sich als günstiger.

Aufgrund der Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter homogener Ideale von G gibt es eine berechenbare Funktion $\overline{\text{DIVIDE}}_G$, deren Spezifikation sich von der der auf Seite 61 eingeführten Funktion DIVIDE_G nur dadurch unterscheidet, daß von dem ausgegebenen Rest A zusätzlich verlangt wird, daß er nur von der Restklasse des Eingabelements a modulo des von der Eingabemenge H erzeugten zweiseitigen Ideals von G abhängt. Sei $\{g_1, \ldots, g_m\}$ die durch GROEBNER berechnete Gröbnerbasis von I. Dann definieren wir

$$Z'_F(a) = Z_F(a) - \sum_{i=1}^{l} \text{in}^*(p_i) g_{r_i} \text{in}^*(q_i) \quad ,$$

wobei sich die Bestandteile p_i, q_i, r_i als Ergebnisse der Berechnung

$$(p_1, \ldots, p_l, q_1, \ldots, q_l, A, r_1, \ldots, r_l) = \overline{\text{DIVIDE}}_G(\text{in}(Z_F(a)), \{\text{in}(g_1), \ldots, \text{in}(g_m)\})$$

ergeben. Die so definierte Funktion $Z'_F : R \to R$ ist ebenfalls Nullsimplifikator von R/I. Außerdem erfolgt jedoch eine Normierung des Initialterms, daß heißt Eigenschaft (5.12) wird dahingehend verschärft, daß nicht nur der Grad des Initialterms des Divisionsrests, sondern sogar der Initialterm selbst nur von der Restklasse von a modulo des von F erzeugten Ideals I abhängt, d.h.

$$\text{in}(Z'_F(a)) = \text{in}(Z'_F(a')) \text{ für alle } a, a' \text{ mit } a - a' \in I \, . \tag{5.14}$$

Die durch

$$S_I(a) = \begin{cases} 0 & : \text{ falls } Z_F(a) = 0 \\ \text{head}(Z'_F(a)) + S_I\left(\text{tail}(Z'_F(a))\right) & : \text{ sonst} \end{cases} \tag{5.15}$$

rekursiv definierte Funktion $S_I : R \to R$ ist total und berechenbar. Einfach zu zeigende Eigenschaften der Funktion S_I sind:

i) S_I ist Nullsimplifikator für R/I.

ii) Ein Element $a \in R$ ist genau dann Fixpunkt von S_I, wenn $\mathrm{in}^*(u)$ für jedes $u \in \mathrm{Mon}(a)$ Fixpunkt von Z'_F ist.

Es bleibt nachzuweisen, daß es sich sogar um einen kanonischen Simplifikator handelt.

Satz 5.10 *Seien $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine effektive graduierte Gröbnerstruktur und F ein endliches Erzeugendensystem des Ideals $I \subseteq R$. Dann ist die in (5.15) definierte Funktion S_I ein kanonischer Simplifikator für R/I.*

Beweis: Seien a und a' zwei beliebige Elemente mit $a - a' \in I$. Es existieren (eindeutig bestimmte) Elemente $b, b' \in R$ mit $\mathrm{Mon}(b) = \mathrm{Mon}(S_I(a)) \backslash \mathrm{Mon}(S_I(a'))$ und $\mathrm{Mon}(b') = \mathrm{Mon}(S_I(a')) \setminus \mathrm{Mon}(S_I(a))$. Die Elemente b und b' sind Fixpunkte der Funktion S_I und damit erst recht der Funktionen Z_F und Z'_F. Aufgrund von $b - b' = S_I(a) - S_I(a') \in I$ folgt aus (5.14) die Beziehung $\mathrm{in}(b) = \mathrm{in}(Z'_F(b)) = \mathrm{in}(Z'_F(b')) = \mathrm{in}(b')$. Wegen $\mathrm{Mon}(b) \cap \mathrm{Mon}(b') = \emptyset$ zieht das mit Notwendigkeit $b = b' = 0$ nach sich. Damit ist die noch ausstehende Eigenschaft $S_I(a) = S_I(a')$ eines kanonischen Simplifikators gezeigt. □

Definition 5.11 *Sei μ eine Funktion, die jedem homogenen Ideal M des assoziierten graduierten Rings G ein (ausgezeichnetes) minimales homogenes Erzeugendensystem $\mu(M)$ zuweist. Falls $F \subseteq I$ den Bedingungen*

i) $\mathrm{in}(F) = \mu(\mathrm{In}(I))$,

ii) $\mathrm{in}(f) \neq \mathrm{in}(f')$ *für alle* $f, f' \in F$ *mit* $f \neq f'$ *und*

iii) $S_I(\mathrm{tail}(f)) = \mathrm{tail}(f)$ *für alle* $f \in F$

genügt, so wird F eine μ-reduzierte Gröbnerbasis *des Ideals I genannt.*

Wegen *i)* ist es offensichtlich, daß jede μ-reduzierte Gröbnerbasis erst recht eine Gröbnerbasis ist. Weiter gilt:

Satz 5.12 *Seien $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur und μ eine Funktion, die für jedes homogene Ideal des assoziierten graduierten Rings ein minimales homogenes Erzeugendensystem auszeichnet.*

Dann besitzt jedes Ideal $I \subseteq R$ eine μ-reduzierte Gröbnerbasis. Bei festgehaltenem Schnitt in^* *der Initialabbildung ist sie sogar eindeutig bestimmt.*

Beweis: Sei F' eine beliebige Teilmenge von Idealelementen mit paarweise verschiedenen Initialtermen und $\mathrm{in}(F') = \mu(\mathrm{In}(I))$ und sei $F = \{\mathrm{head}(f) + S_I(\mathrm{tail}(f)) \mid f \in F'\}$. Dann ist F eine reduzierte Gröbnerbasis von I und die Existenz ist nachgewiesen.

Kommen wir damit zum Eindeutigkeitsnachweis. Seien F und F' zwei Erzeugendensysteme von I, die die Bedingungen *i)* bis *iii)* aus Definition 5.11 erfüllen. Zu jedem $u \in \mu(\mathrm{In}(I))$ enthalten die Mengen F und F' je ein eindeutig bestimmtes Element $f_u \in F$ beziehungsweise $f'_u \in F'$ mit $\mathrm{in}(f_u) = \mathrm{in}(f'_u) = u$. Es gilt $f_u - f'_u = \mathrm{tail}(f_u) - \mathrm{tail}(f'_u) \in I$. Also sind $\mathrm{tail}(f_u)$ und $\mathrm{tail}(f'_u)$ kongruent modulo I, was die Bildgleichheit unter S_I und schließlich unter Ausnutzung der Fixpunktbedingung *iii)* die Gleichheit $f_u = f'_u$ nach sich zieht. Damit ist auch die Eindeutigkeit der reduzierten Gröbnerbasis eines Ideals von R gezeigt. □

Um aus der Berechenbarkeit einer Gröbnerbasis von I auf die Berechenbarkeit seiner reduzierten Gröbnerbasis schließen zu können, benötigt man zusätzlich zu den Eigenschaften einer effektiven graduierten Gröbnerstruktur die Berechenbarkeit von μ, das heißt die Berechenbarkeit ausgezeichneter Erzeugendensysteme endlich erzeugter homogener Ideale von G. Die Berechnung einer homogenen Transformationsmatrix eines beliebigen endlichen homogenen Erzeugendensystems H auf $\mu(G(H)G)$ ist dann aufgrund der Entscheidbarkeit des Idealenthaltenseinsproblems von G immer algorithmisch möglich.

Der angegebene kanonische Simplifikator S_I beruht auf einer zunächst einmal weitgehend willkürlichen Auswahl von $\mathrm{in}^*(u)$ für jedes homogene Element $u \in G$. Der obige Begriff der reduzierten Gröbnerbasis hängt neben der graduierten Ringstruktur $\mathfrak{R}$ von zwei zusätzlichen Festlegungen, nämlich den Funktionen in^* und μ, ab. Daraus erklärt sich auch die Notwendigkeit des Festhaltens von in^* für die Eindeutigkeit der μ-reduzierten Gröbnerbasis eines Ideals von R.

Unter Ausnutzung der algebraischen Struktur von R lassen sich in vielen Situationen "natürliche" Funktionen in^* und μ auszeichnen. So kann man im klassischen Fall der Polynomringe über einem Körper bei Verwendung einer Buchbergerschen Graduierung in^* als die identische Einbettung der Menge aller Monome in R wählen. Weiterhin sind die Elemente einer homogenen Minimalbasis eines beliebigen Monomideals bis auf von Null verschiedene skalare Faktoren eindeutig bestimmt und man kann mittels μ die eindeutig bestimmte Minimalbasis auswählen, welche nur aus Potenzprodukten besteht.

Bei einer graduierten Ringstruktur $\mathfrak{R}$ mit wohlgeordnetem Wertemonoid sind die Ringe $\mathcal{F}_\epsilon$ und R_ϵ vermöge der zueinander inversen Isomorphismen $\mathrm{in}\,|_{\mathcal{F}_\epsilon}$ und $\mathrm{in}^*\,|_{R_\epsilon}$ isomorph. Im weiteren werden wir $\mathcal{F}_\epsilon$ und R_ϵ identifizieren und mit Q bezeichnen. Sowohl R, G als auch jeder direkte Summand R_γ des assoziierten graduierten Rings G sind Q-Bimoduln. Die beiden folgenden Lemmata geben Bedingungen an, unter denen R und G als Q-Bimoduln zueinander isomorph sind. In diesem Fall läßt sich R analog zu G in eine direkte Summe zerlegen und es kann die Totalreduktion eines Elementes $f \in R$ modulo einer endlichen Teilmenge $F \subset R$ erklärt werden, welche die Bestandteile von f bezüglich der direkten Summe sukzessiv modulo F reduziert. Identifiziert man die Q-Moduln R und G mit Hilfe des oben erwähnten Isomorphismus, so ist es natürlich, in^* als Einschränkung der identischen Abbildung auf die Vereinigung aller direkten Summanden festzulegen. Legt man diese Funktion in^* zugrunde, so enthält der Monomträger $\mathrm{Mon}(a)$ eines Elementes $a \in R$ gerade

die (von Null verschiedenen) homogenen Bestandteile von a. Ist Q ein Körper, so beschreibt die Totalreduktion modulo einer Gröbnerbasis F von I gerade den in (5.15) definierten kanonischen Simplifikator S_I für R/I.

Lemma 5.13 *Sei $(R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit Wohlordnung $\prec$. Es existiert genau dann ein Schnitt $\mathrm{in}^* : G \to R$ der Initialabbildung mit der Eigenschaft, daß die Einschränkung $\mathrm{in}^* |_{R_\gamma}$ für jedes $\gamma \in \Gamma$ ein Homomorphismus additiver Gruppen ist, wenn die Untergruppe $\hat{\mathcal{F}}_\gamma$ für jedes $\gamma \in \Gamma$ ein direkter Summand von $\mathcal{F}_\gamma$ ist.*

Beweis: $\Longrightarrow$ Es existiere ein Schnitt in^* der beschriebenen Art. Aufgrund der Injektivität des Schnitts sind alle Homomorphismen $\mathrm{in}^* |_{R_\gamma}$ sogar Monomorphismen und demnach gilt $im\left(\mathrm{in}^* |_{R_\gamma}\right) \cong R_\gamma$ für alle $\gamma \in \Gamma$. Aus der Existenz und Eindeutigkeit der Summendarstellungen (5.13) folgt

$$R = \bigoplus_{\gamma \in \Gamma} im\left(\mathrm{in}^* |_{R_\gamma}\right) \cong \bigoplus_{\gamma \in \Gamma} R_\gamma = G \tag{5.16}$$

und aus $\mathcal{F}_\gamma = \bigoplus_{\gamma' \preceq \gamma} im\left(\mathrm{in}^* |_{R_{\gamma'}}\right) = \hat{\mathcal{F}}_\gamma \oplus im\left(\mathrm{in}^* |_{R_\gamma}\right)$ ergibt sich schließlich die Behauptung.

$\Longleftarrow$ Sei $\hat{\mathcal{F}}_\gamma$ für jedes $\gamma \in \Gamma$ ein direkter Summand von $\mathcal{F}_\gamma$. Nach dem ersten Isomorphiesatz für Gruppen folgt daraus $\mathcal{F}_\gamma = \hat{\mathcal{F}}_\gamma \oplus B$ mit $B \cong R_\gamma = \mathcal{F}_\gamma / \hat{\mathcal{F}}_\gamma$ (vgl. [vW67]). Folglich existiert ein Schnitt in^*, dessen Einschränkung auf R_γ gleich der Hintereinanderausführung eines Isomorphismus $\tau : R_\gamma \to B$ und der natürlichen Einbettung von B in $\mathcal{F}_\gamma$ ist. □

Entsprechende Aussagen gelten auch bei Betrachtung additiver Gruppen mit Operatorenbereich Q, d.h. Q-Moduln.

Lemma 5.14 *Sei $(R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit Wohlordnung $\prec$. Falls alle R_γ freie Q-Linksmoduln sind, so gibt es einen Schnitt $\mathrm{in}^* : G \to R$ der Initialabbildung, so daß die Einschränkung $\mathrm{in}^* |_{R_\gamma}$ für alle $\gamma \in \Gamma$ ein Q-Linksmodulhomomorphismus ist. Insbesondere sind R und G als Q-Linksmoduln isomorph.*

Beweis: Sei U_γ ein freies Erzeugendensystem des Q-Linksmoduls R_γ. Dann läßt sich jede Abbildung $j_\gamma : U_\gamma \to R$ mit $\mathrm{in}(j_\gamma(u)) = u$ für alle $u \in U_\gamma$ auf eindeutige Weise zu einem Monomorphismus $\mathrm{in}^*_\gamma : R_\gamma \to R$ mit der Eigenschaft $\mathrm{in}(\mathrm{in}^*_\gamma(a)) = a$ für alle $a \in R_\gamma$ fortsetzen. Legt man für jedes $\gamma \in \Gamma$ eine derartige Abbildung j_γ fest, so beschreibt $\mathrm{in}^*(a) = \mathrm{in}^*_{\deg_\Gamma(a)}(a)$ auf wohldefinierte Weise einen Schnitt in^* der Initialabbildung mit den behaupteten Eigenschaften. Damit sind die Voraussetzungen von Lemma 5.13, ($\Rightarrow$), für Gruppen mit Linksoperatorenbereich Q erfüllt und es ergibt sich die Isomorphie (5.16) für Q-Linksmoduln. Am Rande halten wir die Gültigkeit von

$$\mathrm{in}^*\left(\sum_{i=1}^{m_\gamma} \alpha_i u_i\right) = \sum_{i=1}^{m_\gamma} \alpha_i j_\gamma\left(u_i\right) \quad (\alpha_i \in Q, u_i \in U_\gamma) \tag{5.17}$$

fest. □

Die meisten bisher in der Literatur betrachteten Anwendungen weisen eine derartige Struktur des assoziierten graduierten Rings auf. Ein den Voraussetzungen von Lemma 5.14 genügender Ring R ist freier Q-Linksmodul und jede Menge $\{j_\gamma(u) \mid \gamma \in \Gamma, u \in U_\gamma\}$, wobei j_γ und U_γ wie im Beweis definiert sind, ist ein freies Erzeugendensystem davon. Aufgrund der Isomorphie (5.16) können R und G als additive Gruppen (mit Operatorenbereich Q) identifiziert und mit gegebenfalls verschiedenen Multiplikationen ausgestattet werden. Dann ist die mit identischen Abbildungen j_γ durch (5.17) definierte Funktion in^* die Einschränkung der obigen Identifizierung von G und R auf die Teilmenge der homogenen Elemente. Ist G ein effektiver graduierter Ring, dann ist die Teilmenge der homogenen Elemente entscheidbar und die Funktion in^* berechenbar.

Es bleibt festzustellen, daß Isomorphie (5.16) im allgemeinen nicht zutrifft. Sei zum Beispiel $R = \mathbb{Z}[X]/(3X-2)$, $(\Gamma, \prec) = (\mathbb{N}, <)$ und φ weise jeder Restklasse den kleinstmöglichen Grad eines seiner Repräsentanten zu. Dann gilt $G = \mathbb{Z} \oplus \mathbb{Z}/(3) \oplus \cdots \oplus \mathbb{Z}/(3) \oplus \cdots$ und keine der Zuordnungen $\mathrm{in}^*(X) = X + \alpha$, $\alpha \in \mathbb{Z}$, bewirkt $3\,\mathrm{in}^*(X) = 0$. Eine Fortsetzung zu einem geeigneten Monomorphismus ist damit unmöglich.

Zum Abschluß betrachten wir noch einmal die Frage nach ausgezeichneten minimalen Erzeugendensystemen homogener Ideale des assoziierten graduierten Rings.

Lemma 5.15 *Der Ring Q habe die Eigenschaft, daß jedes seiner Linksideale von einem einzigen Element erzeugt wird und ν sei eine Funktion, die jedem Linksideal $L \subseteq Q$ ein erzeugendes Element $\nu(L)$ zuordnet. Für alle $\gamma \in \Gamma$ gelte die Q-Linksmodulisomorphie $R_\gamma \cong Q$ vermöge eines Isomorphismus $\iota_\gamma : R_\gamma \to Q$. Dann besitzt jedes homogene Ideal $J \subseteq G$ genau ein minimales Erzeugendensystem $U(J)$ mit der Eigenschaft*

$$\nu\left(\iota_\gamma(J \cap R_\gamma)\right) = \iota_\gamma(u), \text{ wobei } \gamma = \deg_\Gamma(u)\,, \tag{5.18}$$

für alle $u \in U(J)$.

Beweis: Man überlegt sich leicht, daß für beliebige minimale homogene Erzeugendensysteme U und V von J die Gleichheit $\deg_\Gamma(U) = \deg_\Gamma(V)$ der Mengen der Γ-Grade aller Elemente von U beziehungsweise V gelten muß. Wir führen die Bezeichnung $\Gamma(J) = \deg_\Gamma(U) = \deg_\Gamma(V)$ ein. Die Menge

$$U(J) := \left\{\iota_\gamma^{-1}\left(\nu\left(\iota_\gamma(J \cap R_\gamma)\right)\right) \mid \gamma \in \Gamma(J)\right\} \tag{5.19}$$

besteht nur aus homogenen Elementen und erzeugt J. Die Γ-Grade der Elemente von $U(J)$ sind paarweise verschieden. Insbesondere gilt daher $\deg_\Gamma(U) \neq \Gamma(J)$ für alle echten Teilmengen $U \subsetneqq U(J)$, weshalb $U(J)$ minimales Erzeugendensystem sein muß. Die Bedingung (5.18) ist nach Konstruktion erfüllt.

Seien U und V zwei Mengen homogener Elemente, die den an $U(J)$ gestellten Anforderungen genügen. Zu jedem $v \in V$ gibt es ein Element $u \in U$ mit

$\deg_\Gamma(v) = \deg_\Gamma(u)$. Aus (5.18) folgt $u = v$. Also gilt $V \subseteq U$ und da U ein minimales Erzeugendensystem von J ist, ergibt sich $U = V$. □

Ist Q sogar ein Körper, dann ist die Menge $\{\iota_\gamma^{-1}(1) \mid \gamma \in \Gamma\}$ eine Q-Vektorraumbasis von G, vermöge $\iota_\gamma^{-1}(1) \mapsto \gamma$ kann die Basis mit der Menge Γ identifiziert werden. Erklären wir ν durch $\nu(\{0\}) = 0$ und $\nu(Q) = 1$, so besitzt jedes homogene Ideal von G gemäß dem obigen Lemma ein eindeutig bestimmtes minimales Erzeugendensystem, welches nur aus Elementen von Γ besteht. Ähnlich dem Fall des Polynomrings über einem Körper besteht eine bijektive Beziehung zwischen den homogenen Idealen von G und den Monoididealen von Γ. Der auf der Funktion μ mit $\mu(J) := U(J)$ und einem (5.17) genügenden Schnitt in^* der Initialabbildung basierende Begriff der reduzierten Gröbnerbasis ist eine natürliche Verallgemeinerung des klassischen Buchbergerschen Begriffs (siehe [Bu85]).

Betrachten wir ein anderes Beispiel eines graduierten Rings $G = \bigoplus_{\gamma\in\Gamma} R_\gamma$ des in Lemma 5.15 vorausgesetzten Typs. Dabei sei Q ein effektiver Euklidischer Ring und es existiere ein kanonischer Simplifikator $\sigma_\sim : Q \to Q$ der Zerlegung $Q/\sim$ von Q nach der Äquivalenzrelation $\sim$ der Assoziiertheit[4] zweier Elemente. Dann kann zu einer beliebigen endlichen Teilmenge $H \subseteq Q$ mit Hilfe des Euklidischen Algorithmus der bis auf Einheiten eindeutig bestimmte größte gemeinsame Teiler $ggT(H)$ aller Elemente von H bestimmt werden. Anschließende Anwendung von $\sigma_\sim$ auf $ggT(H)$ bewirkt ein Normieren der Einheiten und das entstehende Element kann als ausgezeichneter Erzeuger $\nu(L)$ des von H erzeugten Ideals $L \subseteq Q$ gewählt werden. Beispiele kanonischer Simplifikatoren $\sigma_\sim$ sind $\sigma_\sim(a) = |a|$ für $Q = \mathbb{Z}$ oder $\sigma_\sim(\sum_{i=0}^m \alpha_i X^i) = \sum_{i=0}^m \beta_i X^i$, wobei $\alpha_m \neq 0$ und $\beta_i = \frac{\alpha_i}{\alpha_m}$, im univariaten Polynomring $Q = \mathbb{K}[X]$.

Der folgende Satz beschreibt eine Situation, in der aus der Existenz und Berechenbarkeit endlicher Gröbnerbasen auch die Existenz und Berechenbarkeit μ-reduzierter Gröbnerbasen folgt.

Satz 5.16 *Q sei ein effektiver kommutativer Hauptidealring und $\nu : Fin(Q) \to Q$ sei eine berechenbare Funktion, die jeder endlichen Teilmenge $H \subseteq Q$ ein erzeugendes Element $\nu(H)$ des Ideals $(H) \subseteq Q$ zuordnet. $G = \bigoplus_{\gamma\in\Gamma} R_\gamma$ sei ein effektiver Γ-graduierter Ring mit entscheidbarem Enthaltenseinsproblem für endlich erzeugte homogene Ideale und zu jedem $\gamma \in \Gamma$ existiere ein berechenbarer Isomorphismus $\iota_\gamma : R_\gamma \to Q$. Für beliebige Elemente $\gamma, \omega \in \Gamma$ des Monoids Γ sei die Menge $quot(\gamma, \omega) = \{(\gamma', \gamma'') \in \Gamma \times \Gamma \mid \gamma' \circ \gamma \circ \gamma'' = \omega\}$ endlich und algorithmisch konstruierbar.*

Dann ist die Funktion μ, die jedem homogenen Ideal J das in (5.19) angegebene Erzeugendensystem $U(J)$ zuweist, in dem Sinne berechenbar, daß $U(J)$ aus einem beliebigen endlichen Erzeugendensystem F von J berechnet werden kann.

Beweis: Die an G gemachten Voraussetzungen sichern, daß aus einem beliebigen endlichen Erzeugendensystem von J ein minimales homogenes Erzeugendensystem von J algorithmisch konstruiert werden kann. Habe also F ohne

[4] Zwei Elemente a und b eines Integritätsbereiches heißen assoziiert, wenn es eine Einheit e mit $a = be$ gibt.

Beschränkung der Allgemeinheit diese Eigenschaft. Aus F kann die Menge $\Gamma(J)$ abgelesen werden.

Jedes homogene Element von J vom Grad $\omega \in \Gamma$ ist eine Q-Kombination der Menge $U_\omega = \left\{ \iota_{\gamma'}^{-1}(1) f \iota_{\gamma''}^{-1}(1) \mid f \in F \wedge (\gamma', \gamma'') \in quot(\deg_\Gamma(f), \omega) \right\}$ homogener Elemente. Mit anderen Worten, es gilt die Q-Linksmodulgleichheit $Q\,(J \cap R_\omega) = QU_\omega$ und die Menge $\left\{ \iota_\omega^{-1}(\nu(\iota_\omega(U_\omega))) \mid \omega \in \Gamma(J) \right\}$ ist das gesuchte Erzeugendensystem $\mu(J)$. □

5.4 Effektive graduierte Gröbnerstrukturen

Unsere bisherigen Untersuchungen zeigen, daß sich Idealenthaltenseinsproblem, Syzygienproblem, kanonische Simplifikation und Berechenbarkeit reduzierter Gröbnerbasen auf gleichartige Probleme homogener Ideale des assoziierten graduierten Rings reduzieren lassen. Um daraus einen Nutzen zu ziehen, ist es notwendig, sich der Arithmetik graduierter Ringe zuzuwenden. Ziel ist es, Effektivität des assoziierten graduierten Rings G sowie Entscheidbarkeit des Enthaltenseinsproblems und Lösbarkeit des Syzygienproblems von G auf Berechnungen im Wertemonoid Γ und im Ring $\mathcal{F}_\epsilon$ zu reduzieren. Im Gegensatz zum allgemeinen Konzept der graduierten Strukturen erfolgt hier eine Zusammenfassung zu Teilklassen durchweg effektiver graduierter Strukturen mit gleichartigen Grundalgorithmen. Die Polynomringe über Körpern (vgl. [Bu65]) werden dabei genauso erfaßt werden, wie die Polynomringe über effektiven Hauptidealringen (vgl. [KK84],[KK88],[Pa85]) oder noch allgemeiner über effektiven kommutativen Ringen mit entscheidbarem Idealenthaltenseins- und lösbarem Syzygienproblem (vgl. [Tri78], [Za78],[Sch79],[Mö88],[BW93],[AdL94]). Ebenso überdecken unsere Untersuchungen die Klassen der Einhüllenden von Liealgebren (vgl. [ApL85]), der Algebren von auflösbarem Typ (vgl. [KW90]), der auflösbaren Polynomringe (vgl. [Kr92]) und der G-Algebren (vgl. [Ap88]) sowie die von Mora in [Mo88b] betrachtete Algebrenklasse.

Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur mit wohlgeordnetem Monoid $(\Gamma, \prec)$. Zwischen den Ringen $\mathcal{F}_\epsilon$ und R_ϵ besteht eine natürliche Isomorphie vermöge der wir sie identifizieren wollen. Beide Ringe werden in Zukunft mit Q bezeichnet. Sowohl R als auch G sind Q-Bimoduln. Dem Ziel dieses Abschnitts entsprechend, soll es möglich sein, die graduierte Struktur $\mathfrak{R}$ zur Entscheidung des Enthaltenseinsproblems ein- oder zweiseitiger Ideale von R zu nutzen. Das erfordert insbesondere, daß der assoziierte graduierte Ring G ein effektiver graduierter Ring mit entscheidbarem Enthaltenseinsproblem und lösbarem Syzygienproblem endlich erzeugter Linksideale ist. Man überzeugt sich leicht davon, daß Q im Falle eines effektiven graduierten Rings G eine entscheidbare Teilmenge von G ist, womit sich die Effektivität von G auf Q überträgt. Weiterhin zeigen einfache Gradüberlegungen die Gültigkeit von $f \in QH \iff f \in GH$ und $LSyz_Q(H) = Q(B \cap Q^{|H|})$ für alle $f \in Q$ und $H \subseteq Q$, wobei B ein beliebiges homogenes Erzeugendensystem des Linkssyzygienmoduls $LSyz_G(H)$ von H aufgefaßt als Teilmenge von G bezeichnet. Somit können wir unsere Untersuchungen ohne Beschränkung der Allgemeinheit auf den Fall beschränken, daß Q ein effektiver Ring mit entscheidbarem Enthaltenseins- und lösbarem

Syzygienproblem für endlich erzeugte Linksideale ist.

Weiterhin werden wir voraussetzen, daß Γ ein noethersches Monoid ist. Diese Voraussetzung erscheint akzeptabel und ratsam zugleich, denn läßt man sie fallen, so erhält man bereits im elementaren Fall des Monoidrings $R = Q\langle\Gamma\rangle$ keinen auf der Gröbnertheorie beruhenden Entscheidungsalgorithmus des Idealenthaltenseinsproblems. Ähnliche Überlegungen rechtfertigen die Forderung, daß der Ring Q noethersch sein soll.

Darüberhinaus werden wir nur solche graduierten Strukturen betrachten, deren assoziierter graduierter Ring G ausschließlich zyklische Q-Moduln als homogene direkte Summanden hat. Am Schluß des Abschnitts werden wir noch einmal auf diese Beschränkung zurückkommen, denn im Gegensatz zu unseren bisherigen Annahmen, wurde sie nicht aus der Erreichbarkeit gewisser Berechenbarkeitsziele abgeleitet. Wenngleich ein Abrücken von der Forderung zyklischer homogener Summanden prinzipiell noch großen Raum für die Suche nach erfolgreichen Anwendungen der Gröbnertheorie graduierter Strukturen läßt, so handelt es sich doch um eine häufig gewählte Voraussetzung. Die zyklischen homogenen Summanden führen auf besonders einfache homogene Ideale und gerade das war der Schlüssel des praktischen Erfolgs der Buchbergerschen Methode. Auch basiert eine Reihe von Anwendungen der Gröbnertheorie, wie zum Beispiel die Berechnung von Eliminiationsidealen, auf Besonderheiten dieser besonders feinen graduierten Strukturen.

Ein Q-Linksmodul M heißt *zyklisch*, wenn er von einem einzigen Element erzeugt wird. Für jeden Q-Linksmodul M definiert $ann_L(M) = \{a \in Q \mid \forall m \in M : am = 0\}$ das *annullierende Linksideal* von M. Im weiteren werden wir häufig davon Gebrauch machen, daß $ann_L(M)$ sogar ein zweiseitiges Ideal von Q ist. Ein zyklischer Q-Linksmodul M ist zum Faktormodul $Q/ann_L(M)$ von Q nach seinem annullierenden Linksideal isomorph. Analoge Begriffe werden für Q-Rechtsmoduln M eingeführt, insbesondere bezeichnet $ann_R(M)$ das *annullierende Rechtsideal* des Rechtsmoduls M. Falls der Q-Bimodul M ein Element $\mathbb{1} \in M$ enthält, welches ihn sowohl als Q-Links- als auch als Q-Rechtsmodul erzeugt, so nennen wir ihn *bizyklisch*[5] und $\mathbb{1}$ ein bi-erzeugendes Element von M. Jedes bi-erzeugende Element $\mathbb{1}$ eines bizyklischen Q-Moduls M weist die Eigenschaften $a\mathbb{1} = 0 \Longleftrightarrow a \in ann_L(M)$ und $\mathbb{1}a = 0 \Longleftrightarrow a \in ann_R(M)$ auf, denn wegen $\forall b \in Q \exists b' \in Q : b\mathbb{1} = \mathbb{1}b'$ folgt auch die nichttriviale Richtung $a\mathbb{1} = 0 \Longrightarrow \forall b \in Q : ab\mathbb{1} = a\mathbb{1}b' = 0$. Für jeden bizyklischen Q-Modul M sind die Restklassenringe von Q nach den zweiseitigen Idealen $ann_L(M)$ und $ann_R(M)$ zueinander isomorph. Zum Beweis betrachten wir die durch $\sigma(a) = \{b \in Q \mid \mathbb{1}a = b\mathbb{1}\}$ definierte Abbildung $\sigma : Q \to Q/ann_L(M)$. Zur Rechtfertigung sei bemerkt, daß die oben definierten Mengen $\sigma(a)$ tatsächlich Restklassen von Q modulo des annullierenden Linksideals $ann_L(M)$ sind, denn zum ersten impliziert $b \in \sigma(a)$ trivialerweise die Inklusion $b + ann_L(M) \subseteq \sigma(a)$ und zum zweiten folgt für beliebige $b, b' \in \sigma(a)$ die Gleichheit $(b - b')\mathbb{1} = 0$ und somit $b - b' \in ann_L(M)$. Durch Nachrechnen zeigt man, daß σ ein Ringhomomorphismus mit dem Kern $ker(\sigma) = ann_R(M)$

[5] Da die Begriffsbildung "bizyklisch" bereits beinhaltet, daß es sich um einen Bimodul handeln muß, sprechen wir abkürzend von bizyklischen Q-Moduln.

ist. Da es zu jedem $b \in Q$ ein $a \in Q$ mit $b\mathbb{1} = \mathbb{1}a$ gibt und somit $b \in \sigma(a)$ gilt, ist σ surjektiv. Aus dem Homomorphiesatz folgt schließlich die behauptete Isomorphie $Q/ann_R(M) \cong Q/ann_L(M)$.

Lemma 5.17 *$\mathfrak{R}$ sei eine graduierte Ringstruktur und $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ die dadurch induzierte Filtrierung von R. Das Monoid Γ sei effektiv und R sei ein effektiver Γ-gefilterter Ring. $Q = \mathcal{F}_\epsilon \subseteq R$ sei ein noetherscher Ring mit entscheidbarem Linksidealenthaltenseinsproblem. Der Q-Linksmodul $R_\gamma = \mathcal{F}_\gamma/\hat{\mathcal{F}}_\gamma$ sei für jedes $\gamma \in \Gamma$ zyklisch. Ferner lasse sich zu jedem γ ein erzeugendes Element $\mathbb{1}_\gamma$ von R_γ und ein endliches Erzeugendensystem des annullierenden Linksideals von R_γ berechnen.*

Dann ist der assoziierte graduierte Ring bis auf Isomorphie ein effektiver Γ-graduierter Ring G mit berechenbaren Funktionen in $: R \to G$ *und* $\text{in}^* : G \to R$.

Beweis: Für alle $\gamma \in \Gamma$ bezeichne I_γ das annullierende Linksideal $ann_L(R_\gamma)$ des Q-Linksmoduls R_γ und $g_\gamma \in \mathcal{F}_\gamma$ einen beliebig festen Repräsentanten des Erzeugers $\mathbb{1}_\gamma$ der Faktorgruppe $R_\gamma = \mathcal{F}_\gamma/\hat{\mathcal{F}}_\gamma$.

Aus den Voraussetzungen des Lemmas folgt, daß die additive Gruppe des zu der graduierten Struktur $(R, \Gamma, \prec, \varphi)$ gehörigen assoziierten graduierten Rings bis auf Isomorphie gleich der direkten Summe $\hat{G} = \bigoplus_{\gamma\in\Gamma} Q/I_\gamma$ ist. Q wirkt auf $\hat{G}$ als Linksoperatorenbereich. $\hat{G}$ ist isomorph zu einem Faktorlinksmodul G des freien Q-Linksmoduls $Q\langle\Gamma\rangle$ mit freiem Erzeugendensystem $\{\mathbb{1}_\gamma \mid \gamma \in \Gamma\}$. Aufgrund der Entscheidbarkeit des Linksidealenthaltenseinsproblems von Q besitzt jeder Linksmodul Q/I_γ, $\gamma \in \Gamma$, einen kanonischen Simplifikator $\sigma_\gamma : Q \to Q$ und die Vorschrift $c_1\mathbb{1}_{\gamma_1} + \cdots + c_k\mathbb{1}_{\gamma_k} \mapsto \sigma_{\gamma_1}(c_1)\mathbb{1}_{\gamma_1} + \cdots \sigma_{\gamma_k}(c_k)\mathbb{1}_{\gamma_k}$ definiert einen kanonischen Simplifikator $S : Q\langle\Gamma\rangle \to Q\langle\Gamma\rangle$ des zu $\hat{G}$ isomorphen Linksmoduls G. Für einen effektiven Ring Q und eine rekursiv aufzählbare Menge Γ ist der freie Q-Linksmodul $Q\langle\Gamma\rangle$ eine effektive algebraische Struktur. Da G einen kanonischen Simplifikator besitzt, ist es als Faktorlinksmodul eines effektiven Q-Linksmoduls nach einer entscheidbaren Kongruenzrelation selbst ein effektiver Q-Linksmodul. Darüberhinaus ist die Zerlegung in homogene Bestandteile, das heißt, in die den direkten Summanden zuzuordnenden Bestandteile, für jedes Element $a \in G$ berechenbar. Durch Hinzunahme der induzierten Multiplikation zu G wird aus der Q-Linksmodulisomorphie zwischen G und dem assoziierten graduierten Ring $\bigoplus_{\gamma\in\Gamma} \mathcal{F}_\gamma/\hat{\mathcal{F}}_\gamma$ ein Isomorphismus Γ-graduierter Ringe.

Wir wenden uns der Definition geeigneter Abbildungen in und in^* bei Verwendung der isomorphen Darstellung G als assoziiertem graduiertem Ring zu. Die Tatsache, daß auch die Festlegung der Initialabbildung noch Wahlmöglichkeiten lassen kann, erklärt sich daraus, daß der Isomorphismus zwischen G und $\bigoplus_{\gamma\in\Gamma} \mathcal{F}_\gamma/\hat{\mathcal{F}}_\gamma$ nicht eindeutig bestimmt zu sein braucht. Zu jedem $f \in R$ mit $\varphi(f) = \gamma$ existiert ein $c \in Q$, so daß $f - cg_\gamma \in \hat{\mathcal{F}}_\gamma$. Da Q als entscheidbarer Unterring eines effektiven Rings ebenfalls effektiv ist, gibt es eine Funktion $\nu : \mathbb{N} \to Q$ die Q rekursiv aufzählt. Sukzessives Testen von $\varphi(f - \nu(i)g_\gamma) \prec \gamma$ für $i = 0, 1, \ldots$ muß nach endlicher Zeit, sagen wir für $i = i_0$, zu einem positiven Ergebnis führen. Die durch $\text{in}(f) = \sigma_\gamma(\nu(i_0))\mathbb{1}_\gamma$ definierte Funktion in $: R \to G$ ist eine geeignete Initialabbildung. Sei umgekehrt $u = c\mathbb{1}_\gamma \in G$

mit $\sigma_\gamma(c) = c \neq 0$ ein von Null verschiedenes homogenes Element von G. Dann definiert $\mathrm{in}^*(u) = cg_\gamma$ einen berechenbaren Schnitt von in.

Bisher wurde nur die Effektivität von G als Q-Linksmodul gezeigt. Es verbleibt noch der Nachweis der Berechenbarkeit der Multiplikation. Seien $u, v \in G$ beliebige homogene Elemente. Wegen $uv = 0 \Leftrightarrow \varphi(\mathrm{in}^*(u)\mathrm{in}^*(v)) \prec \deg_\Gamma(u) \circ \deg_\Gamma(v)$ ist die Frage $uv = 0$ entscheidbar. Im Fall $uv \neq 0$ läßt sich das Produkt vermöge $uv = \mathrm{in}(\mathrm{in}^*(u)\mathrm{in}^*(v))$ berechnen. □

Lemma 5.18 *Sei Q ein effektiver noetherscher Ring mit entscheidbarem Linksidealenthaltenseinsproblem und Γ ein effektives noethersches Monoid mit lösbarem Faktorisierungsproblem. Weiterhin sei $G = \bigoplus_{\gamma\in\Gamma} R_\gamma$ ein effektiver Γ-graduierter Ring, dessen direkte Summanden R_γ zyklische Q-Linksmoduln sind. Zu beliebig vorgegebenem γ seien ein erzeugendes Element $\mathbb{1}_\gamma$ sowie ein endliches Erzeugendensystem des annullierenden Linksideals $I_\gamma = ann_L(R_\gamma)$ von R_γ berechenbar.*

Dann ist das Enthaltenseinsproblem endlich erzeugter homogener Linksideale von G entscheidbar.

Falls zusätzlich eine endliche Menge $\{z_1, \ldots, z_k\} \subset Q$ existiert und berechnet werden kann, welche Q als Modul über seinem Zentrum $Z(Q)$ erzeugt, so ist auch das Enthaltenseinsproblem endlich erzeugter homogener zweiseitiger Ideale von G entscheidbar.

Beweis: $H \subseteq G$ sei eine endliche Menge homogener Elemente und $u \in G$ ein homogenes Element. Die Menge $M = \{(\gamma, w) \mid w \in H \wedge \gamma \circ \deg_\Gamma(w) = \deg_\Gamma(u)\}$ ist endlich und algorithmisch konstruierbar. Für alle $(\gamma, w) \in M$ gibt es $d_{\gamma,w} \in Q$, so daß $\mathbb{1}_\gamma w = d_{\gamma,w}\mathbb{1}_{\deg_\Gamma(u)}$. Es gilt genau dann $u \in GH$, wenn es Elemente $c_{\gamma,w} \in Q$ mit $u = \sum_{(\gamma,w)\in M} c_{\gamma,w} d_{\gamma,w} \mathbb{1}_{\deg_\Gamma(u)}$ gibt. Diese Frage ist entscheidbar, da sie auf ein Linksuntermodulenthaltenseinsproblem von $Q/ann_L(R_{\deg_\Gamma(u)})$ und damit unter Verwendung von (3.2) auf ein Linksidealenthaltenseinsproblem von Q reduziert werden kann.

Zur Untersuchung der Frage $u \in GHG$? konstruiert man ähnlich zu oben die (endliche) Menge $M = \{(\gamma, w, \gamma') \mid w \in H \wedge \gamma \circ \deg_\Gamma(w) \circ \gamma' = \deg_\Gamma(u)\}$. Aufgrund der zusätzlich an Q gestellten Voraussetzungen existieren zu beliebigen $\gamma, \gamma' \in \Gamma$, homogenem $w = a\mathbb{1}_{\deg_w}$ und $d_1, \ldots, d_k \in Z(Q)$ Elemente $d'_1, \ldots, d'_k \in Z(Q)$ mit $\mathbb{1}_\gamma w(\sum_{i=1}^k d_i z_i)\mathbb{1}_{\gamma'} = \sum_{i=1}^k (d'_i\mathbb{1}_\gamma)w(z_i\mathbb{1}_{\gamma'})$.

Damit ist $u \in GHG$ äquivalent zur Existenz von Elementen $c_{\gamma,w,\gamma',i} \in Q$, welche die Gleichung $u = \sum_{(\gamma,w,\gamma')\in M} \sum_{i=1}^k c_{\gamma,w,\gamma',i}(\mathbb{1}_\gamma w z_i \mathbb{1}_{\gamma'})$ lösen. Wie im linksseitigen Fall ist die Lösbarkeit der Gleichung auf ein Linksidealenthaltenseinsproblem von Q reduzierbar. □

Die bisher getroffenen Einschränkungen reichen nach wie vor noch nicht aus, um die Existenz eines endlichen Erzeugendensystems des Linkssyzygienmoduls $LSyz(H)$ und erst recht nicht die Lösbarkeit des Linkssyzygienproblems einer endlichen Menge H homogener Elemente zu sichern. Ähnliches trifft im zweiseitigen Fall zu. Das liegt darin begründet, daß sich alle bisherigen Forderungen auf die additive Struktur von G beziehen, wogegen die Multiplikation noch sehr große Freiheiten aufweist. Damit man die Eigenschaften von Γ für

die Lösung des Linkssyzygienproblems von G nutzbar machen kann, bedarf es einer festeren Bindung zwischen den Multiplikationen von Γ und G. Insbesondere müssen Informationen über die Nullteiler von G bereitgestellt werden. Bisher ist sogar folgendes Extrembeispiel einer graduierten Struktur $\mathfrak{R}$ zulässig. Sei $R = \mathbb{K}[X]$ der Polynomring über dem Körper $\mathbb{K}$ in der endlichen Menge X von Unbestimmten. Als Wertemonoid dient das Kreuzprodukt $\Gamma = T(X) \times \mathbb{N}$ der Monoide der Potenzprodukte in X und der natürlichen Zahlen geordnet durch das lexikographische Produkt $\prec$ einer beliebigen Monoidwohlordnung $\prec_X$ von $T(X)$ und der gewöhnlichen Kleinerordnung $<$ von $\mathbb{N}$. Die Pseudobewertung erfülle $\varphi(c) = (1, 0)$ für alle von Null verschiedenen Skalare $0 \neq c \in \mathbb{K}$ und $\varphi(p) = (\mathrm{lpp}_{\prec_X}(p), 1)$ für alle nichtskalaren Polynome $p \in R \backslash \mathbb{K}$. Als $\mathbb{K}$-Vektorraum ist der assoziierte graduierte Ring G der Struktur $\mathfrak{R}$ isomorph zu R, aber der Initialterm $\mathrm{in}(p)$ eines beliebigen nichtskalaren Polynoms $p \in R$ ist Nullteiler von G. Mehr noch, das Produkt der Initialterme zweier beliebiger nichtskalarer Polynome ist in jedem Fall gleich Null.

Lemma 5.19 *Sei Q ein effektiver noetherscher Ring mit entscheidbarem Linksidealenthaltenseins- und lösbarem Linkssyzygienproblem und Γ ein effektives noethersches Monoid mit lösbarem Faktorisierungsproblem. Zu jeder endlichen Teilmenge $\Omega \subseteq \Gamma$ sei die Menge $mgRV(\Omega)$ aller minimalen gemeinsamen Rechtsvielfachen der Elemente von Ω algorithmisch konstruierbar. Weiterhin sei $G = \bigoplus_{\gamma \in \Gamma} R_\gamma$ ein effektiver Γ-graduierter Ring. Jeder direkte Summand R_γ von G sei bizyklischer Q-Modul und für alle $\gamma, \omega \in \Gamma$ gelte die Beziehung $R_\gamma R_\omega = R_{\gamma \circ \omega}$. Zu beliebig vorgegebenem γ seien ein bi-erzeugendes Element $\mathbb{1}_\gamma$ von R_γ und ein endliches Erzeugendensystem des annullierenden Linksideals I_γ des Q-Linksmoduls R_γ berechenbar. Schließlich sei für jedes $\gamma \in \Gamma$ entscheidbar, ob die Menge*

$$\Gamma_\gamma = \{\omega \in \Gamma \mid Q/I_\gamma \ncong Q/I_{\omega \circ \gamma}\}$$

leer ist und falls nicht, so sei ein endliches Monoidlinksidealerzeugendensystem B_γ von Γ_γ auf algorithmischem Wege konstruierbar.

Unter diesen Voraussetzungen ist der Ring G noethersch und hat ein lösbares Linkssyzygienproblem für endlich erzeugte homogene Linksideale.

Beweis: Bevor wir mit dem Beweis der eigentlichen Aussagen beginnen, wenden wir uns dem Aufbau der Menge Γ_γ zu. Für beliebige ω und γ ist das Produkt $\mathbb{1}_\omega \mathbb{1}_\gamma$ ein bi-erzeugendes Element des Moduls $R_{\omega \circ \gamma}$, weshalb $c\mathbb{1}_\omega \mathbb{1}_\gamma = 0$ genau für die Elemente $c \in I_{\omega \circ \gamma}$ gilt. Es ergibt sich $I_\omega \subseteq I_{\omega \circ \gamma}$, also ist der Restklassenring $Q/I_{\omega \circ \gamma}$ homomorphes Bild von Q/I_ω. Anwendung der gleichen Überlegungen auf die annullierenden Rechtsideale der Q-Rechtsmoduln zeigt, daß auch $Q/ann_R(R_{\omega \circ \gamma})$ homomorphes Bild von $Q/ann_R(R_\gamma)$ ist. Ausnutzung der Isomorphie der Restklassenringe von Q modulo der annullierenden Ideale beider Seitigkeiten liefert schließlich die Existenz eines Epimorphismus $\sigma_{\omega,\gamma} : Q/I_\gamma \longrightarrow Q/I_{\omega \circ \gamma}$. Da Q noethersch ist, ist die Zugehörigkeit von ω zur Menge Γ_γ gleichbedeutend mit $\{0\} \subsetneqq ker(\sigma_{\omega,\gamma})$. Für beliebige $\omega \in \Gamma_\gamma$ und $\omega' \in \Gamma$ haben wir die Sequenz

$$Q/I_\gamma \xrightarrow{\sigma_{\omega,\gamma}} Q/I_{\omega \circ \gamma} \xrightarrow{\sigma_{\omega',\omega \circ \gamma}} Q/I_{\omega' \circ \omega \circ \gamma}$$

von Epimorphismen. Da $\sigma_{\omega,\gamma}$ kein Monomorphismus ist, kann auch $\sigma_{\omega,\gamma} \circ \sigma_{\omega',\omega\circ\gamma}$ nicht injektiv sein und folglich gilt $\omega' \circ \omega \in \Gamma_\gamma$. Damit ist zunächst bewiesen, daß jede nichtleere Menge Γ_γ tatsächlich ein Monoidlinksideal von Γ ist.

i) Zum Nachweis des Rechtsnoetherschseins des Γ-graduierten Rings G werden wir zeigen, daß es in jeder unendlichen Folge homogener Elemente ein Element gibt, welches im von seinen Vorgängern erzeugten Rechtsideal liegt. Sei $u_1 = c_1 \mathbb{1}_{\gamma_1}, u_2 = c_2 \mathbb{1}_{\gamma_2}, \ldots$ eine beliebige unendliche Folge homogener Elemente von G, wobei $0 \neq c_i \in Q$ und $\gamma_i \in \Gamma$. Mit Hilfe der in Abschnitt 4.1 bewiesenen Eigenschaften noetherscher Monoide schließt man auf die Existenz einer unendlichen Teilfolge $u_{i_1}, u_{i_2}, \ldots$ mit $\gamma_{i_j} \lfloor \gamma_{i_{j+1}}$ für alle $j = 1, 2, \ldots$. Da Q nach Voraussetzung noethersch ist, gibt es eine natürliche Zahl $k > 1$, so daß c_{i_k} Element des von $\{c_{i_1}, \ldots, c_{i_{k-1}}\}$ erzeugten Rechtsideals von Q ist, mit anderen Worten: es existieren $d_1, \ldots, d_{k-1} \in Q$ mit $c_{i_k} = \sum_{j=1}^{k-1} c_{i_j} d_j$. Für jedes $j = 1, \ldots, k-1$ gibt es $\omega_j \in \Gamma$ und $a_j \in Q$ mit $\mathbb{1}_{\gamma_{i_k}} = \mathbb{1}_{\gamma_{i_j}} \mathbb{1}_{\omega_j} a_j$ und es folgt $u_{i_k} = \sum_{j=1}^{k-1} c_{i_j} d_j \mathbb{1}_{\gamma_{i_k}} = \sum_{j=1}^{k-1} c_{i_j} (d_j \mathbb{1}_{\gamma_{i_j}}) \mathbb{1}_{\omega_j} a_j = \sum_{j=1}^{k-1} u_{i_j} d'_j \mathbb{1}_{\omega_j} a_j$. Also kann es keine unendlichen, echt aufsteigenden Ketten homogener Rechtsideale geben und G ist rechtsnoethersch.

Zum Nachweis, daß G auch linksnoethersch ist, stellt man die Elemente u_i in der Form $u_i = \mathbb{1}_{\gamma_i} c'_i$ dar und verfährt analog.

ii) Sei H eine endliche Menge homogener Elemente von G. Ziel ist es, eine endliche Menge $B(H)$ homogener Linkssyzygien von H zu konstruieren, für welche $B(H) \cup \bigcup_{H' \subsetneq H} LSyz(H')$ den Linkssyzygienmodul $LSyz(H)$ erzeugt[6]. Durch rekursive Anwendung des Verfahrens kann dann ein endliches Erzeugendensystem von $LSyz(H)$ berechnet werden.

Für jede homogene Linkssyzygie $s \in LSyz(H)$, die nicht bereits Linkssyzygie einer echten Teilmenge von H ist, gilt $\deg_\Gamma(u) \rfloor \deg_\Gamma(s)$ für alle $u \in H$. Sei $\gamma \in \Gamma$ ein beliebiges Monoidelement, welches alle $\deg_\Gamma(u)$, $u \in H$, als Postfix hat. Zu jedem $u \in H$ kann effektiv das Element $\gamma_u \in \Gamma$ mit $\gamma_u \circ \deg_\Gamma(u) = \gamma$ berechnet werden. Außerdem läßt sich auf algorithmischem Wege ein endliches Erzeugendensystem D_γ des Linkssyzygienmoduls der Menge $\{d_{\gamma,u} + I_\gamma \in Q/I_\gamma \mid u \in H \wedge \mathbb{1}_{\gamma_u} u = d_{\gamma,u} \mathbb{1}_\gamma\}$ bestimmen. Multipliziert man jede Komponente einer Linkssyzygie $s_Q \in D_\gamma$ von rechts mit dem entsprechenden Element $\mathbb{1}_{\gamma_u}$, wobei sich u auf die zu $d_{\gamma,u}$ gehörige Komponente bezieht, so ergibt sich eine homogene Linkssyzygie $s \in LSyz(H)$ vom Grad γ. Die Menge dieser Linkssyzygien von H bezeichnen wir mit $\tilde{D}_\gamma$.

Sei $s = \sum_{u \in H} c_u \mathbb{1}_{\gamma_u} e_u$ eine beliebige homogene Linkssyzygie von H, die nicht bereits Linkssyzygie einer echten Teilmenge von H ist. Für beliebige $\gamma, \omega \in \Gamma$ mit $\forall u \in H \; : \; \deg_\Gamma(u) \rfloor \omega$ und $\gamma \circ \omega = \deg_\Gamma(s)$ läßt sich s in die Gestalt $s = \mathbb{1}_\gamma \sum_{u \in H} d_u \mathbb{1}_{\gamma'_u} e_u$ umschreiben. Es existiert ein $d \in Q$ mit $\sum_{u \in H} d_u \mathbb{1}_{\gamma'_u} u = \mathbb{1}_\omega d$ und dieses erfüllt $d \in ann_R(R_{\deg_\Gamma(s)}) \supseteq ann_R(R_\omega)$. Gilt sogar $d \in ann_R(R_\omega)$, was insbesondere bei Gleichheit der beiden annullierenden Rechtsideale immer der Fall ist, dann ist $s' = \sum_{u \in H} d_u \mathbb{1}_{\gamma'_u} e_u$ eine Linkssyzygie von H. Somit gehören alle homogenen Linkssyzygien $s \in LSyz(H)$ für die

[6] Dabei werden die Linkssyzygienmoduln $LSyz(H')$ auf natürliche Weise in den freien G-Linksmodul $G^{|H|}$ eingebettet.

ein gemeinsames Rechtsvielfaches ω der Γ-Grade der Elemente von H existiert, so daß $\omega \rfloor \deg_\Gamma(s)$ und $Q/I_\omega \cong Q/I_{\deg_\Gamma(s)}$ erfüllt sind, dem von $\tilde{D}_\omega$ erzeugten G-Linksmodul an. Wir erinnern daran, daß B_γ im Fall $\Gamma_\gamma \neq \emptyset$ ein endliches Monoididealerzeugendensystem von Γ_γ bezeichnet und setzen formal $B_\gamma = \emptyset$ für alle $\gamma \in \Gamma$ mit $\Gamma_\gamma = \emptyset$. Die induktive Definition

$$\begin{aligned} \Omega(H)_0 &= mgRV(\deg_\Gamma(H)), \\ \Omega(H)_{i+1} &= \{\gamma' \circ \gamma \mid \gamma \in \Omega(H)_i \wedge \gamma' \in B_\gamma\} \end{aligned}$$

liefert eine Menge $\Omega(H) = \bigcup_{i=1}^{\infty} \Omega(H)_i$, welche zu jeder Syzygie s ein den obigen Anforderungen genügendes Monoidelement ω enthält. Wir setzen $B(H) = \bigcup_{\omega \in \Omega(H)} \tilde{D}_\omega$ und stellen fest, daß $B(H) \cup \bigcup_{H' \subsetneq H} LSyz(H')$ homogenes Erzeugendensystem des Linkssyzygienmoduls $LSyz(H)$ ist. Jede der Mengen $\Omega(H)_i$ ist endlich und algorithmisch konstruierbar. Falls es ein i_0 mit $\Omega(H)_{i_0} = \emptyset$ gibt, so folgt $\Omega(H)_i = \emptyset$ für alle $i \geq i_0$. Angenommen, keine der Mengen $\Omega(H)_i$ wäre leer, dann gäbe es unendliche Folgen $\gamma_0, \gamma_1, \ldots$ und $\gamma'_0, \gamma'_1, \ldots$ mit $\gamma_i \in \Omega(H)_i$, $\gamma'_i \in B_{\gamma_i}$ und $\gamma_{i+1} = \gamma'_i \circ \gamma_i$ für alle $i = 0, 1, \ldots$. Das hätte, im Widerspruch zur Voraussetzung, daß der Ring Q noethersch ist, die Existenz einer unendliche Sequenz $Q/I_{\gamma_0} \longrightarrow Q/I_{\gamma_1} \longrightarrow \cdots$ nicht injektiver Epimorphismen zur Folge. Also sind $\Omega(H)$ und damit auch $B(H)$ endlich und berechenbar. Die Berechenbarkeit der Menge $\bigcup_{H' \subseteq H} B(H')$ löst das Linkssyzygienproblem für H. □

Unter zusätzlichen Voraussetzungen an Q und die annullierenden Linksideale I_γ der Q-Moduln R_γ kann die Berechnung eines Erzeugendensystems des Linkssyzygienmoduls $LSyz(H)$ stark vereinfacht werden.

Gilt $I_\gamma = \{0\}$ für alle $\gamma \in \Gamma$, so sind alle Mengen $\Omega(H)_i$ mit $i \geq 1$ leer und es brauchen nur die Grade ω untersucht zu werden, die minimales gemeinsames Rechtsvielfaches der Grade einer gewissen Teilmenge von H sind.

Ein weiterer interessanter Spezialfall ist der eines *Hauptidealrings* Q, das heißt Q ist ein nullteilerfreier kommutativer Ring mit Einselement, in welchem jedes Ideal von einem einzigen Element erzeugt wird. Der Syzygienmodul $Syz(F)$ einer beliebigen endlichen Teilmenge $F = \{f_1, \ldots, f_m\}$ eines Hauptidealrings Q wird von Syzygien der Gestalt $g_{i,j} e_{f_i} + k_{i,j} e_{f_j}$, wobei $1 \leq i < j \leq m$, erzeugt und darüberhinaus benötigt man höchstens eine Syzygie zu jedem Paar $(f_i, f_j) \in F \times F$. Das erlaubt die Beschränkung auf die Untersuchung der höchstens zweielementigen Teilmengen von H bei der Berechnung eines Erzeugendensystems von $LSyz(H)$.

Treten beide Spezialfälle gleichzeitig auf, das heißt: Q ist Hauptidealring und alle annullierenden Linksideale I_γ sind Nullideale, dann vereinfacht sich die Berechnung entsprechend weiter. In diesem Fall ist G nullteilerfrei, weshalb sich die Einbeziehung der einelementigen Teilmengen von H erübrigt. Wir erhalten ein homogenes Erzeugendensystem von $LSyz(H)$, welches aus höchstens einer Linkssyzygie $s_{i,j} = u_{i,j} e_i + v_{i,j} e_j$ für jedes Paar $h_i, h_j \in H$ besteht. Damit sind wir schließlich beim originalen Buchbergerschen Ansatz der kritischen Paare angelangt und das Element $\textsc{Lift}(s_{i,j})$ entspricht gerade dem Buchbergerschen *S-Polynom* (siehe [Bu85]).

Satz 5.20 *Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur und $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ die dadurch induzierte Filtrierung von R. Γ sei ein effektives noethersches Monoid mit lösbarem Faktorisierungsproblem und zu jeder endlichen Teilmenge $\Omega \subseteq \Gamma$ sei die Menge $mgRV(\Omega)$ der minimalen gemeinsamen Rechtsvielfachen von Ω algorithmisch konstruierbar. Weiterhin seien R ein effektiver Γ-gefilterter Ring und $Q = \mathcal{F}_\epsilon = R_\epsilon$ ein noetherscher Ring mit entscheidbarem Linksidealenthaltenseins- und lösbarem Linkssyzygienproblem. Jeder Faktormodul $R_\gamma = \mathcal{F}_\gamma/\hat{\mathcal{F}}_\gamma$ sei bizyklisch und für alle $\gamma, \omega \in \Gamma$ gelte die Beziehung $R_\gamma R_\omega = R_{\gamma\circ\omega}$. Zu beliebig vorgegebenem γ seien ein bi-erzeugendes Element $\mathbb{1}_\gamma$ von R_γ und ein endliches Erzeugendensystem des annullierenden Linksideals I_γ des Q-Linksmoduls R_γ berechenbar. Schließlich sei für jedes $\gamma \in \Gamma$ entscheidbar, ob die Menge*

$$\Gamma_\gamma = \{\omega \in \Gamma \mid Q/I_\gamma \ncong Q/I_{\omega\circ\gamma}\}$$

leer ist und falls nicht, so sei ein endliches Monoidlinksidealerzeugendensystem B_γ von Γ_γ auf algorithmischem Wege konstruierbar.

Unter diesen Voraussetzungen ist $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine effektive graduierte Linksgröbnerstruktur.

Beweis: Die Behauptung folgt unmittelbar aus den Lemmata 5.17, 5.18 und 5.19. □

Die einfachsten Beispiele für Ringe mit graduierten Strukturen der beschriebenen Art sind die Monoidringe $Q\langle\Gamma\rangle$, wobei Q und $(\Gamma, \prec)$ den Voraussetzungen des Satzes genügen. Diese gehen durch Ringadjunktion des Monoids Γ zu Q hervor, dabei kommutieren alle Elemente von Q mit allen Elementen von Γ und die Elemente von Γ werden entsprechend der Monoidoperation miteinander multipliziert. Die Funktion lpp weise jedem Nichtnullelement von $Q\langle\Gamma\rangle$ das maximale darin vorkommende Element von Γ zu, dann ist $(Q\langle\Gamma\rangle, \Gamma, \prec, \text{lpp})$ eine effektive graduierte Linksgröbnerstruktur des beschriebenen Typs. Der Ring Q kann beispielsweise ein effektiver Körper, ein effektiver Schiefkörper oder ein effektiver Euklidischer Ring sein. Ebenso darf es sich um einen selbst einer effektiven graduierten Linksgröbnerstruktur $(Q, \Omega, \prec_\Omega, \varphi_\Omega)$ angehörigen Ring Q handeln. Mögliche Monoide Γ sind beispielsweise die endlich erzeugten freien kommutativen Monoide $T(X)$ mit Wohlordnungen des in (4.5) beschriebenen Typs basierend auf einer Matrix mit rationalen Einträgen. In diesem Fall erhalten wir die Polynomringe in endlich vielen Unbestimmten über einem zulässigen Ring Q. Am Rande sei erwähnt, daß die Verwendung freier nichtkommutativer Monoide $S(X)$ mit $|X| > 1$ unzulässig ist, da diese nicht noethersch sind.

Kommen wir zu einer weiteren Klasse geeigneter Ringe. Sei $R = Q\langle X\rangle/J$ Restklassenring eines durch Adjunktion des Monoids $S(X)$, wobei X endlich ist, zu einem den Anforderungen des Satzes genügenden Koeffizientenring Q entstehenden Monoidrings $Q\langle X\rangle = Q\langle S(X)\rangle$. $\prec$ sei eine Monoidwohlordnung von $S(X)$ und ihre Einschränkung (im Sinne der in Abschnitt 4.1 vereinbarten Mengeninklusion $T(X) \subseteq S(X)$) auf $T(X)$ sei eine Monoidordnung von $T(X)$. Außerdem soll $\prec$ zwei Elemente von $S(X)$ zuerst unter Vernachlässigung der Nichtkommutativität vergleichen und verbleibende Unentscheidbarkeiten durch einen lexikographischen Vergleich in $S(X)$ beseitigen. Durch diese Vorgaben

wird eine graduierte Struktur $(Q\langle X\rangle, S(X), \prec, \mathrm{lpp})$ festgelegt. Am Rande sei bemerkt, daß es sich dabei nur in trivialen Ausnahmefällen um eine effektive graduierte (Links-, Rechts-) Gröbnerstruktur handelt. Von dem zweiseitiges Ideal $J \subseteq Q\langle X\rangle$ wird gefordert, daß es zu jedem Paar $(x,y) \in X \times X$ ein Element der Gestalt $yx - c_{x,y}xy + p(x,y)$ enthält, wobei $c_{x,y} \in Q$ eine Einheit ist und $\mathrm{lpp}(p(x,y)) \prec \min(xy, yx)$ gilt. Darüberhinaus soll J eine endliche Gröbnerbasis bezüglich der graduierten Struktur $(Q\langle X\rangle, S(X), \prec, \mathrm{lpp})$ besitzen und durch eine solche gegeben sein.[7] Dann genügt die graduierte Struktur $\left(Q\langle X\rangle/J, T(X), \prec|_{T(X)}, \mathrm{lpp}_J\right)$ mit $\mathrm{lpp}_J(p+J) = \min\{\mathrm{lpp}(q) \mid q \in p+J\}$ den Voraussetzungen von Satz 5.20 und ist daher effektive Linksgröbnerstruktur. Klassische Beispiele derartiger Strukturen sind die Algebren von auflösbarem Typ, für sie wird die schärfere Anforderung gestellt, daß bereits die Menge $\{yx - c_{x,y}xy + p(x,y) \mid x,y \in X\}$ eine Gröbnerbasis von J ist. Auch die umfangreichere Klasse der G-Algebren wird hier überdeckt.

Auch die auflösbaren Polynomringe können mittels Satz 5.20 behandelt werden. Zusätzlich zu den oben betrachteten Relationen $yx = c_{x,y}xy + p(x,y)$ sind in ihnen auch solche der Gestalt $xa = c_{x,a}ax + b_{x,y}$, wobei $x \in X$, $a, b_{x,y} \in Q$ und $c_{x,a} \in Q$ Einheit, zugelassen. Die Konstruktion der entsprechenden graduierten Struktur ist offensichtlich.

Im Unterschied zu vielen in der Literatur untersuchten Spezialfällen läßt der hier dargestellte Kalkül eine größere Freiheit bei der Festlegung des Koeffizientenbereichs Q und des Wertemonids Γ. Legt man einen Epimorphismus $\tau : S(X) \to \Gamma$ geordneter Monoide zugrunde, so läßt sich beispielsweise die Grundidee der G-Algebren auf ein beliebiges den Voraussetzungen des Satzes genügendes Wertemonoid Γ übertragen, indem man die Anforderung an J dahingehend verallgemeinert, daß zu jedem $t \in S(X)$ ein Element der Gestalt $t + c_t s + p(t) \in J$ existieren muß, für welches $c_t \in Q$ Einheit ist und die Beziehung $\mathrm{lpp}(p_t) \prec s = \min\{u \mid \tau(u) = \tau(t)\}$ gilt. Die Forderung der Vorgabe von J durch eine endliche Gröbnerbasis wird aufrecht erhalten.

Erfüllt die graduierte Struktur $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ die Anforderungen von Satz 5.20 und erfüllt auch $(\Omega, \prec_\Omega)$ die in Satz 5.20 an das Wertemonoid gestellten Bedingungen, dann ist $\mathfrak{R}\langle\Omega\rangle = (R\langle\Omega\rangle, \Omega \times \Gamma, \prec_{\Omega\times\Gamma}, \varphi_{R\langle\Omega\rangle})$ ebenfalls vom in Satz 5.20 beschriebenen Typ. Dabei bezeichnet $\prec_{\Omega\times\Gamma}$ das lexikographische Produkt von $\prec_\Omega$ und $\prec$ und es gilt per definitionem $\varphi_{R\langle\Omega\rangle}(\sum_{i=1}^k r_i\omega_i) = \max_{\prec_{\Omega\times\Gamma}}\{(\omega_i, \varphi(r_i)) \mid 1 \le i \le k\}$.

Wenden wir uns nunmehr der Lösung des Syzygienproblems zweiseitiger homogener Ideale von G zu, dazu schränken wir die Klasse der untersuchten graduierten Struktur durch zusätzliche Forderungen an den assoziierten graduierten Ring G weiter ein. A bezeichne den von den Initialtermen aller Elemente des Zentrums $Z(R)$ von R erzeugten Unterring von G. Darüberhinaus bezeich-

[7] Tatsächlich benötigt man nur die Entscheidbarkeit des Enthaltenseinsproblems von J und für jedes $t \in T(X)$ die Berechenbarkeit endlich vieler Elemente $ct + r(c,t)$ mit $\mathrm{lpp}(r(c,t)) \prec t$, so daß ihre Restklassen modulo $\hat{\mathcal{F}}_t$ den Faktormodul $\mathcal{F}_t/\hat{\mathcal{F}}_t$ erzeugen. Damit kann die Forderung, J durch eine endliche Gröbnerbasis vorzugeben, mitunter abgeschwächt werden. Ist J beispielsweise ein homogenes Ideal des $S(X)$-graduierten Rings $Q\langle X\rangle$, dann reicht die Vorgabe eines beliebigen endlichen Erzeugendensystems aus, da sich daraus zu jedem $t \in T(X)$ eine unterhalb t abgeschnittene Gröbnerbasis von J bestimmen läßt.

ne $\hat{Q} = Q \cap Z(R) = Q \cap A$ im weiteren den aus allen zu A gehörigen homogenen Elementen vom Grad ϵ bestehenden Unterring von Q. Während der Diskussion des Algorithmus NONTRIV stellten wir fest, daß anstelle des Syzygienmoduls $Syz(H) \subseteq (G \otimes_U G)^{|H|}$ sein homomorphes Bild $Syz(H)/ker(\iota_A) \subseteq (G \otimes_A G)^{|H|}$ betrachtet werden kann. Der Einfachheit halber vereinbaren wir, daß sich die Bezeichnung $Syz(H)$ in Zukunft auf dieses homomorphe Bild bezieht. Hintergrund des anschließenden Lemmas ist die weitgehende Rückführung des zweiseitigen auf den einseitigen Falls mittels der Kandri-Rody/Weispfenning-Vervollständigungstechnik, die wir hier in einem allgemeineren Kontext wiedertreffen.

Lemma 5.21 *Das Wertemonoid Γ sei kommutativ und werde von der Menge X erzeugt. Jeder direkte Summand R_γ des Γ-graduierten Rings G sei bizyklischer Q-Modul mit bi-erzeugendem Element $\mathbb{1}_\gamma$. Es existiere eine Funktion $\delta : Q \times Q \to Q$ mit der Eigenschaft $c \cdot d = \delta(c,d) \cdot c$ für alle $c, d \in Q$. Weiterhin existiere eine Funktion $\delta_X : X \times Q \to Q$ mit $c \cdot \mathbb{1}_x = \delta_X(x,c) \cdot \mathbb{1}_x \cdot c$ für alle $x \in X$ und $c \in Q$. Schließlich gelte für alle $\gamma, \omega \in \Gamma$ die Beziehung $R_\gamma R_\omega = R_{\gamma \circ \omega}$.*

Sei H eine endliche Menge homogener Elemente von G und Z ein Erzeugendensystem von Q betrachtet als $\hat{Q}$-Modul. Dann existieren zu jedem Paar $(z,u) \in Z \times H$ eine homogene Syzygie der Bauart $s_{z,u} = e_u z - d_{z,u} e_u \in Syz(H)$ und zu jedem Paar $(x,u) \in X \times H$ eine homogene Syzygie der Gestalt $s_{x,u} = e_u \mathbb{1}_x - c_{x,u} \mathbb{1}_x e_u \in Syz(H)$. Seien B_Z eine Menge bestehend aus einer homogenen Syzygie $s_{z,u}$ für jedes Paar $(z,u) \in Z \times H$ und B_X eine Menge bestehend aus einer homogenen Syzygie $s_{x,u}$ für jedes Paar $(x,u) \in X \times H$. Dann erzeugt die Vereinigungsmenge $B_X \cup B_Z \cup LSyz(H) \otimes_A 1$ den Syzygienmodul $Syz(H) \subseteq (G \otimes_A G)^{|H|}$.

Beweis: Seien $z \in Z$ und $u = c_u \mathbb{1}_{\deg_\Gamma(u)} \in H$ beliebig. Da $R_{\deg_\Gamma(u)}$ als Q-Links- und als Q-Rechtsmodul von $\mathbb{1}_{\deg_\Gamma(u)}$ erzeugt wird, existiert ein $d \in Q$ mit $uz = c_u d \mathbb{1}_{\deg_\Gamma(u)} = \delta(c_u,d) c_u \mathbb{1}_{\deg_\Gamma(u)} = \delta(c_u,d) u$. Wir setzen $d_{z,u} = \delta(c_u,d)$ und die Existenz einer Syzygie $s_{z,u}$ ist nachgewiesen.

Seien nun $x \in X$ und $u = c_u \mathbb{1}_{\deg_\Gamma(u)} \in H$ beliebig. Auf ähnliche Weise weist man unter Verwendung der Beziehung $R_{\deg_\Gamma(u)} R_x = R_{x \circ \deg_\Gamma(u)} = R_x R_{\deg_\Gamma(u)}$ die Existenz von $d, d' \in Q$ nach, so daß $u\mathbb{1}_x = c_u \mathbb{1}_{\deg_\Gamma(u)} \mathbb{1}_x = c_u d \mathbb{1}_{\deg_\Gamma(u) \circ x} = c_u d' \mathbb{1}_x \mathbb{1}_{\deg_\Gamma(u)} = \delta(c_u,d') \delta_X(x,c_u) \mathbb{1}_x c_u \mathbb{1}_{\deg_\Gamma(u)} = \delta(c_u,d') \delta_X(x,c_u) \mathbb{1}_x u$. Mit $c_{x,u} = \delta(c_u,d') \delta_X(x,c_u)$ erhält man eine Syzygie $s_{x,u}$ der verlangten Bauart.

Jedes $a \in Q$ besitzt eine endliche Summendarstellung der Gestalt $a = \sum_{z \in Z} a_z z$, $a_z \in \hat{Q}$. Also enthält der von B_Z in $(G \otimes_A G)^{|H|}$ erzeugte G-Biuntermodul für beliebige $a \in Q$ und $u \in H$ eine Syzygie der Gestalt $s_{a,u} = \sum_{z \in Z} a_z s(z,u) = e_u a - d_{a,u} e_u \in Syz(H)$, wobei $d_{a,u} = \sum_{z \in Z} a_z d_{z,u}$.

Als nächstes zeigen wir, daß zu jedem Paar $(\gamma, u) \in \Gamma \times H$ eine homogene Syzygie $s_{\gamma,u} = e_u \mathbb{1}_\gamma - c_{\gamma,u} \mathbb{1}_\gamma e_u \in Syz(H)$ existiert, welche dem von $B = B_X \cup B_Z$ erzeugten G-Biuntermodul $GBG \subseteq (G \otimes_A G)^{|H|}$ angehört. Sei $\gamma = x_1 \circ \cdots \circ x_k$ eine beliebige Darstellung von γ im Erzeugendensystem X.

Wir bedienen uns des Prinzips der vollständigen Induktion über k. Der Induktionsanfang $k = 1$ ist trivial, denn die Menge B_X enthält bereits eine geeignete Syzygie. Sei $k > 1$ und $\gamma' = x_1 \circ \cdots \circ x_{k-1}$. Es gibt ein $a \in Q$

mit $e_u \mathbb{1}_{\gamma' \circ x_k} = e_u \mathbb{1}_{x_k} \mathbb{1}_{\gamma'} a = s_{x_k,u} \mathbb{1}_{\gamma'} a + c_{x_k,u} \mathbb{1}_{x_k} e_u \mathbb{1}_{\gamma'} a$. Nach Induktionsvoraussetzung existiert eine Syzygie $s_{\gamma',u} = e_u \mathbb{1}_{\gamma'} - c_{\gamma',u} \mathbb{1}_{\gamma'} e_u \in GBG$ und somit $e_u \mathbb{1}_{\gamma' \circ x_k} = s_{x_k,u} \mathbb{1}_{\gamma'} a + c_{x_k,u} \mathbb{1}_{x_k} s_{\gamma',u} a + c_{x_k,u} \mathbb{1}_{x_k} c_{\gamma',u} \mathbb{1}_{\gamma'} e_u a = s_{x_k,u} \mathbb{1}_{\gamma'} a + c_{x_k,u} \mathbb{1}_{x_k} s_{\gamma',u} a + c_{x_k,u} \mathbb{1}_{x_k} c_{\gamma',u} \mathbb{1}_{\gamma'} s_{a,u} + c_{x_k,u} \mathbb{1}_{x_k} c_{\gamma',u} \mathbb{1}_{\gamma'} d_{a,u} e_u$.

Damit ist für alle $(\gamma, u) \in \Gamma \times H$ die Existenz einer homogenen Syzygie $s_{\gamma,u} = e_u \mathbb{1}_\gamma - c_{\gamma,u} \mathbb{1}_\gamma e_u \in GBG$ nachgewiesen und es folgt, daß es zu jeder homogenen Syzygie $s = \sum_{j=1}^{k} v_j e_{u_j} w_j \in Syz(H)$ eine Linkssyzygie $s' = \sum_{j=1}^{k} c_j \mathbb{1}_{\deg_\Gamma(v_j w_j)} e_{u_j}$ mit $s - s' \in GBG$ gibt. □

Die Forderung nach der Existenz der Funktionen δ und δ_X mag zunächst einen sehr technischen Eindruck hinterlassen. Als wichtige Spezialfälle könnte man stattdessen auch eine der beiden stärkeren Bedingungen verlangen, daß Q ein Schiefkörper ist oder daß Q ganz im Zentrum von R enthalten ist.

Satz 5.22 *Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur mit effektivem Γ-gefiltertem Ring R. Das Monoid Γ sei kommutativ, noethersch und effektiv und habe das minimale Erzeugendensystem X. Das Faktorisierungsproblem von Γ sei lösbar und zu jeder endlichen Menge $\Omega \subseteq \Gamma$ sei die Menge $mgRV(\Omega)$ der minimalen gemeinsamen Rechtsvielfachen aller Elemente von Ω berechenbar. Weiterhin sei Q als $\hat{Q}$-Modul endlich erzeugt und ein endliches Erzeugendensystem Z sei algorithmisch konstruierbar. Außerdem wird die Existenz berechenbarer Funktionen $\delta : Q \times Q \to Q$ und $\delta_X : X \times Q \to Q$ mit $c \cdot d = \delta(c,d) \cdot c$ und $c \cdot \mathbb{1}_x = \delta_X(x,c) \cdot \mathbb{1}_x \cdot c$ für alle $c, d \in Q$ und $x \in X$ vorausgesetzt. Der Ring Q sei noethersch und habe ein entscheidbares Linksidealenthaltenseinsproblem sowie ein lösbares Linkssyzygienproblem. Jeder homogene direkte Summand R_γ des assoziierten graduierten Rings G sei bizyklischer Q-Modul und zu jedem $\gamma \in \Gamma$ seien ein bi-erzeugendes Element $\mathbb{1}_\gamma$ von R_γ und ein endliches Erzeugendensystem des annullierenden Linksideals $I_\gamma = ann_L(R_\gamma)$ berechenbar. Schließlich gelte für alle $\gamma, \omega \in \Gamma$ die Beziehung $R_\gamma R_\omega = R_{\gamma \circ \omega}$ und für jedes $\gamma \in \Gamma$ sei entscheidbar, ob die Menge*

$$\Gamma_\gamma = \{\omega \in \Gamma \mid Q/I_\gamma \ncong Q/I_{\omega \circ \gamma}\}$$

leer ist und falls nicht, so sei ein endliches Monoidlinksidealerzeugendensystem B_γ von Γ_γ auf algorithmischem Wege konstruierbar.

Dann ist $\mathfrak{R}$ sowohl effektive graduierte Linksgröbnerstruktur als auch effektive graduierte Gröbnerstruktur. Sei I ein zweiseitiges Ideal von R. Dann ist jede Gröbnerbasis des zweiseitigen Ideals I bezüglich der graduierten Struktur $\mathfrak{R}$ auch eine Gröbnerbasis des Linksideals I bezüglich $\mathfrak{R}$.

Beweis: Der assoziierte graduierte Ring von $\mathfrak{R}$ erfüllt die Voraussetzungen von Satz 5.20, somit ist $\mathfrak{R}$ eine effektive Linksgröbnerstruktur. Nach Lemma 5.18 ist das Idealenthaltenseinsproblem endlich erzeugter zweiseitiger homogener Ideale von G entscheidbar. Sei H eine beliebige endliche Menge homogener Elemente von G. Insbesondere sind dann auch die Mengen $Z \times H$ und $X \times H$ endlich. Die gemachten Berechenbarkeitsvoraussetzungen sichern ab, daß zu jedem Paar $(z,u) \in Z \times H$ und zu jedem Paar $(x,u) \in X \times H$ eine geeignete Syzygie $s_{z,u}$ beziehungsweise $s_{x,u}$ berechnet werden kann. Mit Hilfe von Satz 5.20 und

Lemma 5.21 folgt die Lösbarkeit des Syzygienproblems des graduierten Rings G.[8] Folglich ist $\mathfrak{R}$ auch eine effektive graduierte Gröbnerstruktur.

Den Beweisideen von Lemma 5.21 folgend erkennt man, daß jedes homogene Linksideal von G sogar zweiseitig ist. Folglich gilt für jede Menge $F \subseteq R$ die Gleichheit $\mathrm{In}(F) = \mathrm{LIn}(F)$ und damit ist eine Gröbnerbasis des zweiseitigen Ideals $I \subseteq R$ bereits eine Gröbnerbasis von I als Linksideal. □

Sind Idealenthaltenseinsproblem und Syzygienproblem des kommutativen Unterrings $\hat{Q}$ algorithmisch lösbar, so kann man auf die algorithmische Lösbarkeit von Rechtsidealenthaltenseinsproblem und Rechtssyzygienproblem von Q schließen. Insbesondere ist das für treuflache Erweiterungen Q von $\hat{Q}$ stets der Fall. Dem Autor ist jedoch nicht bekannt, ob die gemachten Annahmen über Q und Γ in jedem Fall die Konstruktivität für Rechtsideale von Q und die Berechenbarkeit der Funktion $mgLV$ nach sich ziehen. Falls dies nicht der Fall ist, so folgt die Existenz graduierter Strukturen, welche keine effektive Rechtsgröbner- aber sowohl effektive Linksgröbner- als auch effektive Gröbnerstruktur sind. Eine ähnliche Asymmetrie trat bei den Untersuchungen von Gruppenringen auf (siehe [MR96]).

Ist $\mathfrak{R}$ von der in Satz 5.22 beschriebenen Art und genügt $(\Omega, \prec_\Omega)$ den im gleichen Satz an das Wertemonoid gestellten Voraussetzungen, dann ist auch der Monoidring $\mathfrak{R}\langle\Omega\rangle$ von diesem Typ. Die Klasse der den Bedingungen von Satz 5.22 genügenden graduierten Strukturen $\mathfrak{R}$ besitzt eine zweite Abschlußeigenschaft. Für durch endliche Erzeugendensysteme gegebene zweiseitige Ideale $I \subseteq R$ ist $\mathfrak{R}/I = (R/I, \Gamma, \prec, \varphi_I)$ mit $\varphi_I(a+I) = \min(\varphi(b) \mid b \in a+I)$ eine effektive graduierte Gröbnerstruktur derselben Gestalt. Zwei aus diesen Abschlußeigenschaften resultierende Vorteile sind: anstelle des Umwegs über die Beziehung (3.2) können direkte Algorithmen in den Restklassenringen angewandt werden und die Behandlung endlich erzeugter R-Linksmoduln kann mit Hilfe des Nagataschen Idealisierungsprinzips (siehe [Na62]) auf ein Linksidealproblem des gleichgearteten Rings $R[X]/(X_iX_j \mid X_i, X_j \in X)$ zurückgeführt werden.

Eine abgeschwächte Abschlußeigenschaft gegenüber Restklassenringbildung nach zweiseitigen Idealen gilt für effektive graduierte Linksgröbnerstrukturen der in Satz 5.20 beschriebenen Art. Dabei muß zusätzlich die Entscheidbarkeit des Idealenthaltenseinsproblems des zweiseitigen Ideals I und die Berechenbarkeit endlicher Erzeugendensysteme der annullierenden Linksideale der homogenen Summanden des assoziierten graduierten Rings von $\mathfrak{R}/I$ gefordert werden. Kann I bereits durch ein endliches Linksidealerzeugendensystem vorgegeben werden, so sind diese Zusatzbedingungen auf jeden Fall erfüllt. Ist $\mathfrak{R}$ sogar eine effektive graduierte Gröbnerstruktur, so sind keine Einschränkungen an I erforderlich. Aus einem beliebigen endlichen Erzeugendensystem F von I kann in diesem Fall eine Gröbnerbasis des zweiseitigen Ideals I von R berechnet werden. Mit Hilfe dieser Gröbnerbasis kann man nicht nur effektiv in R/I rechnen, sondern es ist auch möglich, daraus die möglicherweise neu hinzukommenden erzeugenden Elemente der annullierenden Linksideale abzulesen.

[8] Der Bezug auf das homomorphe Bild des Syzygienmoduls $Syz(H)$ in $(G \otimes_A G)^{|H|}$ ersetzt den Ausschluß trivialer Syzygien der Gestalt $ce_u - e_u c$ mit $c \in A$.

Satz 5.22 überdeckt beispielsweise die Untersuchungen zweiseitiger Ideale in Algebren von auflösbarem Typ, auflösbaren Polynomringen sowie G-Algebren. Bisher nicht erfaßt wurden die freien $\mathbb{K}$-Algebren und die Klasse der von Mora in [Mo88b] untersuchten Faktoralgebren freier $\mathbb{K}$-Algebren. Ersteres kann im Rahmen der hier gesteckten Ziele nicht unser Anliegen sein, da in freien $\mathbb{K}$-Algebren nur eine Semientscheidbarkeit des Idealenthaltenseinsproblems vorliegt. Anders verhält es sich bei den Moraschen Faktoralgebren. Diese weisen die Besonderheit auf, daß im allgemeinen nur die aufsteigende Kettenbedingung zweiseitiger Ideale, nicht aber die einseitiger Ideale, erfüllt ist. Der Hauptunterschied zu unseren bisherigen Untersuchungen besteht grob gesprochen darin, daß die Bedingung $R_\gamma R_\omega = R_{\gamma\circ\omega}$ zu $\gamma \mid \omega \Longrightarrow \exists \gamma', \gamma'' \in \Gamma \ : \ R_{\gamma'} R_\gamma R_{\gamma''} = R_\omega$ abgeschwächt wird. Betrachten wir dazu ein Beispiel. $\mathbb{K}$ sei ein beliebiger Körper und $R = G = \mathbb{K}\langle x, y, z\rangle / (yx - xy, zx, zy - yz)$ ein $T(x, y, z)$-graduierter Ring mit $\deg(cx^i y^j z^k) = x^i y^j z^k$. G ist ein $\mathbb{K}$-Vektorraum mit Basis $T(x, y, z)$. Alle annullierenden Linksideale $I_{x^i y^j z^k}$ sind gleich dem Nullideal. Das Produkt uv zweier Potenzprodukte $u, v \in T(x, y, z)$ unterscheidet sich nur dann von dem im Polynomring $\mathbb{K}[x, y, z]$, wenn u die Variable z und v die Variable x enthält. In diesem Fall gilt die Gleichung $uv = 0$. Dennoch ist u in G genau dann durch v teilbar, wenn die Teilbarkeit in $\mathbb{K}[x, y, z]$, oder dazu gleichbedeutend in $T(x, y, z)$, vorliegt, denn man kann es stets so einrichten, daß alle x von links und alle z von rechts multipliziert werden. Andererseits gilt die Beziehung $\{0\} = R_z R_x \subsetneqq R_{z\circ x} = R_{xz} \cong \mathbb{K}$.

Satz 5.23 *Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur mit effektivem Γ-gefiltertem Ring R. Γ sei ein noethersches, kommutatives, effektives Monoid mit lösbarem Faktorisierungsproblem und zu jeder endlichen Teilmenge $\Omega \subseteq \Gamma$ sei die Menge $mgV(\Omega)$ der minimalen gemeinsamen Vielfachen der Elemente von Ω algorithmisch konstruierbar. $Q = F_\epsilon \cong R_\epsilon$ sei ein noetherscher Unterring des Zentrums von R, das Idealenthaltenseinsproblem von Q sei entscheidbar und das Syzygienproblem von Q sei lösbar. Jeder homogene direkte Summand R_γ des assoziierten graduierten Rings G sei ein zyklischer Q-Modul, für welchen ein erzeugendes Element $\mathbb{1}_\gamma$ und ein endliches Erzeugendensystem des annullierenden Ideals $I_\gamma = ann_L(R_\gamma) = ann_R(R_\gamma)$ berechenbar sind. Weiterhin wird zu beliebigen $\gamma, \omega \in \Gamma$ mit $\gamma \mid \omega$ die Existenz zweier Elemente γ' und γ'' mit $\gamma' \circ \gamma \circ \gamma'' = \omega$ vorausgesetzt, so daß für alle Tripel $(\delta', \delta, \delta'')$ von Teilern $\delta' \mid \gamma'$, $\delta \mid \gamma$ und $\delta'' \mid \gamma''$ die Beziehung*

$$R_{\delta'} R_\delta R_{\delta''} = R_{\delta'\circ\delta\circ\delta''} \tag{5.20}$$

erfüllt ist. Schließlich sei die Frage, ob die Menge

$$\Gamma_\gamma = \{\omega \in \Gamma \ \mid \ \gamma \mid \omega \wedge Q/I_\gamma \ncong Q/I_\omega\}$$

leer ist, für jedes $\gamma \in \Gamma$ entscheidbar und im Falle einer nichtleeren Menge sei ein endliches Monoididealerzeugendensystem B_γ von Γ_γ berechenbar[9].

[9] Da Q als Unterring des Zentrums von G vorausgesetzt ist, ist die Bedingung $Q/I_\gamma \ncong Q/I_\omega$ zu $I_\gamma \subsetneqq I_\omega$ äquivalent.

Dann besitzt jedes zweiseitige Ideal I von R eine endliche Gröbnerbasis bezüglich $\mathfrak{R}$ und aus einem beliebigen endlichen Erzeugendensystem von I kann eine solche endliche Gröbnerbasis von I berechnet werden.

Beweis: Zunächst führen wir den Nachweis, daß jede nichtleere Menge Γ_γ ein Monoidideal ist. Zu beliebigen γ und ω mit $\gamma \mid \omega$ existieren $\gamma', \gamma'' \in \Gamma$, für welche $\mathbb{1}_{\gamma'}\mathbb{1}_\gamma\mathbb{1}_{\gamma''}$ und $\mathbb{1}_{\gamma'}\mathbb{1}_\gamma$ erzeugende Elemente der Moduln R_ω beziehungsweise $R_{\gamma'\circ\gamma}$ sind. Daher existiert eine Sequenz

$$Q/I_\gamma \longrightarrow Q/I_{\gamma'\circ\gamma} \longrightarrow Q/I_\omega \tag{5.21}$$

von Epimorphismen und somit ist Q/I_ω für jedes Vielfache ω von γ homomorphes Bild von Q/I_γ. Für beliebige $\omega \in \Gamma_\gamma$ und $\omega', \omega'' \in \Gamma$ ergibt sich die Epimorphismensequenz

$$Q/I_\gamma \xrightarrow{\sigma} Q/I_\omega \xrightarrow{\tau} Q/I_{\omega'\circ\omega\circ\omega''}$$

und da σ nicht injektiv ist, ist auch $\sigma \circ \tau$ kein Isomorphismus. Daraus folgt schließlich, daß jede nichtleere Menge Γ_γ ein Monoidideal von Γ ist.

i) Gemäß Lemma 5.17 ist G ein effektiver Γ-graduierter Ring mit berechenbaren Funktionen in und in*.

ii) Sei $u_1 = c_1\mathbb{1}_{\gamma_1}, u_2 = c_2\mathbb{1}_{\gamma_2}, \ldots$ eine beliebige Folge homogener Elemente von G. Da Γ noethersch ist, existiert eine Teilfolge $u_{i_1}, u_{i_2}, \ldots$ mit der Eigenschaft $\mathbb{1}_{\gamma_{i_j}} \mid \mathbb{1}_{\gamma_{i_k}}$ für alle $j < k$. Da Q noethersch ist, existiert ein k mit $c_{i_k} = \sum_{j=1}^{k-1} d_j c_{i_j}$. Zu jedem $1 \leq j < k$ gibt es γ'_{i_j} und γ''_{i_j}, so daß $\mathbb{1}_{\gamma'_{i_j}}\mathbb{1}_{\gamma_{i_j}}\mathbb{1}_{\gamma''_{i_j}}$ den Q-Modul $R_{\gamma_{i_k}}$ erzeugt, insbesondere existieren Elemente $b_j \in Q$ mit $\mathbb{1}_{\gamma_{i_k}} = \mathbb{1}_{\gamma'_{i_j}}\mathbb{1}_{\gamma_{i_j}}\mathbb{1}_{\gamma''_{i_j}} b_j$. Unter Berücksichtigung der Tatsache, daß die Elemente von Q mit jedem Element von G vertauschen, ergibt sich $u_{i_k} = \sum_{j=1}^{k-1} d_j c_{i_j} \mathbb{1}_{\gamma'_{i_j}}\mathbb{1}_{\gamma_{i_j}}\mathbb{1}_{\gamma''_{i_j}} b_j = \sum_{j=1}^{k-1} d_j \mathbb{1}_{\gamma'_{i_j}} u_{i_j} b_j \mathbb{1}_{\gamma''_{i_j}}$. Demzufolge erfüllt G die aufsteigende Kettenbedingung für zweiseitige Ideale.

iii) Nach Lemma 5.18 hat G ein entscheidbares Enthaltenseinsproblem für endlich erzeugte homogene Ideale beliebiger Seitigkeit.

iv) Es verbleibt die Untersuchung der algorithmischen Lösbarkeit des Syzygienproblems endlich erzeugter homogener zweiseitiger Ideale von G. X bezeichne das minimale Erzeugendensystem von Γ.

Sei $H = \{u_1, \ldots, u_m\}$ eine Menge homogener Elemente von G. Wir verfolgen eine ähnliche Strategie wie im Beweis von Lemma 5.19. Wir suchen nach einer endlichen Menge homogener Syzygien, welche gemeinsam mit den Syzygien aller echten Teilmengen von H den Syzygienmodul $Syz(H)$ erzeugt. Rekursive Anwendung dieses Verfahrens auf alle Teilmengen von H führt dann auf ein endliches Erzeugendensystem von $Syz(H)$. Für festes ω kann das Problem der Berechnung eines endlichen Erzeugendensystems M_ω des Q-Moduls aller homogenen Syzygien von H vom Γ-Grad ω auf ein Syzygienproblem eines Restklassenrings von Q reduziert werden. Unsere Aufgabe besteht also in der Konstruktion einer endlichen Menge Ω von gemeinsamen Vielfachen der

Γ-Grade der Elemente von H, so daß $\bigcup_{\omega\in\Omega} M_\omega \cup \bigcup_{H'\subsetneq H} Syz(H')$ ein Erzeugendensystem des Syzygienmoduls $Syz(H) \subseteq (G\otimes_Q G)^{|H|}$ ist.

Der Hauptunterschied zum Linkssyzygienfall besteht darin, daß aus $\tau = \gamma\circ\deg_\Gamma(u_i)\circ\gamma' = \omega\circ\deg_\Gamma(u_j)\circ\omega'$ und $\deg_\Gamma(u_i),\deg_\Gamma(u_j) \mid \tau' \mid \tau$ nicht notwendigerweise die Existenz von Präfixen $\delta\lfloor\gamma$ und $\sigma\lfloor\omega$ sowie Postfixen $\delta'\rfloor\gamma'$ und $\sigma'\rfloor\omega'$ mit der Eigenschaft $\delta\circ\tau'\circ\delta' = \sigma\circ\tau'\circ\sigma' = \tau$ folgt. Im in Lemma 5.21 behandelten zweiseitigen Fall wurde dieses Problem dadurch behoben, daß man sich modulo einer endlichen Syzygienmenge $B_X\cup B_Z$ auf den Fall $\gamma' = \omega' = \epsilon$, in welchem die Existenz der Prä- und Postfixe gesichert ist, zurückziehen kann. In der gegenwärtigen Situation gelingt die Rückführung auf den Fall $\gamma' = \omega' = \epsilon$ im allgemeinen nicht, dennoch werden wir auf ähnlichem Wege zum Ziel gelangen.

Zu beliebigen $x\in X$ und $u_j\in H$ existiert eine Syzygie der Gestalt $s_{x,u_j} = a_{x,u_j}e_{u_j}\mathbb{1}_x - b_{x,u_j}\mathbb{1}_x e_{u_j}$. Man kann eine endliche Menge $B_X\subset Syz(H)$ konstruieren, welche zu jedem Paar $(x,u_j)\in X\times H$ eine derartige Syzygie enthält. Zusätzlich können wir es so einrichten, daß im Fall $R_xR_{\deg_\Gamma(u)} = R_{\deg_\Gamma(u)\circ x}$ die Gleichheit $a_{x,u_j} = 1$ gilt und b_{x,u_j} im Falle $R_{\deg_\Gamma(u)}R_x = R_{\deg_\Gamma(u)\circ x}$ eine Einheit ist.

Da a_{x,u_j} nicht invertierbar modulo $I_{\deg_\Gamma(u)\circ x}$ zu sein braucht, gibt es zu vorgegebenem $\gamma\in\Gamma$ und $u_j\in H$ nicht mehr notwendigerweise ein $c_{\gamma,u_j}\in Q$ mit $e_{u_j}\mathbb{1}_\gamma - c_{\gamma,u_j}\mathbb{1}_\gamma e_{u_j}\in GB_XG$. Anstelle dessen zeigen wir die schwächere Aussage, daß es Elemente $\omega,\omega'\in\Gamma$ sowie $c\in Q$ mit

$$e_{u_j}\mathbb{1}_\gamma - c\mathbb{1}_\omega e_{u_j}\mathbb{1}_{\omega'}\in GB_XG \tag{5.22}$$

gibt, wobei für alle Teiler $x\in X$ von ω' eine echte Inklusion $R_xR_{\deg_\Gamma(u_j)}\subsetneq R_{\deg_\Gamma(u_j)\circ x}$ vorliegt. Dazu bedienen wir uns der vollständigen Induktion über die Anzahl der irreduziblen Faktoren $x\in X$ mit der Eigenschaft

$$R_{\deg_\Gamma(u_j)\circ x} = R_xR_{\deg_\Gamma(u_j)}\quad , \tag{5.23}$$

die maximal in einer Faktorzerlegung von γ auftreten können. Ist die Anzahl 0, so sind wir fertig. Andernfalls halten wir einen (5.23) genügenden Teiler $x\in X$ von γ fest. Es existieren δ und δ' mit $R_\delta R_x R_{\delta'} = R_\gamma$. Falls es ein $X\ni y\mid\delta$ mit der Eigenschaft $R_{\deg_\Gamma(u_j)\circ y} = R_yR_{\deg_\Gamma(u_j)}$ gibt, so liefert zweimalige Anwendung der Induktionsvoraussetzung die Existenz der gesuchten Syzygie der Gestalt (5.22).

Kommen wir zum Fall, daß für alle Teiler $X\ni y\mid\delta$ die echte Inklusion $R_yR_{\deg_\Gamma(u_j)}\subsetneq R_{\deg_\Gamma(u_j)\circ y}$ vorliegt. Wir betrachten die Teilerbeziehung $\deg_\Gamma(u_j)\circ x \mid \deg_\Gamma(u_j)\circ\delta\circ x$ und gemäß Voraussetzung (5.20) existieren Elemente $\delta_1,\delta_2\in\Gamma$ mit $\delta_1\circ\delta_2 = \delta$, so daß für beliebige Teiler $\alpha_1\mid\delta_1$, $\alpha_2\mid\delta_2$ sowie $\beta\mid\deg_\Gamma(u_j)\circ x$ die Gleichung $R_{\alpha_1}R_\beta R_{\alpha_2} = R_{\alpha_1\circ\beta\circ\alpha_2}$ erfüllt wird. Hätte δ_1 einen Teiler $y\in X$, so würde der Spezialfall $\alpha_1 = y$, $\beta = \deg_\Gamma(u_j)$ und $\alpha_2 = \epsilon$ auf einen Widerspruch führen. Also gilt $\delta_1 = \epsilon$ und damit $\delta_2 = \delta$. Der Fall $\alpha_1 = \epsilon$, $\beta = x$ und $\alpha_2 = \delta$ liefert $R_xR_\delta = R_{\delta\circ x}$. Folglich besitzt $\mathbb{1}_\gamma$ eine Darstellung $\mathbb{1}_\gamma = d\mathbb{1}_x\mathbb{1}_\delta\mathbb{1}_{\delta'}$. Gleichung (5.23) und die Konstruktion von B_X sichern die Existenz einer homogenen Syzygie $s_{x,u_j} = e_{u_j}\mathbb{1}_x - b_{x,u_j}\mathbb{1}_x e_{u_j}\in B_X$. Damit ergibt sich $e_u\mathbb{1}_\gamma - db_{x,u_j}\mathbb{1}_x e_{u_j}\mathbb{1}_\delta\mathbb{1}_{\delta'} = ds_{x,u_j}\mathbb{1}_\delta\mathbb{1}_{\delta'}\in GB_XG$. Anwendung

der Induktionsvoraussetzung auf $\delta \circ \delta'$ und Ersetzen des zweiten Summanden der linken Seite führt schließlich auf die gesuchte Syzygie vom Typ (5.22).

Auf ähnliche Weise zeigt man für beliebige $u_j \in H$ und $\gamma, \gamma' \in \Gamma$ die Existenz homogener Syzygien

$$\mathbb{1}_\gamma e_{u_j} \mathbb{1}_{\gamma'} - c\mathbb{1}_\omega e_{u_j} \mathbb{1}_{\omega'} \in GB_X G \tag{5.24}$$

$$\mathbb{1}_\gamma e_{u_j} \mathbb{1}_{\gamma'} - d\mathbb{1}_\delta e_{u_j} \mathbb{1}_{\delta'} \in GB_X G \tag{5.25}$$

mit folgenden Eigenschaften:

i) $X \ni x \mid \omega' \Longrightarrow R_x R_{\deg_\Gamma(u_j)} \subsetneqq R_{\deg_\Gamma(u_j)\circ x}$,

ii) $X \ni y \mid \omega \Longrightarrow R_y R_{\deg_\Gamma(u_j)} = R_{\deg_\Gamma(u_j)\circ y}$,

iii) $X \ni x \mid \delta \Longrightarrow R_{\deg_\Gamma(u_j)} R_x \subsetneqq R_{\deg_\Gamma(u_j)\circ x}$ und

iv) $X \ni y \mid \delta' \Longrightarrow R_{\deg_\Gamma(u_j)} R_y = R_{\deg_\Gamma(u_j)\circ y}$.

Betrachten wir nun eine beliebige Syzygie $s = \sum_{j=1}^k v_j e_{u_{i_j}} w_j \in Syz(H)$ vom Grad $\deg_\Gamma(s) = \tau$. Falls s nicht bereits Syzygie einer echten Teilmenge von H ist, so muß τ ein gemeinsames Vielfaches der Γ-Grade $\deg_\Gamma(u_i)$ aller Elemente von H sein. Entsprechend der eingangs gemachten Bemerkungen reicht die Behandlung dieses Falls aus. Sei $\tau' \in mgV(\deg_\Gamma(H))$ ein minimales gemeinsames Vielfaches der Grade von H mit $\tau' \mid \tau$. Dann gibt es $\sigma, \sigma' \in \Gamma$ mit $\sigma \circ \tau' \circ \sigma' = \tau$, so daß für alle Teiler $\delta' \mid \sigma$, $\delta \mid \tau'$ und $\delta'' \mid \sigma'$ die Gleichung (5.20) erfüllt ist.

Durch Addition geeigneter Syzygien der Bauart (5.24) erhält man eine homogene Syzygie $s' = \sum_{j=1}^k v'_j e_{u_{i_j}} w'_j \in Syz(H)$ mit $s - s' \in GB_X G$ und den Eigenschaften $X \ni x \mid \deg_\Gamma(w'_j) \Longrightarrow R_x R_{\deg_\Gamma(u_{i_j})} \subsetneqq R_{\deg_\Gamma(u_{i_j})\circ x}$ sowie $X \ni y \mid \deg_\Gamma(v'_j) \Longrightarrow R_y R_{\deg_\Gamma(u_{i_j})} = R_{\deg_\Gamma(u_{i_j})\circ y}$. Für alle $1 \leq j \leq k$ gilt $\sigma \mid \deg_\Gamma(v'_j)$, denn besäße σ einen Teiler $X \ni x \mid \sigma$, der für wenigstens ein j die Teilerbeziehung $x \mid \deg_\Gamma(w'_j)$ erfüllt, so ergäbe der Spezialfall $\delta' = x \mid \sigma$, $\delta = \deg_\Gamma(u_{i_j}) \mid \tau'$ und $\delta'' = \epsilon \mid \sigma'$ einen Widerspruch zu Gleichung (5.20). Bei beliebig festgehaltenem j existieren jeweils Teiler $\delta \mid \tau'$ und $\delta'' \mid \sigma'$ mit $\sigma \circ \delta \circ \delta'' = \deg_\Gamma(v'_j)$ und nach Konstruktion von σ und σ' haben wir $R_\sigma R_\delta R_{\delta''} = R_{\deg_\Gamma(v'_j)} \ni v'_j$. Somit gibt es für jedes $1 \leq j \leq k$ ein homogenes Element $v''_j \in G$ mit $v'_j = \mathbb{1}_\sigma v''_j$. Wir erhalten $s' = \mathbb{1}_\sigma \sum_{j=1}^k v''_j e_{u_{i_j}} w'_j$. Durch Addition geeigneter Vielfacher der zu $u_{i_j}, \deg_\Gamma(v''_j)$ und $\deg_\Gamma(w'_j)$ gehörigen Syzygien vom Typ (5.25) erhält man schließlich eine Syzygie $\hat{s} = \mathbb{1}_\sigma \sum_{j=1}^k \widehat{v_j} e_{u_{i_j}} \widehat{w_j}$ mit $s' - \hat{s} \in GB_X G$, also auch $s - \hat{s} \in GB_X G$, und den Eigenschaften $X \ni x \mid \deg_\Gamma(\widehat{v_j}) \Longrightarrow R_{\deg_\Gamma(u_{i_j})} R_x \subsetneqq R_{\deg_\Gamma(u_{i_j})\circ x}$ sowie $X \ni y \mid \deg_\Gamma(\widehat{w_j}) \Longrightarrow R_{\deg_\Gamma(u_{i_j})\circ y} = R_{\deg_\Gamma(u_{i_j})} R_y$. Analoge Argumentationen zu oben gestatten es nunmehr, aus allen Termen $\widehat{w_{i_j}}$ den rechten Faktor $\mathbb{1}_{\sigma'}$ herauszuziehen. Man beachte, daß wir diesen nochmaligen Reorganisationsschritt von s' zu $\hat{s}$ benötigen, da die Syzygien der Gestalten (5.24) beziehungsweise (5.25) alle Monoiderzeuger $x \in X$ mit $R_{\deg_\Gamma(u_{i_j})} R_x = R_x R_{\deg_\Gamma(u_{i_j})} = R_{\deg_\Gamma(u_{i_j})\circ x}$ entweder alle nach links oder alle nach rechts schieben. Für zwei Erzeuger $x, y \in X$ mit dieser

Eigenschaft braucht aber keineswegs $R_x R_y = R_y R_x = R_{x \circ y}$ zu gelten. Derartige Faktoren von $\deg_\Gamma(v_j)$ und $\deg_\Gamma(w_j)$ lassen sich also nicht beliebig auf den linken und den rechten Kofaktor von $e_{u_{i_j}}$ verteilen. Das gewählte Vorgehen sichert ab, daß eine geeignete und gleichzeitig zulässige Aufteilung entsteht. Letztendlich erhalten wir eine Darstellung $\hat{s} = \mathbb{1}_\sigma \left(\sum_{j=1}^k \widehat{v_j} e_{u_{i_j}} \widehat{w_j}' \right) \mathbb{1}_{\sigma'}$.

An dieser Stelle können wir wieder der Argumentation von Lemma 5.19 folgen. Es gibt ein $d \in Q$ mit $\sum_{j=1}^k \widehat{v_j} u_{i_j} \widehat{w_j}' = d\mathbb{1}_{\tau'}$. Gehört d dem annullierenden Ideal $I_{\tau'}$ an, so folgt $\sum_{j=1}^k \widehat{v_j} u_{i_j} \widehat{w_j}' \in Syz(H)$ und s liegt in dem von B_X und den Syzygien vom Grad τ' erzeugten Untermodul von $Syz(H)$. Andernfalls impliziert $d \notin I_{\tau'}$ wegen $d \in I_\tau$ die Enthaltenseinsbeziehung $\tau \in \Gamma_{\tau'}$. Zur Erinnerung, für $\Gamma_\gamma \neq \emptyset$ ist B_γ ein endliches Monoididealerzeugendensystem von Γ_γ. Im Fall $\Gamma_\gamma = \emptyset$ vereinbaren wir formal $B_\gamma = \emptyset$. Da Q und Γ noethersch sind, wird die rekursiv durch $\Omega_0(H) = mgV(\deg_\Gamma(H))$ und $\Omega_{i+1}(H) = \bigcup_{\gamma \in \Omega_i(H)} B_\gamma$ definierte Folge von Teilmengen von Γ nach endlich vielen Schritten bei der leeren Menge stationär und die Vereinigungsmenge $\Omega(H) = \bigcup_{i=1}^\infty \Omega_i(H)$ ist endlich und algorithmisch konstruierbar. Für jedes $\omega \in \Omega(H)$ kann ein endliches Erzeugendensystem $M_\omega(H)$ des Q-Moduls aller homogenen Syzygien $s \in Syz(H)$ vom Γ-Grad ω berechnet werden und die Menge $B_X \cup \bigcup_{H' \subset H} \bigcup_{\omega \in \Omega(H')} M_\omega(H')$ ist ein endliches homogenes Erzeugendensystem von $Syz(H)$.

Aus den gezeigten Eigenschaften *i)-iv)* folgt, daß jeder Schritt des in Abschnitt 5.2 entwickelten Algorithmus GROEBNER berechenbar ist und daß er bei Eingabe einer beliebigen endlichen Teilmenge $F \subset R$ nach endlicher Zeit anhält. Damit sind die Behauptungen des Satzes bewiesen. □

Für Polynomringe sind neben den Buchbergerschen Filtrierungen auch grobere, d.h. solche die durch eine Buchbergersche verfeinert werden können, betrachtet wurden (siehe z.B. [MöMo86],[Stu96]). In diesem Fall sind die direkten Summanden R_γ des assoziierten graduierten Ringes G nicht mehr notwendigerweise zyklische, sondern nur noch endlich erzeugte Q-Moduln. Falls Q Hauptidealring ist, so läßt sich jedes R_γ nach dem Hauptsatz für abelsche Gruppen (vgl. z.B. [vW67], [Ku70]) in eine direkte Summe zyklischer Moduln zerlegen. Auf dieser Grundlage sind unmittelbare Untersuchungen "grober" Filtrierungen möglich.

Im allgemeinen ist es leider unmöglich, eine vorgegebene graduierte Struktur so zu verfeinern, daß ein assoziierter graduierter Ring mit ausschließlich zyklischen homogenen Summanden entsteht. Selbst wenn sich die homogenen Summanden der Ausgangsgraduierung in direkte Summen zyklischer Moduln zerlegen lassen, braucht es keine Verfeinerung mit diesen als homogene Summanden zu geben. Ein klassisches Gegenbeispiel stellen die Arbeiten zu Gröbnerbasen in Gruppenalgebren dar (siehe [MR93],[Ros93],[Rei95],[MR96]).

5.5 Gröbnerbasen von R-Moduln

Die Theorie der Gröbnerbasen endlichdimensionaler Moduln über Polynomringen wurde erstmals von Möller und Mora in [MöMo86] aufgegriffen. Einerseits lassen sich die in Abschnitt 5.2 dargestellten Ideen unmittelbar von Idealen

$I \subseteq R$ auf Untermoduln $N \subseteq R^m$ verallgemeinern. Andererseits führt gerade diese geradlinige Verallgemeinerung nicht auf die von Möller und Mora entwickelte Theorie. Die Hauptschwierigkeit der Gröbnerbasistheorie besteht in homogenen Berechnungen im assoziierten graduierten Ring beziehungsweise Modul. Dem wird durch die Suche nach möglichst feinen Filtrierungen Rechnung getragen. Bei fast allen Untersuchungen zur Gröbnertheorie werden assoziierte graduierte Ringe verwendet, deren homogene Bestandteile zyklische Q-Moduln über dem Ring $Q = R_\epsilon$ sind. Auf diese Weise erzielt man eine monomiale Gestalt der homogenen Ideale und die in Frage stehenden Enthaltenseins- und Syzygienprobleme stellen sich besonders einfach dar. Das folgende Beispiel zeigt, daß im Modulfall einige zusätzliche Überlegungen erforderlich sind, um ähnlich günstige Voraussetzungen zu schaffen.

Sei R eine Algebra von auflösbarem Typ und $\mathfrak{R} = (R, T, \prec, \mathrm{lpp})$ eine zugehörige graduierte Ringstruktur. $T = T(X)$ ist Vektorraumbasis von R und lpp weist jedem von Null verschiedenen Polynom f den bezüglich der Monoidwohlordnung $\prec$ größten in f vorkommenden Term zu. Damit gilt $\mathrm{lpp}(R\backslash\{0\}) = T(X)$. Sei $M = R^m$ der von $E = \{e_1, \ldots, e_m\}$ frei erzeugte R-Linksmodul. Weiterhin gelte $m > 1$ und jedem Erzeuger $e_i \in E$, $1 \leq i \leq m$, werde ein Potenzprodukt $t_i \in T(X)$ zugeordnet. Zu beliebigen $e_i, e_j \in E$, $i \neq j$, existieren Elemente $f, g \in R\backslash\{0\}$ mit $\mathrm{lpp}(f) \circ t_i = \mathrm{lpp}(g) \circ t_j$. Damit spannen die Initialterme von fe_i und ge_j einen zweidimensionalen Unterraum des $\mathbb{K}$-Vektorraums aller homogenen Elemente vom Grad $\mathrm{lpp}(f) \circ t_i$ des durch die graduierte Ringstruktur $\mathfrak{R}$ und die Erzeugergrade t_i bestimmten assoziierten graduierten Moduls von M auf.

Wir werden sehen, daß sich alle für Linksideale des Rings R erzielten Ergebnisse unmittelbar auf Linksuntermoduln freier Moduln R^m übertragen lassen. Insbesondere ist bei geeigneter Wahl der graduierten Struktur von R keine separate Untersuchung der Entscheidbarkeit des Enthaltenseinsproblems und der Lösbarkeit des Syzygienproblems des assoziierten graduierten Moduls erforderlich. Die Untersuchungen Möllers und Moras passen sich harmonisch in das hier dargestellte Konzept ein. Im Anschluß an die Linksmoduluntersuchungen werden wir uns dem Bimodulfall zuwenden, in diesem ist leider keine ähnlich einfache Übertragung der Ergebnisse aus dem Ringfall mehr möglich.

5.5.1 Einseitige Moduln

Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit wohlgeordnetem Wertemonoid $(\Gamma, \prec)$. $M = R^m$ sei der freie R-Linksmodul mit freiem Erzeugendensystem $E = \{e_1, \ldots, e_m\}$. Weist man jedem Erzeuger $e_i \in E$ ein beliebiges $\varphi_M(e_i) = \delta_i \in \Gamma$ zu, dann läßt sich φ_M vermöge

$$\varphi_M\left(\sum_{i=1}^{m} f_i e_i\right) = \max_{i=1,\ldots,m} (\varphi(f_i) \circ \delta_i) \tag{5.26}$$

zu einer Funktion $\varphi_M : M \to \hat{\Gamma}$ fortsetzen. Diese definiert durch

$$\mathcal{F}_\gamma^M = \{h \mid \varphi_M(h) \preceq \gamma\} \tag{5.27}$$

eine Linksmodulfiltrierung $\mathfrak{F}^M = \left(\mathcal{F}_\gamma^M\right)_{\gamma\in\Gamma}$ und einen dazu assoziierten graduierten Linksmodul von M. Überträgt man die Ideen aus Abschnitt 5.2 sinngemäß von Linksidealen $I \subseteq R$ auf Linksuntermoduln $N \subseteq M$, so erhält man eine Gröbnertheorie für Linksmoduln und die für Linksideale nachgewiesenen Resultate und Algorithmen sind ohne große Mühe auf den Modulfall übertragbar.

Definition 5.24 *Seien $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur, $M = R^m$ der freie von $E = \{e_1, \ldots, e_m\}$ erzeugte R-Linksmodul und $\mathfrak{M} = (M, \Gamma, \mathfrak{F}^M)$ eine gefilterte $\mathfrak{R}$-Linksmodulstruktur. G bezeichne den assoziierten graduierten Ring von $\mathfrak{R}$ und G_M den assoziierten graduierten G-Linksmodul von $\mathfrak{M}$. Dann wird $F \subseteq M$ eine* Gröbnerbasis *des von F erzeugten R-Linksuntermoduls $N \subseteq M$ bezüglich $\mathfrak{M}$ genannt, wenn die von* $\mathrm{in}(F)$ *und* $\mathrm{in}(N)$ *erzeugten G-Linksuntermoduln von G_M gleich sind.*

Im einleitenden Beispiel wurde deutlich, daß es ratsam ist, zunächst nach einer zur Behandlung von Linksuntermoduln $N \subseteq M$ geeigneten graduierten Ringstruktur $(R, \Omega, \prec_\Omega, \varphi_\Omega)$ für R zu suchen. Dazu bilden wir das Kreuzprodukt $\Omega = \Gamma \times T(E)$ von Γ und dem freien von E erzeugten kommutativen Monoid $T(E)$ und legen eine beliebige der Bedingung

$$\forall s, t \in \Gamma\ \forall u \in T(E)\ :\ (t, u) \prec_\Omega (s, u) \Longleftrightarrow t \prec s \tag{5.28}$$

genügende Monoidwohlordnung $\prec_\Omega$ auf Ω fest. Die durch $\varphi_\Omega(f) = (\varphi(f), 1)$ für alle $f \in R\backslash\{0\}$ und $\varphi_\Omega(0) = -\infty$ definierte Funktion $\varphi_\Omega : R \to \hat{\Omega}$ ist eine Pseudobewertung und somit ist $\mathfrak{R}_\Omega = (R, \Omega, \varphi_\Omega, \prec_\Omega)$ eine graduierte Ringstruktur von R. Die Γ-graduierte und die Ω-graduierte Struktur von R erfüllen die Voraussetzungen von Bemerkung (5.9). Dementsprechend ist die Beantwortung einander entsprechender Entscheidbarkeits- und Berechenbarkeitsfragen für beide graduierte Strukturen äquivalent.

Im Vergleich zur Γ-graduierten Struktur bietet die Ω-graduierte Struktur den breiteren Spielraum bei der Definition der Linksmodulfiltrierung. Im weiteren betrachten wir die durch $\varphi_{\Omega,M}(e_i) = (\epsilon, e_i)$ und Gleichung (5.27) definierte gefilterte $\mathfrak{R}_\Omega$-Linksmodulstruktur. Ihr assoziierter graduierter Linksmodul G_M ist direkte Summe

$$G_M = \bigoplus_{i=1}^{m} G \cdot e_i \tag{5.29}$$

von m Exemplaren des assoziierten graduierten Ringes G von $\mathfrak{R}_\Omega$ aufgefaßt als G-Linksmodul. In der Zerlegung eines beliebigen homogenen Elements von G_M bezüglich der direkten Summe (5.29) tritt höchstens ein von Null verschiedener Summand auf. Daher induziert (5.29) für jeden homogenen G-Linksuntermodul $N \subseteq G_M$ eine Zerlegung in eine direkte Summe $N = \bigoplus_{i=1}^m (N \cap G \cdot e_i)$ und jeder der direkten Summanden $N \cap G \cdot e_i$ kann in natürlicher Weise sowohl als Ω-homogenes als auch als Γ-homogenes Linksideal von G aufgefaßt werden.

Satz 5.25 *Mit den Bezeichnungen von oben ist das Enthaltenseinsproblem endlich erzeugter homogener G-Linksuntermoduln des Ω-graduierten Linksmoduls*

G_M relativ zur Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter homogener Linksideale des Γ-graduierten Rings G entscheidbar. Weiterhin ist das Linkssyzygienproblem endlich erzeugter homogener G-Linksuntermoduln von G_M relativ zur Lösbarkeit des Linkssyzygienproblems endlich erzeugter homogener Linksideale von G lösbar.

Beweis: Sei B ein homogenes Erzeugendensystem des homogenen Linksuntermoduls $N \subseteq G_M$ und sei $a \in G_M \backslash \{0\}$ ein homogenes Element. Für jedes $i \in \{1, \ldots, m\}$ führen wir die Bezeichnungen N_i für den direkten Summanden $N \cap G \cdot e_i$ von N und B_i für sein homogenes Erzeugendensystem $B \cap G \cdot e_i$ ein. Es gilt genau dann $a \in N$, wenn für das eindeutig bestimmte $i \in \{1, \ldots, m\}$ mit $a \in G \cdot e_i$ die Enthaltenseinsrelation $a \in N_i = G \cdot B_i$ erfüllt ist. Da N_i als Γ-homogenes Linksideal von G aufgefaßt werden kann, folgt die Behauptung.

Der einfach zu führende Nachweis, daß die Vereinigung $\bigcup_{i=1}^{m} S_i$ homogener Erzeugendensysteme S_i der Linkssyzygienmoduln von B_i ein homogenes Erzeugendensystem des Linkssyzygienmoduls von B liefert, zeigt die zweite Behauptung. □

Analog zum Ringfall zeigt man mit Hilfe dieses Satzes die folgende Verallgemeinerung von Satz 5.6.

Folgerung 5.26 *Für eine effektive graduierte Linksgröbnerstruktur $(R, \Gamma, \prec, \varphi)$ ist das Enthaltenseinsproblem endlich erzeugter R-Linksmoduln entscheidbar. Darüberhinaus kann zu jeder endlichen Teilmenge $F \subset R^m$ ein endliches Erzeugendensystem des Linkssyzygienmoduls $LSyz(F)$ berechnet werden.*

Man beachte insbesondere, daß die Berechenbarkeitsvoraussetzungen an eine für den Idealfall besonders geeignete Γ-graduierte Struktur gestellt werden konnten. Die Algorithmen zur Division und zur Konstruktion von Gröbnerbasen können ohne wesentliche Änderungen aus dem Ringfall übernommen werden. Nur die Teilschritte der Division und der Syzygienberechnung der Initialterme bedürfen einer Anpassung an den Modulfall, wobei jedoch sogar ein Zurückdrücken der Rechnungen bis in den assoziierten graduierten Ring möglich ist.

Bei der Konstruktion der Ω-graduierten Ringstruktur von R verblieb eine Freiheit bei der Festsetzung der Monoidwohlordnung $\prec_\Omega$ auf dem Kreuzprodukt $\Gamma \times T(E)$. Im Falle der Kommutativität des Monoids Γ kann diese Freiheit dazu ausgenutzt werden, daß die Ω-Filtrierung von M eine Verfeinerung der durch (5.26) definierten Γ-Filtrierung von M wird. Wir wählen eine beliebige Monoidwohlordnung $\prec_E$ von $T(E)$ und definieren durch $\delta(e_1^{i_1} \cdots e_m^{i_m}) = \delta_1^{i_1} \circ \cdots \circ \delta_m^{i_m}$ einen Homomorphismus $\delta : T(E) \to \Gamma$. Man überzeugt sich leicht davon, daß die durch

$$(t,u) \prec_\Omega (s,v) \iff t \circ \delta(u) \prec s \circ \delta(v) \vee (t \circ \delta(u) = s \circ \delta(v) \wedge u \prec_E v), \quad (t, s \in \Gamma,\ u, v \in T(E))$$

definierte binäre Relation $\prec_\Omega$ eine unseren Anforderungen genügende Monoidwohlordnung von Ω ist. Im eingangs betrachteten Beispiel der Algebren von

auflösbarem Typ erhält man auf die beschriebene Art und Weise eine Filtrierung von M, bei welcher alle von Null verschiedenen direkten Summanden des assoziierten graduierten Linksmoduls eindimensional sind und welche von der in [MöMo86] betrachteten Art ist.

5.5.2 Bimoduln

Dieser Abschnitt beschäftigt sich mit der Untersuchung von R-Bimoduln

$$M = (R \otimes_S R)^m = \bigoplus_{i=1}^{m} (R \otimes_S R)_{e_i} \quad ,$$

wobei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit wohlgeordnetem Wertemonoid $(\Gamma, \prec)$ und S ein das Einselement enthaltender Unterring von R sind. Da bereits die Elemente von $R \otimes_S R$ im allgemeinen mehrere Darstellungen als Summe von Elementartensoren $a \otimes b$ aufweisen, ist die Darstellung der Elemente von M im Modulerzeugendensystem $E = \{e_1, \ldots, e_m\}$ natürlich erst recht nicht eindeutig bestimmt.

$$Rep(h) = \left\{ ((f_1, i_1, g_1), \ldots, (f_k, i_k, g_k)) \;\mid\; h = \sum_{j=1}^{k} f_j e_{i_j} g_j \right\} \tag{5.30}$$

bezeichne die Menge aller formalen Darstellungen des Elementes $h \in M$ im freien Modulerzeugendensystem E. Durch die Festlegung $\varphi_M(e_i) = \delta_i \in \Gamma$, $i = 1, \ldots, m$, wird eine Funktion

$$\varphi_M(h) = \min_{Rep(h)} \left(\max_{1 \le j \le k} \left(\varphi(f_j) \circ \delta_{i_j} \circ \varphi(g_j) \right) \right) \tag{5.31}$$

erklärt, welche vermöge

$$\mathcal{F}_\gamma^M = \{ h \;\mid\; \varphi_M(h) \preceq \gamma \} \tag{5.32}$$

eine gefilterte $\mathfrak{R}$-Bimodulstruktur $\mathfrak{M} = (M, \Gamma, \mathfrak{F}^M)$ auf M induziert. In der anschließenden Definition der Gröbnerbasis eines R-Biuntermoduls von M wird die Modulstruktur von M in eine Links- und eine Rechtsmodulstruktur aufgespalten. Ginge man ähnlich der oben definierten Γ-Filtrierung $\mathfrak{F}^M$ den naheliegenden Weg, für beide Seiten die gleiche graduierte Struktur von R zugrunde zu legen, dann wäre es im allgemeinen bereits unmöglich, die Untersuchungen auf den Fall $m = 1$ zu reduzieren. Noch weniger wäre an eine Übertragung der im Ringfall erzielten Resultate zu denken.

Definition 5.27 *Seien $\mathfrak{R}_l = (R, \Gamma, \prec, \varphi_l)$ und $\mathfrak{R}_r = (R, \Gamma, \prec, \varphi_r)$ zwei graduierte Strukturen des Ringes R mit den davon induzierten Filtrierungen $\mathfrak{F}_l$ und $\mathfrak{F}_r$. Weiterhin sei $S \subseteq R$ ein das Einselement enthaltender Unterring von R und $M = (R \otimes_S R)^m$. Schließlich sei $\mathfrak{M} = (M, \Gamma, \mathfrak{F}^M)$ eine gefilterte $(R, \Gamma, \mathfrak{F}_l, \mathfrak{F}_r)$-Bimodulstruktur von M. Die assoziierten graduierten Ringe von $\mathfrak{R}_l$ und $\mathfrak{R}_r$ werden mit G_l beziehungsweise G_r und der assoziierte graduierte Modul von $\mathfrak{M}$ wird mit G_M bezeichnet. Dann wird $F \subseteq M$ eine* Gröbnerbasis *des von F erzeugten R-Biuntermoduls $N \subseteq M$ bezüglich $\mathfrak{M}$ genannt, wenn die Gleichheit $G_l \cdot \mathrm{in}(F) \cdot G_r = G_l \cdot \mathrm{in}(N) \cdot G_r$ erfüllt ist.*

Analog zum linksseitigen Fall bilden wir das Monoid $\Omega = \Gamma \times T(E) \times \Gamma$ und fixieren auf ihm eine Monoidwohlordnung $\prec_\Omega$ mit der Eigenschaft

$$\forall s, s', t, t' \in \Gamma \; \forall u \in T(E) \; : \; (s, u, s') \prec_\Omega (t, u, t') \Longleftrightarrow s \circ s' \prec t \circ t' \quad .$$

Durch $\varphi_{l,\Omega}(f) = (\varphi(f), 1, \epsilon)$ beziehungsweise $\varphi_{r,\Omega}(f) = (\epsilon, 1, \varphi(f))$ für alle $f \in R \backslash \{0\}$ definieren wir zwei graduierte Ringstrukturen $(R, \Omega, \prec_\Omega, \varphi_{l,\Omega})$ und $(R, \Omega, \prec_\Omega, \varphi_{r,\Omega})$ für R. Die zugehörigen Filtrierungen bezeichnen wir mit $\mathfrak{F}_{l,\Omega}$ beziehungsweise $\mathfrak{F}_{r,\Omega}$. Gemäß Bemerkung 5.9 sind die beiden Ω-graduierten Strukturen in Bezug auf die Gröbnertheorie zur ursprünglichen Γ-graduierten Struktur von R gleichwertig. Die zu den drei graduierten Strukturen gehörigen graduierten Ringe G,G_l und G_r sind als Ringe zueinander isomorph und es existieren jeweils Isomorphismen, die homogene Elemente in homogene Elemente überführen. Obwohl die Ringe nicht als graduierte Ringe zueinander isomorph sind, da zum einen nicht alle Wertemonoide übereinstimmen und zum anderen auch für G_l und G_r keine Gradgleichheit zwischen Bild und Urbild vorliegt, werden wir die Ringe G_l,G_r und G identifizieren und gleichermaßen mit G bezeichnen. Aus dieser Identifizierung werden keine Mißverständnisse erwachsen, da eine Unterscheidung nur in Bezug auf den genauen Grad homogener Elemente bedeutsam ist und in einem solchen Falle stets aus dem Kontext heraus klar werden wird, um welchen der drei Ringe G_l,G_r oder G es sich handelt.

Jede Zuordnung $\varphi_{\Omega,M}(e_i) = \delta_i \in \Omega$, $i = 1, \ldots, m$, definiert durch

$$\varphi_M(h) = \min_{Rep(h)} \left(\max_{1 \leq j \leq k} \left(\varphi_{l,\Omega}(f_j) \circ \delta_{i_j} \circ \varphi_{r,\Omega}(g_j) \right) \right) \tag{5.33}$$

und Gleichung (5.32) eine gefilterte $(R, \Omega, \mathfrak{F}_{l,\Omega}, \mathfrak{F}_{r,\Omega})$-Bimodulstruktur $\mathfrak{M} = (M, \Omega, \mathfrak{F}^M)$. Ist das Monoid Γ kommutativ, so kann man die Monoidwohlordnung $\prec_\Omega$ in Analogie zum einseitigen Fall geeignet wählen, so daß die auf die obige Weise von der Zuordnung $\varphi_{\Omega,M}(e_i) = (\epsilon, e_i, \epsilon)$, $i = 1, \ldots, m$, induzierte $(R, \Omega, \mathfrak{F}_{l,\Omega}, \mathfrak{F}_{r,\Omega})$-Filtrierung eine Verfeinerung der bei entsprechender Zuordnung durch (5.31) und (5.32) erklärten $(R, \Gamma, \mathfrak{F}_\Gamma, \mathfrak{F}_\Gamma)$-Filtrierung von M ist. Für die Gültigkeit der im folgenden abgeleiteten Aussagen ist diese Verfeinerungseigenschaft jedoch ohne Bedeutung. Insbesondere darf das Wertemonoide durchaus auch nichtkommutativ sein.

$\mathfrak{M} = (M, \Omega, \mathfrak{F}^M)$ sei die durch $\varphi_{\Omega,M}(e_i) = (\epsilon, e_i, \epsilon)$, $i = 1, \ldots, m$, induzierte gefilterte $(R, \Omega, \mathfrak{F}_{l,\Omega}, \mathfrak{F}_{r,\Omega})$-Bimodulstruktur. Dann zerfällt der assoziierte graduierte G-Bimodul G_M von $\mathfrak{M}$ analog zu Gleichung (5.29) in eine direkte Summe

$$G_M = \bigoplus_{i=1}^{m} (G \otimes_{\hat{S}} G)_{e_i} \tag{5.34}$$

und dabei gehört jedes von Null verschiedene homogene Element von G_M (genau) einem der direkten Summanden $(G \otimes_{\hat{S}} G)_{e_i}$ an. $\hat{S}$ ist hier der von allen Initialtermen von Elementen von S erzeugte Unterring des assoziierten graduierten Rings G von R. Für jeden homogenen G-Biuntermodul $N \subseteq G_M$ beschreibt $N = \bigoplus_{i=1}^{m} \left(N \cap (G \otimes_{\hat{S}} G)_{e_i} \right)$ eine Zerlegung in eine direkte Summe von Biuntermoduln von $G \otimes_{\hat{S}} G$. Damit läßt sich Satz 5.25 in dem Sinne auf

den Bimodulfall übertragen, daß die Lösungen des Enthaltenseinsproblems und des Syzygienproblems homogener G-Biuntermoduln von G_M auf den Spezialfall $m = 1$, das heißt auf homogene G-Biuntermoduln von $G \otimes_{\hat{S}} G$, reduziert werden können. Wenden wir uns nun der genaueren Untersuchung des Falls $m = 1$ zu und bezeichnen den erzeugenden Tensor $1 \otimes 1$ von $G_M = G \otimes_{\hat{S}} G$ mit dem Symbol e. Damit erhält Ω die Gestalt $\Gamma \times T(\{e\}) \times \Gamma$.

Sei $\tau : G \otimes_{\hat{S}} G \to G$ der durch $a \otimes b \mapsto ab$ erklärte natürliche Homomorphismus. Homogene Elemente werden durch τ in homogene Elemente überführt. Sind das Enthaltenseinsproblem und ein T-Syzygienproblem endlich erzeugter homogener zweiseitiger Ideale von G lösbar, so lassen sich mit Hilfe von τ notwendige Bedingungen für die Lösung entsprechender Probleme von $G \otimes_{\hat{S}} G$ ableiten. So erfordert die Enthaltenseinsrelation $a \in N \subseteq G \otimes_{\hat{S}} G$ selbstverständlich die Gültigkeit von $\tau(a) \in \tau(N)$. Sei H eine endliche Menge homogener Elemente von $G \otimes_{\hat{S}} G$ und betrachten wir die Sequenz

$$(G \otimes_U G)^{|H|} \xrightarrow{\varphi} G \otimes_{\hat{S}} G \xrightarrow{\tau} G$$

von Homomorphismen, wobei U den vom Einselement erzeugten Unterring von $\hat{S}$ bezeichnet und φ durch $e_h \mapsto h$ definiert ist. Dann ergibt sich folgende Inklusion der Syzygienmoduln:

$$Syz(H) = ker(\varphi) \subseteq Syz(\tau(H)) = ker(\varphi \circ \tau)$$

und $B \cup T(\tau(H))$ ist Erzeugendensystem eines Biobermoduls von $Syz(H)$ für jedes T-Erzeugendensystem B von $Syz(\tau(H))$.

Das folgende Beispiel demonstriert, daß das Auffinden eines T'-Erzeugendensystems, wobei $T'(H) = T(\tau(H)) \cap Syz(H)$, vorerst ein offenes Problem bleibt. So reicht es keineswegs aus, einfach die Menge $B \cap Syz(H)$ zu bilden oder nur unter den $\hat{S}$-Kombinationen von B nach einem Erzeugendensystem für $Syz(H)$ zu suchen. Seien $G = \mathbb{Z}\langle X, Y\rangle$, $G_M = G \otimes_{\mathbb{Z}} G$ und $H = \{X \otimes Y^3, X \otimes XY^2, X^3 \otimes Y\}$. Wertemonoid sei die freie Worthalbgruppe $S(X, Y)$ mit einer beliebigen zulässigen Wohlordnung $\prec$. Während $B = \{Xe_1 - e_2Y, Xe_2 - e_3Y\}$ ein $Triv$-Erzeugendensystem des Syzygienmoduls von $\tau(H) = \{XY^3, X^2Y^2, X^3Y\}$ in Bezug auf die in Gleichung (3.3) beschriebenen Moraschen trivialen Syzygien ist, wird der Syzygienmodul $Syz(H)$ von $\{X^2e_1 - e_3Y^2\}$ erzeugt, ohne daß die Hinzunahme trivialer Syzygien erforderlich ist. Keines der Elemente von B und keine $\mathbb{Z}$-Kombination davon gehört $Syz(H)$ an, aber es gilt $X(Xe_1 - e_2Y) - (Xe_2 - e_3Y)Y = X^2e_1 - e_3Y^2$.

Alles in allem stellen wir fest, daß uns die Homomorphiebetrachtungen bei der Suche nach geeigneten Algorithmen im allgemeinen nicht voranbringen.

Wir führen die Bezeichungen $R_{G,\gamma}$ für die Menge aller homogenen Elemente von G vom Γ-Grad $\gamma \in \Gamma$ und $R_{G_M,\omega}$ für die Menge aller homogenen Elemente von G_M vom Ω-Grad $\omega \in \Omega$ ein. Von jetzt an beschränken wir uns auf die Untersuchung des Falls, daß $\hat{S} = Q = R_{G,\epsilon}$ gilt, Q Unterring des Zentrums von G ist und jeder homogene direkte Summand $R_{G,\gamma}$ von G ein zyklischer Q-Modul ist. Wir bezeichnen das annullierende Ideal des Q-Moduls $R_{G,\gamma}$ mit $I_\gamma = ann_L(R_\gamma)$ und weisen nochmals auf die Q-Modulisomorphie $Q/I_\gamma \cong R_{G,\gamma}$ hin.

Lemma 5.28 *Der assoziierte Γ-graduierte Ring G sei effektiv und $Q = R_{G,\epsilon} \subseteq Z(G)$ sei ein effektiver noetherscher Ring mit entscheidbarem Idealenthaltenseinsproblem. Zu jedem $\gamma \in \Gamma$ existiere eine berechenbare Funktion $\iota_\gamma : R_{G,\gamma} \to Q$, so daß die Abbildungsvorschrift $a \mapsto \iota_\gamma(a) + I_\gamma$ einen Isomorphismus $\hat{\iota}_\gamma : R_{G,\gamma} \to Q/I_\gamma$ beschreibt. Schließlich existiere eine berechenbare Funktion $B : \Gamma \to Fin(Q)$, die jedem $\gamma \in \Gamma$ ein endliches Erzeugendensystem $B(\gamma)$ des Ideals I_γ zuordnet.*

Dann ist G_M ein effektiver Ω-graduierter G-Bimodul und für beliebige $\gamma, \gamma' \in \Gamma$ gilt die Isomorphie

$$R_{G_M,(\gamma,e,\gamma')} \cong Q/(I_\gamma + I_{\gamma'}) \quad . \tag{5.35}$$

Beweis: Die Isomorphie 5.35 folgt sofort aus der Gültigkeit von

$$R_{G_M,(\gamma,e,\gamma')} \cong Q/I_\gamma \otimes_Q Q/I_{\gamma'} \cong Q/(I_\gamma + I_{\gamma'}) \quad .$$

Nach Satz 2.9 sichert die vorausgesetzte Entscheidbarkeit des Idealenthaltenseinsproblems des noetherschen Rings Q für jedes durch ein beliebiges endliches Erzeugendensystem gegebenes Ideal $I \subseteq Q$ die Existenz eines kanonischen Simplifikators $S_I : Q \to Q$ für den Restklassenring Q/I. Wir setzen[10]

$$\mathbb{1}_\gamma := \hat{\iota}_\gamma^{-1}(1 + I_\gamma) \quad , \gamma \in \Gamma \quad . \tag{5.36}$$

Für jeden homogenen Elementartensor $a \otimes b \in G_M$ vom Ω-Grad (γ, e, γ') gilt die Gleichheit

$$\begin{aligned} a \otimes b &= \iota_\gamma(a)\mathbb{1}_\gamma \otimes \iota_{\gamma'}(b)\mathbb{1}_{\gamma'} \\ &= \iota_\gamma(a) * \iota_{\gamma'}(b)(\mathbb{1}_\gamma \otimes \mathbb{1}_{\gamma'}) \\ &= S_{(B(\gamma)\cup B(\gamma'))}\left(\iota_\gamma(a) * \iota_{\gamma'}(b)\right)(\mathbb{1}_\gamma \otimes \mathbb{1}_{\gamma'}) \quad . \end{aligned} \tag{5.37}$$

Jede der Umformungen ist berechenbar und lineares Fortsetzen auf beliebige Elemente von G_M liefert einen kanonischen Simplifikator von G_M. Der Nachweis der restlichen Eigenschaften eines effektiven Ω-graduierten G-Moduls für G_M ist trivial. □

Lemma 5.29 *$\mathfrak{R}$ sei sowohl effektive Links- als auch effektive Rechtsgröbnerstruktur. Der assoziierte graduierte Ring G von $\mathfrak{R}$ erfülle die Voraussetzung von Lemma 5.28. Dann ist das Enthaltenseinsproblem endlich erzeugter homogener G-Biuntermoduln von $G \otimes_Q G$ entscheidbar.*

Beweis: Seien $a = c\mathbb{1}_\gamma \otimes \mathbb{1}_{\gamma'}$ ein homogenes Element von $G \otimes_Q G$ und $H = \{h_1 = c_1\mathbb{1}_{\gamma_1} \otimes \mathbb{1}_{\gamma'_1}, \ldots, h_k = c_k\mathbb{1}_{\gamma_k} \otimes \mathbb{1}_{\gamma'_k}\}$ eine endliche Menge homogener Elemente von $G \otimes_Q G$. Alle Elemente seien in der kanonisch simplifizierten Gestalt

[10] Am Rande weisen wir darauf hin, daß das so definierte $\mathbb{1}_\gamma$ auch Null sein kann. Allerdings nur im Falle $R_{G,\gamma} = \{0\}$. Alle im weiteren Verlauf getroffenen Aussagen über $\mathbb{1}_\gamma$ gelten, sofern nicht explizit auf das Gegenteil hingewiesen wird, selbstverständlich auch in diesem Spezialfall.

(5.37) gegeben. $a \in GHG$ ist äquivalent zur Existenz von $\alpha_1, \ldots, \alpha_k \in Q$ und $\tau_1, \ldots, \tau_k, \tau'_1, \ldots, \tau'_k \in \Gamma$ mit der Eigenschaft

$$a = \sum_{i=1}^{k} \alpha_i \mathbb{1}_{\tau_i} h_i \mathbb{1}_{\tau'_i} , \tag{5.38}$$

wobei $\gamma = \tau_i \circ \gamma_i$ und $\gamma' = \gamma'_i \circ \tau'_i$ für alle $i = 1, \ldots, k$ mit $\alpha_i \neq 0$. Da $\mathfrak{R}$ eine effektive Linksgröbnerstruktur ist, kann ein endliches homogenes Erzeugendensystem des Linkssyzygienmoduls von $\{\mathbb{1}_\gamma, \mathbb{1}_{\gamma_1}, \ldots, \mathbb{1}_{\gamma_k}\}$ berechnet werden. Da G ein effektiver Γ-graduierter Ring ist, können insbesondere die Grade der Linkssyzygien und auch die Grade ihrer von Null verschiedenen Komponenten berechnet werden. Für alle $1 \leq i \leq k$ mit $\gamma_i \rfloor \gamma$ und $\mathbb{1}_{\tau_i} \mathbb{1}_{\gamma_i} \neq 0$, wobei $\tau_i \circ \gamma_i = \gamma$, kann daher τ_i auf algorithmischem Wege aus dem Erzeugendensystem dieses Linkssyzygienmoduls bestimmt werden. Die h_i, für die diese Eigenschaft nicht zutrifft, werden in (5.38) nicht benötigt, da für sie o.B.d.A. $\alpha_i = 0$ angenommen werden kann. Auf analoge Weise bestimmt man alle Elemente τ'_i, für die in (5.38) möglicherweise $\alpha_i \neq 0$ notwendig ist. Nach Einsetzen der Grade in Gleichung (5.38) führt kanonische Simplifikation gemäß (5.37) auf eine inhomogene, lineare Gleichung in den Variablen α_i mit Koeffizienten aus $Q/(I_\gamma + I_{\gamma'})$. Genau wenn diese Gleichung eine Lösung in $Q/(I_\gamma + I_{\gamma'})$ besitzt, dann gehört a dem von H erzeugten G-Biuntermodul von $G \otimes_Q G$ an. Die Frage nach der Lösung der Gleichung kann auf ein Idealenthaltenseinsproblem von Q reduziert werden und ist daher entscheidbar. □

Die Übertragung der Gröbnertheorie auf den Modul $R \otimes_Q R$ bedarf noch der Lösung des Syzygienproblems für endliche Mengen H homogener Elemente des assoziierten graduierten Moduls $G \otimes_Q G$. Anstelle des Syzygienmoduls $Syz(H) \subseteq G \otimes_U G$, wobei U den vom Einselement erzeugten Unterring von Q bezeichnet, betrachten wir sein homomorphes Bild unter dem natürlichen Homomorphismus $\iota_Q : (G \otimes_U G)^{|H'|} \to (G \otimes_Q G)^{|H'|}$. Die Funktion T weise jeder Teilmenge $H \subseteq G \otimes_Q G$ homogener Elemente die Menge aller Syzygien der Gestalt $ae_h - e_h a$, wobei $h \in H$ und $a \in Q$, zu. Dann entspricht die Lösung des T-Syzygienproblems von H gerade der Berechnung eines endlichen Erzeugendensystems von $\iota_Q(Syz(H))$.

Lemma 5.30 *$\mathfrak{R}$ sei sowohl effektive Links- als auch effektive Rechtsgröbnerstruktur. Der assoziierte graduierte Ring G von $\mathfrak{R}$ erfülle die Voraussetzung von Lemma 5.28 und Q sei ein Körper. Dann ist das T-Syzygienproblem endlich erzeugter homogener Biuntermoduln von $G \otimes_Q G$ lösbar.*

Beweis: Sei $H = \{h_1 = c_1 \mathbb{1}_{\gamma_1} \otimes \mathbb{1}_{\gamma'_1}, \ldots, h_k = c_k \mathbb{1}_{\gamma_k} \otimes \mathbb{1}_{\gamma'_k}\}$ eine endliche Menge homogener Elemente von $G \otimes_Q G$. Wir weisen die Existenz und algorithmische Konstruierbarkeit einer endlichen Menge $B(H)$ zweiseitiger Syzygien von H nach, so daß

$$\iota_Q(Syz(H)) \subseteq G\, \iota_Q(B(H))\, G + \sum_{H' \subsetneq H} \iota_Q(Syz(H')) . \tag{5.39}$$

Die Behauptung folgt dann mittels vollständiger Induktion über die Mächtigkeit $|H| = k$.

Seien $p \in \bigcap_{i=1}^{k} G\mathbb{1}_{\gamma_i}$ und $q_1, \ldots, q_k$ homogene Elemente von G, so daß $q_i\mathbb{1}_{\gamma_i} = p$ für alle $1 \leq i \leq k$. Dann kann zu jedem $1 \leq i \leq k$ das Element $h_i' \in Q$ mit $q_i h_i = \mathbb{1}_{\deg_\Gamma(p)} \otimes h_i'$ berechnet werden. Nach Voraussetzung ist das Rechtssyzygienproblem der Menge $H_{l,p} = \{h_1', \ldots, h_k'\} \subseteq G$ lösbar und daher kann ein endliches homogenes Erzeugendensystem $\hat{B}_{l,p}$ von $RSyz(H_{l,p})$ berechnet werden. Jede Rechtssyzygie aus $\hat{B}_{l,p}$ läßt sich auf offensichtliche Weise als zweiseitige Syzygie von H auffassen, die Menge dieser zweiseitigen Syzygien bezeichnen wir mit $B_{l,p}$. Auf analoge Weise kann zu $q \in \bigcap_{i=1}^{k} \mathbb{1}_{\gamma_i'} G$ eine Menge zweiseitiger Syzygien $B_{r,q}$ von H berechnet werden. Unter Berücksichtigung der Darlegungen aus Abschnitt 3.3.3 lassen sich relativ zur Lösbarkeit des Links- und des Rechtssyzygienproblems von G endliche homogene Erzeugendensysteme D_l und D_r der Durchschnitte $\bigcap_{i=1}^{k} G\mathbb{1}_{\gamma_i}$ beziehungsweise $\bigcap_{i=1}^{k} \mathbb{1}_{\gamma_i'} G$ berechnen. Im weiteren zeigen wir, daß die Menge

$$B(H) = \bigcup_{p \in D_l} B_{l,p} \cup \bigcup_{q \in D_r} B_{r,q}$$

der Anforderung (5.39) genügt.

Sei $k = 1$ und $s \in Syz(H) = Syz(\{h_1\})$ eine Syzygie vom Grad $\deg_\Omega(s) = (\tau, e, \tau')$. $\iota_Q(s)$ läßt sich in der Form $d\mathbb{1}_\delta e_{h_1} \mathbb{1}_{\delta'}$ darstellen. Für $d = 0$ sind wir fertig. Andernfalls muß die Beziehung $I_\tau + I_{\tau'} = Q$ gelten und da Q ein Körper ist, muß wenigstens eines der beiden Ideale gleich Q sein. Demnach ist s Vielfaches einer Syzygie der Gestalt $e_{h_1}\mathbb{1}_{\tau_1'}$ oder $\mathbb{1}_{\tau_1} e_{h_1}$, wobei $\mathbb{1}_{\gamma_1'}\mathbb{1}_{\tau_1'} = 0$ beziehungsweise $\mathbb{1}_{\tau_1}\mathbb{1}_{\gamma_1} = 0$ gelten. Diese Syzygien gehören dem von $\iota_Q(B(\{h_1\}))$ erzeugten G-Bimodul an.

Sei nun $k > 1$ und $s \in Syz(H)$ eine homogene Syzygie vom Grad $\deg_\Omega(s) = (\tau, e, \tau')$. Das Bild $\iota_Q(s)$ läßt sich in der Gestalt $\iota_Q(s) = \sum_{j=1}^{l} d_j \mathbb{1}_{\delta_j} e_{h_{i_j}} \mathbb{1}_{\delta_j'}$ mit $d_j \neq 0$ $(1 \leq j \leq l)$ und $i_j < i_{j+1}$ $(1 \leq j < l)$ darstellen. Falls $l < k$, so ist s bereits Syzygie einer echten Teilmenge $H \setminus \{h_i\} \subset H$. Sei also $l = k$ und damit $\iota_Q(s) = \sum_{j=1}^{k} d_j \mathbb{1}_{\delta_j} e_{h_j} \mathbb{1}_{\delta_j'}$. Gibt es ein $1 \leq j \leq k$ mit $\mathbb{1}_{\delta_j}\mathbb{1}_{\gamma_j} = 0$, so zerfällt $\iota_Q(s)$ in eine Summe aus einer Syzygie von $\{h_j\}$ und einer Syzygie von $H \setminus \{h_j\}$. Andernfalls gilt $\mathbb{1}_\tau \in \bigcap_{i=1}^{k} G\mathbb{1}_{\gamma_i}$. Da Q Körper ist, gibt es ein $p \in D_l$ und ein homogenes $u \in G$ mit $\mathbb{1}_\tau = up$. Aus $\iota_Q(s)$ läßt sich u als linker Faktor ausklammern und wir erhalten $\iota_Q(s) = us'$. Dabei ist s' Bild einer homogenen Syzygie von H vom Grad $\deg_\Omega(s') = (\deg_\Gamma(p), e, \tau')$ unter ι_Q. s' und somit auch $\iota_Q(s)$ gehören dem von $\iota_Q(B_{l,p})$ erzeugten Untermodul von $Syz(H)$ an. □

Zusammenfassend stellen wir fest:

Satz 5.31 *$(R, \Gamma, \prec, \varphi)$ sei eine effektive Links- und eine effektive Rechtsgröbnerstruktur. $R_{G,\epsilon} = Q$ sei ein effektiver Körper und Unterring des Zentrums von R. Jeder Q-Vektorraum $R_{G,\gamma}$, $\gamma \in \Gamma$, habe höchstens die Dimension 1.*

Dann ist das Enthaltenseinsproblem endlich erzeugter R-Biuntermoduln des Moduls $M = (R \otimes_Q R)^m$ semientscheidbar.

Falls R ein Σ-graduierter Ring ist, wobei seine Γ-Filtrierung die Σ-Filtrierung verfeinert, dann ist das Enthaltenseinsproblem endlich erzeugter Σ-homoge-

ner R-Biuntermoduln von M für jede durch eine Funktion $\deg_\Sigma : \{e_1, \ldots, e_m\} \to \Sigma$ *induzierte* Σ*-Modulgraduierung von* M *entscheidbar.*

Beweis: Sei $\mathfrak{M}$ eine in diesem Abschnitt untersuchte gefilterte $(R, \Omega, \mathfrak{F}_{l,\Omega}, \mathfrak{F}_{r,\Omega})$-Bimodulstruktur von M. Da Q Unterring des Zentrums von R ist, sind alle zu $ker(\iota_Q)$ gehörigen homogenen Syzygien trivial.

Die Lemmata 5.28 und 5.29 sichern für ein beliebiges Modulelement $f \in M$ und eine beliebige Teilmenge $F = \{f_1, \ldots, f_n\} \subset M$ die Berechenbarkeit der Bestandteile $g_1, \ldots, g_l, g'_1, \ldots, g'_l \in R$, $f_{i_1}, \ldots, f_{i_l} \in F$ und $\hat{f} \in M$ einer Divisionsformel $f = \sum_{j=1}^{l} g_j f_{i_j} g'_j + \hat{f}$, wobei $\varphi_{l,\Omega}(g_j) \circ \deg_\Omega(\mathrm{in}(f_{i_j})) \circ \varphi_{r,\Omega}(g'_j) \preceq \deg_\Omega(\mathrm{in}(f))$ sowie $\hat{f} = 0$ oder $\hat{f} \notin G \cdot \mathrm{in}(F) \cdot G$. Der Rest $\hat{f}$, den f bei Division modulo F läßt, bezeichnen wir mit $\hat{f} = \mathrm{REM}(f, F)$. Ziel ist es, zu zeigen, daß für beliebige $f \in M$ und $F = \{f_1, \ldots, f_n\} \subset M$ genau dann die Beziehung $f \in_R (F)_R = N$ gilt, wenn die Abarbeitung der folgenden Anweisungsfolge bei Eingabe von f und F anhält und eine Null ausgegeben wird.

$F' := F$, $f := \mathrm{REM}(f, F)$
while $f \neq 0$ and $F' \neq \emptyset$ **do**
$B :=$ endliches homogenes T-Erzeugendensystem von $Syz(\mathrm{in}(F))$
$F' := \{\mathrm{REM}(\mathrm{LIFT}(s), F) \mid s \in B\} \backslash \{0\}$
$F := F \cup F'$
$f := \mathrm{REM}(f, F)$
return(f)

Wird $f = 0$ ausgegeben, so ist die Korrektheit der Antwort offensichtlich. Bei Ausgabe von $f \neq 0$ ist F zum Terminationszeitpunkt eine Gröbnerbasis von N, da jede (nichttriviale) Syzygie der Initialterme zu einer Syzygie der Elemente von F geliftet werden konnte. Also ist die Antwort auch in diesem Falle korrekt.

Diskutieren wir nun das Terminationsverhalten. Die Berechenbarkeit aller Anweisungen folgt aus den vorausgesetzten Effektivitätsbedingungen und den Lemmata 5.28, 5.29 und 5.30. Insbesondere folgt die Berechenbarkeit eines T-Erzeugendensystems B aus Lemma 5.30. Auch für noethersche Ringe G ist der G-Bimodul $(G \otimes_Q G)^m$ im allgemeinen nicht noethersch und somit steht das im Ringfall angewandte Hauptargument für die Termination der **while**-Schleife nicht zur Verfügung.

Seien $f \in N$ und $\omega \in \Omega$ minimal mit der Eigenschaft $\mathrm{REM}(f, F) \in \mathcal{F}_\omega^{(F)}$, wobei $\mathfrak{F}^{(F)}$ die durch F bestimmte Gröbnerfiltrierung des R-Bimoduls N ist. Falls $\mathrm{REM}(f, F) \neq 0$, so gilt $\deg_\Omega(\mathrm{in}(\mathrm{REM}(f, F))) \prec \omega$ und es existiert eine Syzygie $s \in Syz(\mathrm{in}(F))$ vom Grad $\deg_\Omega(s) = \omega$ mit $\mathrm{REM}(f, F) - \mathrm{LIFT}(s) \in \hat{\mathcal{F}}_\omega^{(F)}$. Diese Syzygie s besitzt eine homogene Darstellung $s = \sum_{i=1}^{r} p_i s_i q_i$ mit $s_1, \ldots, s_r \in B \cup T(\mathrm{in}(F))$ und es gilt $\mathrm{LIFT}(s) - \sum_{i=1}^{r} \mathrm{in}^*(p_i)\mathrm{LIFT}(s_i)\,\mathrm{in}^*(q_i) \in \hat{\mathcal{F}}_\omega^{(F)}$. Sei $F \cup F'$ das im nächsten Schleifendurchlauf gültige Erzeugendensystem von N. Gemäß der Abarbeitungsvorschrift gilt $\mathrm{LIFT}(s_i) \in \hat{\mathcal{F}}_{\deg_\Omega(s_i)}^{(F \cup F')}$ für alle $1 \leq i \leq r$ und damit $\mathrm{LIFT}(s) \in \hat{\mathcal{F}}_\omega^{(F \cup F')}$, was $\mathrm{REM}(f, F \cup F'), \mathrm{REM}(f, F) \in \hat{\mathcal{F}}_\omega^{(F \cup F')}$ nach sich zieht. Also verkleinert sich ω bei jedem Schleifendurchlauf, weshalb nach endlich vielen Durchläufen in Bezug auf das dann aktuelle Erzeugendensystem

F die Gleichheit $\text{REM}(f, F) = 0$ gelten muß. Somit hält das Verfahren im Fall $f \in N$ stets nach endlich vielen Schritten an und die behauptete Semientscheidbarkeit ist gezeigt.

Schließlich steht noch der Beweis der zweiten Behauptung bezüglich des Enthaltenseinsproblems homogener Untermoduln Σ-graduierter Moduln M aus. Sei $\tau : \Gamma \to \Sigma$ ein schwach ordnungsverträglicher Monoidhomomorphismus, vermöge dem die Γ-Filtrierung die Σ-Filtrierung von R verfeinert. Weiter seien $f \in R$ ein Σ-homogenes Element vom Grad $\deg_\Sigma(f) = \sigma$ und $F \subset M$ eine endliche Menge Σ-homogener Modulelemente. Die Abarbeitung der obigen Anweisungsfolge kann abgebrochen werden, sobald für jede Syzygie $s \in B$ mit $\tau(\deg_\Gamma(s)) \preceq_\Sigma \sigma$ die Beziehung $\text{REM}(\text{LIFT}(s), F) = 0$ gilt. Offensichtlich würden bei Fortsetzung der Abarbeitung alle später zu F hinzugefügten Elemente g die Relation $\sigma \prec_\Sigma \deg_\Sigma(g)$ erfüllen. Aus diesem Grund kann aus der Gültigkeit von $\text{REM}(f, F) \neq 0$ zum Abbruchzeitpunkt auf $f \notin N$ geschlossen werden. □

Die Rückführbarkeit auf Probleme einseitiger Ideale und die Möglichkeit, alle trivialen Syzygien a priori auszufaktorisieren, könnten den Anschein erwecken, daß der Modulfall einfacher zu handhaben ist, als der Spezialfall zweiseitiger Ideale. Die Auflösung dieses Paradoxons besteht in der Feststellung, daß die zweiseitigen Ideale von R im Rahmen des konstruktiven Teils der hier beschriebenen Theorie nicht behandelt werden können, da ihr volles Urbild unter einem Epimorphismus $\tau : R \otimes_Q R \to R$ mit Ausnahme einiger uninteressanter Trivialfälle kein endlich erzeugter R-Biuntermodul von $R \otimes_Q R$ ist.

Kapitel 6

Topologische Methoden

In bestimmten Situationen ist es möglich und notwendig, die im vorangegangenen Kapitel beschriebenen konstruktiven Verfahren gefilterter Ringe durch topologische Methoden zu ergänzen. Insbesondere mußten wir bisher voraussetzen, daß uns eine Filtrierung bezüglich eines wohlgeordneten Monoids vorliegt. Ohne diese Voraussetzung würde beispielsweise die Terminationseigenschaft des Algorithmus $\textsc{Divide}_R$ verlorengehen. Betrachten wir einmal die von den Werten von $\hat{a}$ nach jedem Durchlauf der **while**-Schleife gebildete Folge von Idealelementen. Unter gewissen noch näher zu spezifizierenden Bedingungen läßt sich eine Topologie finden, in der diese Folge gegen ein Element des Ideals I konvergiert, welches als Divisionsrest verwendet werden kann.

Wir beginnen zunächst mit Untersuchungen zu solchen topologischen Ringen, deren Topologie durch die Filtrierung induziert wird. Dieser Fall wurde in allgemeiner Form von Robbiano und Mora (siehe [Rob86], [Mo88a]) behandelt. Außerdem gibt es eine Reihe diesbezüglicher Untersuchungen in speziellen Situationen lokaler Potenzreihenringe (siehe z.B. [Hi64],[Mo82],[Bec90], [AMR92],[Gr95]). Das Hauptaugenmerk unserer Ausführungen liegt auf dem Aufbau einer Divisionsformel und der Approximation ihrer Bestandteile zu beliebig vorgegebener Genauigkeit. Dazu bedarf es einerseits einer wesentlichen Einschränkung der Klasse der von Mora in [Mo88a] untersuchten Ringe und der Beschränkung auf einseitige Ideale. Andererseits werden uns diese Einschränkungen erlauben, weitreichendere Resultate für diesen Spezialfall abzuleiten. Insbesondere können wir die Stetigkeit der Divisionsformel in beiden Argumenten nachweisen und auch Näherungslösungen für die Kofaktoren ermitteln. Moras Beweise werden dahingehend präzisiert, daß der Divisionsrest, und nicht nur sein Initialterm, im Falle einer Standardbasis F als zweitem Argument nur von der Restklasse des ersten Arguments modulo des von F erzeugten Linksideals abhängt.

Im Anschluß daran beschäftigen wir uns mit dem Fall, daß sich Ringtopologie und Filtrierung konträr gegenüberstehen. Erste Untersuchungen dieser Art findet man in [ASTW].

6.1 Standardbasen

Wir betrachten graduierte Ringstrukturen $(R, \Gamma, \prec, \varphi)$ mit einer beschränkten Wohlordnung $\prec$. Den bereits in Kapitel 5 behandelten Spezialfall wohlgeordneter Wertemonoide wollen wir hier ausschließen. Darüberhinaus ist der Kalkül aus Kapitel 5 bereits dann anwendbar, wenn nur der Bildbereich $im(\varphi)$ wohlgeordnet ist. In diesem Abschnitt setzen wir voraus, daß Γ beschränkt wohlgeordnetes Monoid ist und daß $im(\varphi)$ kein kleinstes Element besitzt. $\mathfrak{F}$ bezeichne die durch die Pseudobewertung $\varphi : R \to \hat{\Gamma}$ beschriebene Γ-Filtrierung des Ringes R. Indem man die Mengen $\mathcal{F}_\gamma$ als Umgebungen des Nullelementes auffaßt, definiert $\mathfrak{F}$ eine Topologie $\mathfrak{T}_\mathfrak{F}$ auf R. $\mathfrak{T}_\mathfrak{F}$ ist Hausdorff-Topologie, denn gäbe es ein $0 \neq a \in \bigcap_{\gamma\in\Gamma} \mathcal{F}_\gamma$, so wäre $\varphi(a)$ untere Schranke von $im(\varphi)$. Mit Hilfe der beschränkten Wohlordnungseigenschaft von $\prec$ gelingt es, die Stetigkeit der Ringmultiplikation in $\mathfrak{T}_\mathfrak{F}$ nachzuweisen (siehe [Mo88a]). Also bildet R mit $\mathfrak{T}_\mathfrak{F}$ einen *topologischen Ring*. Eine Folge $(r_i)_{i=1,2,\ldots}$ von Elementen aus R heißt *Cauchy-Folge*, falls zu jedem $\gamma \in \Gamma$ eine natürliche Zahl $\nu_0(\gamma)$ exisiert, so daß für alle $\nu, \mu \geq \nu_0(\gamma)$ die Beziehung $r_\nu - r_\mu \in \mathcal{F}_\gamma$ erfüllt ist. Wenn jede Cauchy-Folge von Elementen aus R gegen ein Element von R konvergiert, so bezeichnet man R als *kompletten topologischen Ring*. Falls jede Cauchy-Folge von Elementen des (Links-, Rechts-) Ideals I gegen ein Element von I konvergiert, so wird I ein *abgeschlossenes (Links-, Rechts-) Ideal* genannt.

Zum besseren Verständnis fügen wir an dieser Stelle einige Beispiele für die untersuchten Ringe ein.

Formale Potenzreihenringe Seien $R = \mathbb{K}[[X_1, \ldots, X_n]]$ der Ring der formalen Potenzreihen in den Unbestimmten $X_1, \ldots, X_n$ über dem Körper $\mathbb{K}$ und $\Gamma = T(X)$ das von $X = \{X_1, \ldots, X_n\}$ frei erzeugte kommutative Monoid. Wir ordnen $T(X)$ vermöge einer operationsverträglichen beschränkten Wohlordnung $\prec$ mit maximalem Element. Die Funktion φ wird so definiert, daß sie jeder Potenzreihe $f \in R\backslash\{0\}$ das bezüglich $\prec$ größte Potenzprodukt[1], welches mit von Null verschiedenem Koeffizient in f vorkommt, zuweist. Die Topologie $\mathfrak{T}$, die durch die von φ induzierte Filtrierung von R definiert wird, stimmt mit der *Krullschen Topologie* überein. Die Krullsche Topologie wird auch $\mathfrak{m}$-*adische Topologie* genannt, sie wird durch die von den Potenzen des maximalen Ideals $\mathfrak{m} = (X_1, \ldots, X_n)$ gebildete 0-Umgebungsbasis bestimmt.

Lokale Unterringe formaler Potenzreihenringe Analog zum vorangegangenen Beispiel können auch lokale Unterringe $S \subseteq R = \mathbb{K}[[X_1, \ldots, X_n]]$ betrachtet werden.

Beliebige lokale Ringe Seien S ein lokaler Ring und $\mathfrak{m}$ sein maximales Ideal. Dann ist die durch $\varphi(a) = \max\{k \mid a \in \mathfrak{m}^k\}$ $(a \neq 0)$ induzierte $(\mathbb{N}, >)$-Filtrierung von S ebenfalls vom untersuchten Typ.

[1] Da alle Variablen negatives Gewicht haben müssen, ist dieses Potenzprodukt stets von "kleinem" gewöhnlichen Totalgrad. Sind alle Gewichte -1, so handelt es sich um ein Potenzprodukt von kleinstem Totalgrad.

Wertemonoid ohne maximales Element Schließlich führen wir noch ein Beispiel mit beschränkt wohlgeordnetem Wertemonoid ohne maximales Element an. Sei $R = \mathbb{K}[[X]][Y]$ der Polynomring in Y mit formalen Potenzreihen in X als Koeffizienten. Wir setzen $\Gamma = T(X,Y)$ und vergleichen die Potenzprodukte gemäß der Vorschrift: $X^{n_1}Y^{m_1} \prec X^{n_2}Y^{m_2}$ genau dann, wenn $n_1 > n_2$ oder $n_1 = n_2$ und $m_1 < m_2$. Die Pseudobewertung φ weist jedem $f \neq 0$ das mit von Null verschiedenem Koeffizient in f vorkommende Potenzprodukt zu, dessen Exponent für X minimal ist und unter diesen den maximalen Exponent für Y aufweist.

Stellvertretend für den Fall einseitiger Ideale betrachten wir Linksideale. Die Untersuchung zweiseitiger Ideale ist ungleich schwieriger und kann nicht in ähnlicher Weise durchgeführt werden.

Definition 6.1 *Sei $(R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit beschränkter Wohlordnung $\prec$. Ein Erzeugendensystem F eines Linksideals $I \subseteq R$ wird eine* Standardbasis *von I genannt, falls die Menge $\mathrm{in}(F)$ der Initialterme von Elementen von F das Linksinitialideal von I erzeugt, d.h. $\mathrm{LIn}(F) = \mathrm{LIn}(I)$.*

Die Bezeichnung *Standardbasis* geht auf Hironaka zurück, welcher Basen der obigen Art in formalen Potenzreihenringen einführte (siehe [Hi64]). Unter gewissen Nebenbedingungen sind die beschränkt wohlgeordneten Wertemonoide gerade noch ausreichend, um Satz 5.2 übertragen zu können.

Satz 6.2 *Sei $(R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit einer beschränkten Wohlordnung $\prec$. Ist der Ring R in der durch φ induzierten Topologie komplett und ist der assoziierte graduierte Ring G linksnoethersch, dann ist jede Teilmenge $F \subseteq I$ eines Linksideals $I \subseteq R$, für welche $\mathrm{in}(F)$ das Linksinitialideal $\mathrm{LIn}(I)$ erzeugt, ein Erzeugendensystem von I.*

Beweis: Ohne Beschränkung der Allgemeinheit können wir annehmen, daß F endlich ist. Die Menge F erzeugt ein Unterlinksideal J von I. Angenommen, es existiert ein Element $a_1 \in I \backslash J$. Nach Voraussetzung läßt sich der Initialterm von a_1 als homogene Linkskombination der Initalterme der Elemente von F darstellen, d.h. es existieren homogene Elemente $h_f \in G$ mit $\mathrm{in}(a_1) = \sum_{f \in F} h_f \ \mathrm{in}(f)$ und $\deg_\Gamma(h_f) \circ \varphi(f) = \varphi(a_1)$ für alle $f \in F$ mit $h_f \neq 0$. Wir wählen beliebige Elemente $b_{1,f} \in R$ mit $\mathrm{in}(b_{1,f}) = h_f$. Offensichtlich gilt $a_2 = a_1 - \sum_{f \in F} b_{1,f} f \in I \backslash J$ und $\varphi(a_2) \prec \varphi(a_1)$. Iteration dieses Verfahrens liefert eine unendliche Folge $A = (a_i)_{i=1,2,\ldots}$ von Elementen mit den Eigenschaften:

i) $a_i \in I \backslash J$,

ii) $\exists b_{i,f} \in R \ : \ (b_{i,f} = 0 \vee \varphi(b_{i,f}) \circ \varphi(f) = \varphi(a_i)) \wedge a_{i+1} = a_i - \sum_{f \in F} b_{i,f} f$ und

iii) $\varphi(a_{i+1}) \prec \varphi(a_i)$

für alle $i = 1, 2, \ldots$. Mittels vollständiger Induktion weist man leicht die Gültigkeit von

$$a_{i+1} = a_1 - \sum_{f \in F} (\sum_{j=1}^{i} b_{j,f}) f \tag{6.1}$$

nach. Aus Eigenschaft *iii)* ergibt sich $\lim_{i \to \infty} a_i = 0$. Für beliebige $j, k \in \mathbb{N}$ und $f \in F$ mit $1 \leq j < k$ sowie $b_{j,f}, b_{k,f} \neq 0$ gilt die Beziehung $\varphi(b_{k,f}) \prec \varphi(b_{j,f})$. Folglich bilden die Partialsummen $\sum_{j=1}^{m} b_{j,f}$ für jedes $f \in F$ eine Cauchy-Folge in der durch φ induzierten Topologie und da R in dieser komplett ist, existieren die unendlichen Summen $b_f = \lim_{m \to \infty} \sum_{j=1}^{m} b_{j,f} = \sum_{j=1}^{\infty} b_{j,f}$. Beim Grenzübergang $i \to \infty$ führt Gleichung (6.1) auf

$$a_1 - \sum_{f \in F} b_f f = 0 \quad .$$

Das steht im Widerspruch zu $a_1 \notin J$, also $I = J$. □

Der Satz ist nicht auf die Betrachtung zweiseitiger Ideale, nicht kompletter Ringe R oder graduierter Ringstrukturen, deren assoziierter graduierter Ring G nicht linksnoethersch ist, übertragbar. In diesen Situationen tritt ein Auseinanderfallen der Begriffe Standardbasis[2] und Standardmenge[3] ein (siehe [Rob86] und [Mo88a]).

Folgerung 6.3 *Unter den Voraussetzungen von Satz 6.2 ist R linksnoethersch und jedes Linksideal von R besitzt eine endliche Standardbasis.*

Beweis: Die Behauptung folgt unmittelbar aus Satz 6.2. □

Zunächst geben wir einen Vorschrift an, die relativ zur Berechenbarkeit aller gerufenen Funktionen einen schwachen Divisionsalgorithmus $\textsc{Divide}_{R,\mathfrak{T}}$ für Ringelemente a modulo eines endlichen Erzeugendensystems F eines Linksideals beschreibt. Dabei wird vom Divisionsrest $\hat{a}$, den a bei Division modulo F mittels $\textsc{Divide}_{R,\mathfrak{T}}$ läßt, nur dann die Beziehung $\mathrm{in}(\hat{a}) \notin \mathrm{LIn}(F)$ gefordert, wenn der Initialterm von $\hat{a}$ einen Grad größer als γ aufweist.

Aufruf: $(g_1, \ldots, g_m, \hat{a}) := \textsc{Divide}_{R,\mathfrak{T}}(a, F, \gamma)$
Eingaben: $F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Linksideals I, $a \in R$, $\gamma \in \Gamma$
Ausgaben: $g_1, \ldots, g_m, \hat{a} \in R$ mit $a = \sum_{i=1}^{m} g_i f_i + \hat{a}$, wobei
$\varphi(g_i) \circ \varphi(f_i) \preceq \varphi(a)$ für $i = 1, \ldots, m$ sowie $\varphi(\hat{a}) \preceq \gamma$ oder $\mathrm{in}(\hat{a}) \notin \mathrm{LIn}(F)$.

[2] An dieser Stelle beziehen wir uns auf einen Standardbasisbegriff, welcher für jedes $a \in I$ die Existenz einer Summendarstellung $a = \sum_{i=1}^{k} g_i f_i h_i$ mit $\varphi(g_i) \circ \varphi(f_i) \circ \varphi(h_i) \preceq \varphi(a)$ fordert. Unsere Entscheidung für Definition 6.1 liegt darin begründet, daß wir uns nur mit Situationen beschäftigen, in denen keine begriffliche Unterscheidung zwischen Standardbasen und Standardmengen notwendig ist.

[3] An eine *Standardmenge* F des zweiseitigen Ideals I werden nur die Bedingungen $F \subseteq I$ und $\mathrm{In}(F) = \mathrm{In}(I)$ gestellt. Entsprechende Definitionen gelten für einseitige Ideale.

$\hat{a} := a,\ g_i := 0 \quad (i = 1, \ldots, m)$
$(p_1, \ldots, p_m, A) := \textsc{Divide}_G(\mathrm{in}(\hat{a}),\ \mathrm{in}(F))$
while $A = 0 \quad \wedge \quad \gamma \prec \varphi(\hat{a})$ **do**
$\quad g_i := g_i + \mathrm{in}^*(p_i)$
$\quad \hat{a} := \hat{a} - \sum_{i=1}^{m} \mathrm{in}^*(p_i) f_i$
$\quad (p_1, \ldots, p_m, A) := \textsc{Divide}_G(\mathrm{in}(\hat{a}),\ \mathrm{in}(F))$
return$(g_1, \ldots, g_m, \hat{a})$

Dabei genüge die in $\textsc{Divide}_{R,\mathfrak{T}}$ gerufenen Funktion $\textsc{Divide}_G$ der Spezifikation:

Aufruf: $(p_1, \ldots, p_m, A) := \textsc{Divide}_G(a, H)$
Eingaben: a homogenes Element von G
$H = \{h_1, \ldots, h_m\}$ endliche Menge homogener Elemente von G.
Ausgaben: $p_1, \ldots, p_m, A \in G$ homogene Elemente, so daß $a = \sum_{i=1}^{m} p_i h_i + A$,
wobei $p_i = 0$ oder $\deg_\Gamma(p_i) \circ \deg_\Gamma(h_i) = \deg_\Gamma(a)$ für alle $i = 1, \ldots, m$
und $A = 0 \iff a \in GH$

Beweis der Korrektheit und Termination von $\textsc{Divide}_{R,\mathfrak{T}}$: Relativ zur Berechenbarkeit aller gerufenen Funktionen verläuft der Korrektheitsbeweis völlig analog zum Beweis des auf Seite 62 dargestellten Algorithmus $\textsc{Divide}_R$. Kommen wir zur Frage der Termination. Bei jedem Durchlauf der **while**-Schleife verkleinert sich der Grad von $\mathrm{in}(\hat{a})$. Da die Menge $\{\gamma' \in \Gamma \mid \gamma \prec \gamma'\}$ bezüglich $\prec$ wohlgeordnet ist, wird die Schleife nach endlich vielen Durchläufen verlassen. □

Lemma 6.4 *Sei $(R, \Gamma, \prec, \varphi)$ eine graduierte Struktur mit beschränkter Wohlordnung $\prec$. Dann ist die Menge $\varphi(a + I) = \{\varphi(b) \mid a - b \in I\}$ für jedes abgeschlossene (Links-, Rechts-) Ideal $I \subseteq R$ und jedes Ringelement $a \notin I$ eine nach unten beschränkte Teilmenge von Γ.*

Beweis: $\varphi(a + I) \subseteq \Gamma$ folgt sofort aus $0 \notin a + I$. Angenommen, die Menge $\varphi(a + I)$ wäre nach unten unbeschränkt. Dann gäbe es eine Cauchy-Folge $b_1 = a - h_1, b_2 = a - h_2, \ldots$, wobei $h_n \in I$ für alle $n = 1, 2, \ldots$, mit $\lim_{n\to\infty} b_n = 0$. Folglich: $a = \lim_{n\to\infty} h_n \in I$, im Widerspruch zur Voraussetzung $a \notin I$. □

Lassen wir bei Algorithmus $\textsc{Divide}_{R,\mathfrak{T}}$ formal auch die Eingabe von $\gamma = -\infty$ zu, so wird im Falle der Termination weiterhin die Ausgabespezifikation erfüllt. Weiterhin bricht nach Lemma 6.4 die Abarbeitung für Eingaben $a \notin \bar{I}$, wobei $\bar{I}$ den topologischen Abschluß des Linksideals I bezeichnet, stets mit von Null verschiedenem $\hat{a}$ ab. Ist I ein abgeschlossenes Linksideal und F eine Standardbasis von I, so zieht das die Semientscheidbarkeit der Frage: $a \notin I$ *?* nach sich.

Für beliebige Eingaben ist die Folge $\varphi(\hat{a})$ im Falle der Nichttermination streng monoton fallend und folglich konvergiert die Folge der Zwischenreste $\hat{a}$ gegen 0. Auf ähnliche Weise wie für b_f im Beweis von Satz 6.2 überzeugt man sich davon, daß für jedes $i = 1, \ldots, m$ auch die Folge der Zwischenwerte der Variablen g_i eine Cauchy-Folge bildet. Die in $\textsc{Divide}_{R,\mathfrak{T}}$ gerufenen Funktionen

$\textsc{Divide}_G$ und in^* sind durch ihre Spezifikationen nicht eindeutig bestimmt. Im weiteren setzen wir beide Funktionen als beliebig fest gewählt voraus. Sei $\gamma_1 \succ \gamma_2 \succ \cdots$ eine beliebige, streng monoton fallende Folge von Elementen von Γ. Seien $g_1^{(i)}, \ldots, g_m^{(i)}, \hat{a}^{(i)} \in R$ so, daß $\left(g_1^{(i)}, \ldots, g_m^{(i)}, \hat{a}^{(i)}\right) = \textsc{Divide}_{R,\mathfrak{T}}(a, F, \gamma_i)$ für $i = 1, 2, \ldots$. Falls R ein kompletter topologischer Ring ist, so ist die durch

$$\textsc{Divide}_{R,\lim}(a, F) = \left(\lim_{i\to\infty} g_1^{(i)}, \ldots, \lim_{i\to\infty} g_m^{(i)}, \lim_{i\to\infty} \hat{a}^{(i)}\right)$$

definierte Funktion total und ihre Funktionswerte hängen nicht von der konkreten Wahl der γ_i ab.

Bemerkung 6.5 *Im Falle der Berechenbarkeit der Funktion* $\textsc{Divide}_{R,\lim}$ *ist das Enthaltenseinsproblem durch endliche Standardbasen F gegebener Linksideale I des kompletten Ringes R entscheidbar.*

Der Beweis dieser Aussage besteht in der trivialen Festellung, daß $\textsc{Divide}_{R,\lim}$ einen Algorithmus zur Entscheidung dieses Enthaltenseinsproblems liefert. □

Satz 6.6 *Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit beschränkter Wohlordnung $\prec$. Der Ring R sei in der durch $\mathfrak{R}$ induzierten Topologie $\mathfrak{T}_\mathfrak{F}$ komplett und der assoziierte graduierte Ring G von $\mathfrak{R}$ sei linksnoethersch. Dann ist jedes Linksideal $I \subseteq R$ topologisch abgeschlossen bezüglich $\mathfrak{T}_\mathfrak{F}$.*

Beweis: Zum ersten hatten wir gerade gezeigt, daß die Funktion $\textsc{Divide}_{R,\lim}$ im vorliegenden kompletten Ring total ist, zum zweiten schließen wir aus Folgerung 6.3 auf die Existenz einer endlichen Standardbasis F von I. Betrachten wir den Rest $\hat{a}$ bei Anwendung von $\textsc{Divide}_{R,\lim}$ auf $a \in R$ und F. Falls $\hat{a} = 0$ gilt, so erhalten wir eine Darstellung $a = \sum_{i=1}^m h_i f_i$, also gilt $a \in I$. Im Fall $\hat{a} \neq 0$ muß insbesondere $\varphi(\hat{a}) \notin \mathrm{LIn}(F) = \mathrm{LIn}(I)$ vorliegen, also $\hat{a} \notin I$ und somit $a \notin I$. Es gilt also genau dann $a \in I$, wenn $\hat{a} = 0$ ist.

Sei nun b ein von Null verschiedenes Element des topologischen Abschlusses von I und $a_1, a_2, \ldots$ eine gegen b konvergierende Cauchy-Folge von Elementen aus I. Es existiert eine natürliche Zahl n_0, so daß $\varphi(b - a_n) \prec \varphi(b)$ für alle $n > n_0$ gilt. Daraus ergibt sich $\mathrm{in}(b) = \mathrm{in}(a_n)$ für alle $n > n_0$. Aus diesem Grund ist 0 das einzige Element aus dem topologischen Abschluß von I, welches als Rest bei Division mittels $\textsc{Divide}_{R,\lim}$ modulo der Standardbasis F auftreten kann. Da der Divisionsrest eines Elementes aus dem topologischen Abschluß von I wieder in diesem liegt, ist bewiesen, daß I topologisch abgeschlossen ist. □

Setzen wir nun voraus, daß das Wertemonoid Γ ein maximales Element besitzt. Wie in Abschnitt 4.1 gezeigt wurde, muß dann $\max(\Gamma) = \epsilon$ gelten, was für alle $\gamma, \gamma' \in \Gamma$ die Gültigkeit von $\gamma \circ \gamma' \preceq \gamma$ und $\gamma' \circ \gamma \preceq \gamma$ nach sich zieht. Somit ist jede der Filtrierung $\mathfrak{F}$ angehörige additive Gruppe $\mathcal{F}_\gamma = \{a \in R \mid \varphi(a) \preceq \gamma\}$ ein zweiseitiges Ideal des Rings R. Dem Restklassenring $R/\mathcal{F}_\gamma$ kann die graduierte Struktur $\mathfrak{R}/\mathcal{F}_\gamma = (R/\mathcal{F}_\gamma, \Gamma, \prec, \varphi_\gamma)$ mit

$$\varphi_\gamma(a + \mathcal{F}_\gamma) = \begin{cases} \varphi(a) : & \text{falls } \gamma \prec \varphi(a) \\ \gamma \quad : & \text{sonst} \end{cases}$$

zugeordnet werden. Für alle $\gamma \in \Gamma$ ist die durch $\mathfrak{R}/\mathcal{F}_\gamma$ induzierte Topologie $\mathfrak{T}_\gamma$ des Restklassenringes $R/\mathcal{F}_\gamma$ diskret.

Satz 6.7 *Der assoziierte graduierte Ring G der graduierten Ringstruktur $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ sei linksnoethersch. Das Monoid $(\Gamma, \prec)$ sei beschränkt wohlgeordnet und besitze ein größtes Element. Weiterhin sei G ein effektiver graduierter Ring mit entscheidbarem Enthaltenseins- und lösbarem Syzygienproblem für endlich erzeugte homogene Linksideale. Es existiere ein Unterring R' von R, welcher mit der induzierten Filtrierung effektiv ist. Die Einschränkung* $\mathrm{in}|_{R'}$ *der Initialabbildung auf R' sei berechenbar und es existiere ein berechenbarer Schnitt* in^* *der Initialabbildung, so daß* $im(\mathrm{in}^*) \subseteq R'$.

Dann ist für beliebiges $\gamma \in \Gamma$ das Enthaltenseinsproblem endlich erzeugter Linksideale des Restklassenrings $R/\mathcal{F}_\gamma$ entscheidbar.

Beweis: Der assoziierte graduierte Ring von $\mathfrak{R}/\mathcal{F}_\gamma$ ist isomorph zu $G/\mathrm{In}(\mathcal{F}_\gamma)$. Er ist ein effektiver graduierter Ring, da G diese Eigenschaft hat und der Kern $\mathrm{In}(\mathcal{F}_\gamma)$ aufgrund der Berechenbarkeit der Gradfunktion von G und der Effektivität des geordneten Monoids Γ entscheidbar ist.

Nächstes Ziel ist es, zu zeigen, daß die natürliche Einbettung ι des Unterringes $R'/(\mathcal{F}_\gamma \cap R')$ in $R/\mathcal{F}_\gamma$ ein Isomorphismus ist. Dazu haben wir ihre Surjektivität nachzuweisen. Wir untersuchen die Menge $M = \{a \in R \mid (a + \mathcal{F}_\gamma) \cap R' = \emptyset\}$ aller derjenigen Elemente von R, welche zu keinem Element von R' kongruent modulo des Ideals $\mathcal{F}_\gamma$ sind. Angenommen, $M \neq \emptyset$. Trivialerweise gilt $M \cap \mathcal{F}_\gamma = \emptyset$, weshalb γ untere Schranke der nichtleeren Menge $\varphi(M) \subset \Gamma$ ist. Aus der beschränkten Wohlordnungseigenschaft von $\prec$ folgt die Existenz eines kleinsten Elementes von $\varphi(M)$ bezüglich $\prec$. Sei $a \in M$ so, daß $\varphi(a)$ dieses kleinste Element ist. Wegen $im(\mathrm{in}^*) \subseteq R'$ existiert ein $b \in R'$ mit $\mathrm{in}(a) = \mathrm{in}(b)$, also $\varphi(a - b) \prec \varphi(a)$. Nach Konstruktion von a muß $a - b \notin M$ gelten, was die Existenz eines $b' \in R'$ mit $(a - b) - b' \in \mathcal{F}_\gamma$ nach sich zieht. Somit $a - (b + b') \in \mathcal{F}_\gamma$ und $b + b' \in R'$, im Widerspruch zu $(a + \mathcal{F}_\gamma) \cap R' = \emptyset$. Folglich war die Annahme $M \neq \emptyset$ falsch.

Sei $b : \Omega^* \to R'$ eine Beschreibungsvorschrift, bezüglich welcher der gefilterte Ring R' effektiv ist. $\mathcal{F}_\gamma \cap R'$ ist eine entscheidbare Teilmenge von R', also ist $R'/(\mathcal{F}_\gamma \cap R')$ gemäß Satz 2.8 bezüglich der durch $\bar{b}(w) = b(w) + (\mathcal{F}_\gamma \cap R')$ definierten Beschreibungsvorschrift effektiv. Schließlich liefert $\tilde{b} : \Omega^* \to R/\mathcal{F}_\gamma$ mit $\tilde{b}(w) = b(w) + \mathcal{F}_\gamma$ eine Beschreibungsvorschrift des gefilterten Ringes $R/\mathcal{F}_\gamma$, bezüglich der auch dieser effektiv ist. Als Beweisskizze betrachten wir das kommutative Diagramm

$$\begin{array}{ccc} & & R/\mathcal{F}_\gamma \\ & & \iota \big| \\ R'/(\mathcal{F}_\gamma \cap R') & & \tilde{b} \\ & \bar{b} & \\ \mathbb{N} & \longrightarrow & \Omega^* \end{array}$$

Wenn das innere Dreieck ein Diagramm des Typs (2.1) für $A = R'/(\mathcal{F}_\gamma \cap R')$ ist, so ist das äußere Diagramm vom Typ (2.1) für $A = R/\mathcal{F}_\gamma$. Grob gesprochen

kann man sagen, daß $R/\mathcal{F}_\gamma$ unter der Bedingung effektiv ist, daß die Restklassen stets durch Repräsentanten aus R' gegeben werden müssen.

Das Noetherschsein und die Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter Ideale übertragen sich von G auf $G/\mathrm{In}(\mathcal{F}_\gamma)$. Sei $H \subset G$ eine beliebige endliche Teilmenge homogener Elemente von G. Wir betrachten die Sequenz

$$G^{|H|} \xrightarrow{\sigma} G \xrightarrow{\tau_\gamma} G/\mathrm{In}(\mathcal{F}_\gamma)$$

der durch $\sigma(e_h) = h$ beziehungsweise $\tau_\gamma(g) = g + \mathcal{F}_\gamma$ definierten natürlichen Homomorphismen graduierter G-Linksmoduln. Für

$$T(H) = \{ge_h \mid h \in H \wedge g \text{ homogenes Element von } G \wedge \deg_\Gamma(g) \circ \deg_\Gamma(h) \preceq \gamma\}$$

wird $ker(\sigma \circ \tau_\gamma)$ von $ker(\sigma) \cup T(H)$ erzeugt. Die Lösbarkeit des Syzygienproblems endlich erzeugter Linksideale von G erlaubt die Berechnung eines endlichen homogenen Erzeugendensystems B von $LSyz(H) = ker(\sigma)$. ι bezeichne den natürlichen Homomorphismus von $G^{|H|}$ nach $(G/\mathrm{In}(\mathcal{F}_\gamma))^{|H|}$. Aus dem kommutativen Diagramm

$$\begin{array}{ccccc} G^{|H|} & & \xrightarrow{\sigma} & & G \xrightarrow{\tau_\gamma} G/\mathrm{In}(\mathcal{F}_\gamma) \\ {\scriptstyle\iota}\downarrow & & & \nearrow_{\sigma_\gamma} & \\ (G/\mathrm{In}(\mathcal{F}_\gamma))^{|H|} & & & & \end{array}$$

erkennt man die Isomorphie $LSyz(\tau_\gamma(H)) = ker(\sigma_\gamma) \cong ker(\sigma \circ \tau_\gamma)/ker(\iota)$ graduierter G-Linksmoduln. Also repräsentieren die Elemente von $B \cup T(H)$ ein homogenes Erzeugendensystem des Linkssyzygienmoduls $LSyz(\tau_\gamma(H))$. Damit ist die Lösbarkeit des T-Syzygienproblems[4] endlich erzeugter homogener Linksideale des assoziierten graduierten Rings $G/\mathrm{In}(\mathcal{F}_\gamma)$ nachgewiesen. Für jede Linkssyzygie $s \in T(\tau_\gamma(H))$ gilt $\textsc{Lift}(s) = 0$, weshalb sie als trivial angesehen werden kann und bei der Standardbasisberechnung unberücksichtigt bleiben darf. Am Rande halten wir fest, daß der Q-Linksmodul $ker(\iota)$ von der Menge $\{ge_h \mid h \in H \wedge g \in \mathrm{In}(\mathcal{F}_\gamma)\} \subseteq T(H)$ erzeugt wird, weshalb viele der trivialen Syzygien aus $T(H)$ sogar nur die Nullsyzygie repräsentieren. Weiterhin betonen wir, daß die Verwendung trivialer Syzygien ein einfaches Kriterium zum Vermeiden unnötiger Reduktionen liefert. Da der assoziierte graduierte Ring von $\mathfrak{R}/\mathcal{F}_\gamma$ noethersch ist, könnte aber auch ganz auf triviale Syzygien verzichtet werden.
Für jedes $a \in R$ bezeichne $[a]_\gamma = a + \mathcal{F}_\gamma$ die Restklasse von a modulo $\mathcal{F}_\gamma$. Da 0 das einzige Element von $R/\mathcal{F}_\gamma$ mit einem Initialterm vom Grad kleiner oder gleich γ ist, gilt

$$\textsc{Divide}_{R/\mathcal{F}_\gamma,\mathrm{lim}}([a]_\gamma, \{[f_1]_\gamma, \ldots, [f_m]_\gamma\}) = [\textsc{Divide}_{R,\mathfrak{T}}(a, \{f_1, \ldots, f_m\}, \gamma)]_\gamma \quad .$$

Aufgrund der Berechenbarkeit von $\textsc{Divide}_{R,\mathfrak{T}}$ ist auch $\textsc{Divide}_{R/\mathcal{F}_\gamma,\mathrm{lim}}$ berechenbar. Da $\mathfrak{T}_\gamma$ diskret ist, sind alle Linksideale von $R/\mathcal{F}_\gamma$ trivialerweise abgeschlossen. Insbesondere ist $R/\mathcal{F}_\gamma$ komplett.

[4] Der Einfachheit halber bezeichnen wir die Funktion, die der Menge $\tau_\gamma(H)$ die durch $T(H)$ repräsentierten Linkssyzygien zuweist, ebenfalls mit T.

Ersetzt man die Funktion $\textsc{Divide}_R$ in der linksseitigen Variante des auf Seite 63 dargestellten Algorithmus GbTest durch $\textsc{Divide}_{R/\mathcal{F}_\gamma,\lim}$ und ruft die auf diese Weise modifizierte Funktion GbTest im Algorithmus Groebner von Seite 63, so erhält man einen Algorithmus, der zu einer beliebigen endlichen Menge eine dasselbe Linksideal erzeugende endliche Standardbasis konstruiert. Anwendung von Bemerkung 6.5 vervollständigt den Beweis. □

In Analogie zu den wohlgeordneten graduierten Strukturen erklären wir die Begriffe des Kopfes und des Restes eines Elementes $a \in R$ durch $\mathrm{head}(a) = \mathrm{in}^*(\mathrm{in}(a))$ beziehungsweise $\mathrm{tail}(a) = a - \mathrm{head}(a)$. Auch der Monomträgerbegriff läßt sich auf die gegenwärtige Situation übertragen, allerdings müssen nun auch unendliche Monomträger zugelassen werden. Eine (möglicherweise endliche) Menge $U = \{u_0, u_1, \ldots\} \subset G$ homogener Elemente mit $\deg_\Gamma(u_{i+1}) \prec \deg_\Gamma(u_i)$ für alle $i = 0, 1, \ldots$ wird im Falle der Existenz der unendlichen Summe $a = \sum_{i=0}^{\infty} \mathrm{in}^*(u_i)$ als Monomträger $\mathrm{Mon}(a)$ von a bezeichnet. Per definitionem ist $\emptyset$ der Monomträger des Nullelements. Jedes Element $a \in R$ besitzt genau einen Monomträger, nämlich die Menge $\mathrm{Mon}(a) = \{u_0 = \mathrm{in}(a), u_1 = \mathrm{in}(\mathrm{tail}(a)), \ldots, u_i = \mathrm{in}(\mathrm{tail}^i(a)), \ldots\} \backslash \{0\}$, wobei $\mathrm{tail}^i(a)$ das Ergebnis der i-maligen Anwendung der Funktion tail auf a bezeichnet. Für jede Folge homogener Elemente u_i mit streng monoton fallenden Γ-Graden bilden die Partialsummen $\sum_{i=0}^{k} \mathrm{in}^*(u_i)$ eine Cauchy-Folge. Somit besteht in einem kompletten Ring R eine Bijektion zwischen den Teilmengen $U = \{u_0, u_1, \ldots\} \subset G$ homogener Elemente mit $\deg_\Gamma(u_{i+1}) \prec \deg_\Gamma(u_i)$ für alle $i = 0, 1, \ldots$ und den Elementen von R. Da $\prec$ beschränkte Wohlordnung ist, ist die Menge $\{u \in \mathrm{Mon}(a) \mid \gamma \preceq \deg_\Gamma(u)\}$ für beliebige $a \in R$ und $\gamma \in \Gamma$ endlich. Das Element $\mathrm{trunc}(a, \gamma) \in R$ mit $\mathrm{Mon}(\mathrm{trunc}(a, \gamma)) = \{u \in \mathrm{Mon}(a) \mid \gamma \prec \deg_\Gamma(u)\}$ wird γ-*Anfangsstück* von a genannt. In Anlehnung an die übliche Sprechweise für Potenzreihen sagen wir auch, daß $\mathrm{trunc}(a, \gamma)$ durch *Abschneiden* von a beim Grad γ entsteht.

Im weiteren setzen wir voraus, daß der assoziierte graduierte Ring G der graduierten Struktur $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ effektiv und noethersch ist sowie ein entscheidbares Enthaltenseinsproblem für homogene Linksideale aufweist. Außerdem sei R in der von $\mathfrak{R}$ induzierten Topologie komplett. Gemäß Satz 6.6 und Folgerung 6.3 ist jedes Linksideal $I \subseteq R$ topologisch abgeschlossen und besitzt eine endliche Standardbasis F. Da G effektiv ist und ein entscheidbares Enthaltenseinsproblem für homogene Linksideale aufweist, gibt es einen kanonischen Simplifikator $S_{\mathrm{LIn}(I)} : G \to G$ des Faktorlinksmoduls $G/\mathrm{LIn}(I)$, welcher homogene Elemente in gradgleiche homogene Elemente überführt. Ein derartiges $S_{\mathrm{LIn}(I)}$ werden wir auch *homogenen kanonischen Simplifikator* nennen. Da R komplett ist, ist die Funktion $\textsc{Divide}_{R,\lim}$ total. Verwenden wir F als zweites Argument der Funktion, so hängt der Wert $\varphi(\hat{a})$ des Restes $\hat{a}$ bei Division von $a \in R$ modulo F mittels $\textsc{Divide}_{R,\lim}$ nur noch von der Restklasse von a modulo I ab. Durch einen anschließenden Normierungsschritt gelangt man zu einer Divisionsfunktion $\underline{\textsc{Divide}}_{R,\lim}$, bei welcher der Initialterm des Divisionsrestes von a modulo der Standardbasis F ein Fixpunkt von $S_{\mathrm{LIn}(I)}$ ist und daher auch nur noch von der Restklasse $a + I$ abhängt. Mit Hilfe einer Rekursion des Typs (5.15) gelangt man schließlich zu einer echten Divisions-

funktion $\overline{\text{DIVIDE}}_{R,\lim}$, bei welcher der gesamte Divisionsrest von a modulo der Standardbasis F bereits durch die Restklasse $a+I$ eindeutig bestimmt wird. Die Funktion $S_I : R \to R$, welche jedem Element $a \in R$ ihren eindeutig bestimmten Rest bei der Division $\overline{\text{DIVIDE}}_{R,\lim}$ modulo der Standardbasis F von I zuweist, ist eine kanonische Auswahlfunktion für R/I. Falls $\text{DIVIDE}_{R,\lim}$ berechenbar ist, die Hauptrekursion in $\overline{\text{DIVIDE}}_{R,\lim}$ terminiert und aus einem beliebigen endlichen Erzeugendensystem von I eine Standardbasis F berechnet werden kann, dann ist die Funktion $\overline{\text{DIVIDE}}_{R,\lim}$ berechenbar und S_I ein kanonischer Simplifikator von R/I. In Restklassenringen $R/\mathcal{F}_\gamma$ des in Satz 6.7 beschriebenen Typs sind alle Anforderungen erfüllt. Natürlich kann in Analogie zu Definition 5.11 auch der Begriff der *reduzierten Standardbasis* eingeführt werden.

Die Restklasse $a+I$ kann höchstens ein Element $\hat{a}$ enthalten, dessen Monomträger nur aus Fixpunkten von $S_{\text{LIn}(I)}$ besteht. Außerdem erfüllt $S_I(a)$ gerade diese an $\hat{a}$ gestellten Bedingungen. Somit ist gezeigt, daß $S_I(a)$ das eindeutig bestimmte Element von R ist, welches kongruent zu a modulo I ist und dessen Monomträger ausschließlich Fixpunkte von $S_{\text{LIn}(I)}$ enthält.

Während die in Frage stehenden topologischen Ringe, wie zum Beispiel der Ring der formalen Potenzreihen, unbeschränkte direkte Summen zyklischer Moduln sein können, sind die assoziierten graduierten Ringe, ähnlich dem wohlgeordneten Fall, nur beschränkte direkte Summen. Beispielsweise haben der Polynomring $Q[x]$ und der formale Potenzreihenring $Q[[X]]$ bezüglich einer üblichen $T(X)$-graduierten Struktur bis auf Isomorphie beide den Polynomring $Q[X]$ als assoziierten graduierten Ring. Die formalen Potenzreihenringe $R = Q[[X]]$ stellen den Hauptanwendungsfall der in diesem Abschnitt beschriebenen Theorie dar. Aufgrund seiner Überabzählbarkeit ist ein formaler Potenzreihenring nicht gödelisierbar. Somit ist er keine effektive algebraische Struktur und besitzt erst recht kein entscheidbares Idealenthaltenseinsproblem. Weder die Funktion $\text{DIVIDE}_{R,\lim}$ noch die Auswahlfunktion S_I sind berechenbar. Dennoch kann man interessante konstruktive Teilergebnisse erzielen, denn es wird sich herausstellen, daß, grob gesprochen, beliebig genaue Näherungen der Funktionswerte von $\overline{\text{DIVIDE}}_{R,\lim}$ und S_I berechnet werden können.

Satz 6.8 *Die graduierte Ringstruktur $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ und der Unterring $R' \subseteq R$ mögen den Voraussetzungen von Satz 6.7 genügen. Außerdem sei R in der durch $\mathfrak{R}$ festgelegten Topologie komplett. Für jedes Linksideal $I \subseteq R$ bezeichne $S_{\text{LIn}(I)}$ einen beliebigen festen homogenen kanonischen Simplifikator des Restklassenmoduls $G/\text{LIn}(I)$. $H \subset R'$ sei eine endliche Teilmenge und I bezeichne das davon in R erzeugte Linksideal.*

Dann ist die Funktion $S_I^{(\gamma)} : R' \to R'$, die jedem $a \in R'$ das γ-Anfangsstück $\text{trunc}(\hat{a}, \gamma)$ des Elementes $\hat{a} \in R$ mit $a - \hat{a} \in I$ und $\forall u \in \text{Mon}(\hat{a}) : S_{\text{LIn}(I)}(u) = u$ zuordnet, für alle $\gamma \in \Gamma$ berechenbar.

Beweis: Zunächst einmal halten wir fest, daß das Element $\hat{a} = S_I(a)$ als der Wert der oben eingeführten Auswahlfunktion eindeutig bestimmt ist und somit ist $S_I^{(\gamma)}$ wohldefiniert. I_γ bezeichne das homomorphe Bild von I unter dem natürlichen Homomorphismus $\sigma : R \to R/\mathcal{F}_\gamma$.

Der assoziierte graduierte Ring der induzierten graduierten Struktur $\mathfrak{R}/\mathcal{F}_\gamma$ des Restklassenringes $R/\mathcal{F}_\gamma$ ist isomorph zum Restklassenring $G/\mathrm{In}(\mathcal{F}_\gamma)$ des assoziierten graduierten Rings G von $\mathfrak{R}$ nach dem Initialideal von $\mathcal{F}_\gamma$. Das vollständige Urbild $im(u+\mathrm{In}(\mathcal{F}_\gamma))$ eines beliebigen von Null verschiedenen homogenen Elements $u+\mathrm{In}(\mathcal{F}_\gamma) \in G/\mathrm{In}(\mathcal{F}_\gamma)$ unter dem natürlichen Homomorphismus von G nach $G/\mathrm{In}(\mathcal{F}_\gamma)$ enthält genau ein homogenes Element $\tilde{u} \in G$ und die durch $S_{\mathrm{LIn}(I_\gamma)}(\mathrm{In}(\mathcal{F}_\gamma)) = \mathrm{In}(\mathcal{F}_\gamma)$ und $S_{\mathrm{LIn}(I_\gamma)}(u+\mathrm{In}(\mathcal{F}_\gamma)) = S_{\mathrm{LIn}(I)}(\tilde{u}) + \mathrm{In}(\mathcal{F}_\gamma)$ definierte Funktion ist ein homogener kanonischer Simplifikator des Faktormoduls von $G/\mathrm{In}(\mathcal{F}_\gamma)$ nach $\mathrm{LIn}(I_\gamma)$.

Ausgehend von $S_{\mathrm{LIn}(I_\gamma)}$ kann man aus jeder Restklasse $a+I_\gamma$ des Restklassenringes von $R/\mathcal{F}_\gamma$ modulo I_γ das eindeutig bestimmte Element $\hat{a} \in R/\mathcal{F}_\gamma$ mit $a-\hat{a} \in I_\gamma$ und $\forall u+\mathrm{In}(\mathcal{F}_\gamma) \in \mathrm{Mon}(\hat{a}) : S_{\mathrm{LIn}(I_\gamma)}(u+\mathrm{In}(\mathcal{F}_\gamma)) = u+\mathrm{In}(\mathcal{F}_\gamma)$ auszeichnen. Die durch $a \mapsto \hat{a}$ definierte Funktion $S_{I_\gamma} : R/\mathcal{F}_\gamma \to R/\mathcal{F}_\gamma$ ist gerade der im Vorfeld dieses Satzes beschriebene kanonische Simplifikator von $R/\mathcal{F}_\gamma$ modulo I_γ, welcher auf dem homogenen kanonischen Simplifikator $S_{\mathrm{LIn}(I_\gamma)}$ beruht. Ein Algorithmus zu seiner Berechnung wurde in diesem Zusammenhang bereits skizziert.

Sei $\mathrm{Mon}(S_I(a)) = \{u_0, u_1, \ldots\}$, also insbesondere $S_I(a) = \sum_{i=0}^{\infty} \mathrm{in}^*(u_i) = \sum_{i=0}^{k} \mathrm{in}^*(u_i) + \sum_{i=k+1}^{\infty} \mathrm{in}^*(u_i)$, wobei k so gewählt ist, daß $\deg_\Gamma(u_0) \succ \deg_\Gamma(u_1) \succ \cdots \succ \deg_\Gamma(u_k) \succ \gamma \succeq \deg_\Gamma(u_{k+1}) \succ \cdots$ erfüllt wird. Dabei setzen wir für endliche Mengen $\mathrm{Mon}(S_I(a))$ formal $u_i = 0$ und $\deg_\Gamma(u_i) = -\infty$ für alle $i \geq |\mathrm{Mon}(S_I(a))|$. Unterwirft man $S_I(a)$ dem natürlichen Homomorphismus $\sigma : R \to R/\mathcal{F}_\gamma$, so ergibt sich

$$\sigma(S_I(a)) = \sum_{i=0}^{k} \sigma(\mathrm{in}^*(u_i)) + \sigma\left(\sum_{i=k+1}^{\infty} \mathrm{in}^*(u_i)\right) = \sigma\left(S_I^{(\gamma)}(a)\right) \quad .$$

Man erkennt

$$\mathrm{Mon}\left(\sigma\left(S_I^{(\gamma)}(a)\right)\right) = \{u_0 + \mathrm{In}(\mathcal{F}_\gamma), \ldots, u_k + \mathrm{In}(\mathcal{F}_\gamma)\}$$

und $S_{\mathrm{LIn}(I_\gamma)}(u_i + \mathrm{In}(\mathcal{F}_\gamma)) = u_i + \mathrm{In}(\mathcal{F}_\gamma)$ für alle $0 \leq i \leq k$. Somit erfüllt $\sigma\left(S_I^{(\gamma)}(a)\right)$ alle an $S_{I_\gamma}(a+\mathcal{F}_\gamma)$ gestellten Anforderungen, weshalb Gleichheit vorliegen muß. Also:

$$\forall a \in R : S_{I_\gamma}(a+\mathcal{F}_\gamma) = \sigma\left(S_I^{(\gamma)}(a)\right) = \sigma(S_I(a)) = S_I(a) + \mathcal{F}_\gamma \quad . \qquad (6.2)$$

Kommen wir auf unser Ausgangsproblem der Berechnung von $S_I^{(\gamma)}(a)$ für $a \in R'$ und I gegeben durch ein endliches Linksidealerzeugendensystem $H \subset R'$ zurück. Man berechnet das Bild von $a+\mathcal{F}_\gamma$ unter dem kanonischen Simplifikator S_{I_γ}. Da alle Eingabedaten dem Unterring R' angehören, kann im zu $R/\mathcal{F}_\gamma$ isomorphen effektiven Ring $R'/(\mathcal{F}_\gamma \cap R')$ gerechnet werden. Als Ausgabe erhält man einen Repräsentanten $b \in R'$ von $S_{I_\gamma}(a+\mathcal{F}_\gamma)$. Der Monomträger von $S_{I_\gamma}(a+\mathcal{F}_\gamma)$ ist in jedem Fall endlich und zu jedem Element des Monomträgers kann der eindeutig bestimmte homogene Repräsentant aus G berechnet werden. Die Menge dieser homogenen Repräsentanten bildet gerade den Monomträger $\{u_0, \ldots, u_k\}$ von

$S_I^{(\gamma)}(a)$. Aufgrund der Berechenbarkeit von in^*, der Beziehung $im(\mathrm{in}^*) \subseteq R'$ und der Effektivität von R' kann schließlich die endliche Summe $S_I^{(\gamma)}(a) = \sum_{i=0}^{k} \mathrm{in}^*(u_i) \in R'$ berechnet werden. □

Die Abbildungsvorschrift von $S_I^{(\gamma)}$ läßt sich ohne weiteres auf Elemente aus ganz R ausdehnen. Ebenso können entsprechende Funktionen $S_I^{(\gamma)}$ auch für Linksideale I, die kein Erzeugendensystem aus R' besitzen, erklärt werden. Allerdings sind diese verallgemeinerten Funktionen $S_I^{(\gamma)} : R \to R'$ nur noch relativ zu einer Funktion $\mu_\gamma : R \to R'$ mit $a - \mu_\gamma(a) \in \mathcal{F}_\gamma$ berechenbar und falls R nicht gödelisierbar ist, so kann es keine berechenbare Funktion μ_γ geben. Identifiziert man die Elemente des Restklassenringes $R/\mathcal{F}_\gamma$ in natürlicher Weise mit den Elementen von R, deren Monomträger keine Elemente vom Grad kleiner oder gleich γ enthalten, so konvergieren die kanonischen Simplifikatoren S_{I_γ} für $\gamma \to -\infty$ gegen die kanonische Auswahlfunktion S_I. Genauer bedeutet das: für jede streng monoton fallende Folge $\gamma_0 \succ \gamma_1 \succ \cdots$ und alle $a \in R$ gilt:

$$\lim_{i \to \infty} S_{I_{\gamma_i}}(a) = S_I(a) \quad .$$

Ähnliche Untersuchungen wie für den Divisionsrest zeigen, daß auch die weiteren Bestandteile des Funktionswertes von $\overline{\textsc{Divide}}_{R,\lim}(a, F)$, also die Kofaktoren der Elemente von F, bei sukzessiver Berechnung in den Restklassenringen R/F_{γ_i} für $\gamma_0 \succ \gamma_1 \succ \cdots$ ein derartiges Konvergenzverhalten aufweisen. Bei der Abschätzung der Güte der Näherung ist nur zu berücksichtigen, daß nicht die Rechnung in R/F_γ sondern erst die in $R/F_{\gamma \circ \varphi(f_j)}$ auf das Anfangsstück $\mathrm{trunc}(g_j, \gamma)$ des Kofaktors g_j von f_j führt. Die vorangegangenen Untersuchungen zeigen, daß die Funktion $\overline{\textsc{Divide}}_{R,\lim}$ in beiden Argumenten stetig ist.

Kommen wir noch einmal auf die Einordnung der formalen Potenzreihenringe in die dargestellte Theorie zu sprechen. Der Ring $R = Q[[X_1, \ldots, X_n]]$ wird mit dem freien von $X = \{X_1, \ldots, X_n\}$ erzeugten kommutativen Monoid $\Gamma = T(X)$ bewertet, dabei ist auf $T(X)$ eine beschränkte Monoidwohlordnung $\prec$ mit $X_1^{\nu_1} \cdots X_n^{\nu_n} \preceq 1$ für alle $\nu_1, \ldots, \nu_n \in \mathbb{N}$ erklärt. Eine Möglichkeit zur Beschreibung einer derartigen Ordnung $\prec$ findet man in Bemerkung 4.1. Die Funktion φ weist jeder formalen Potenzreihe $a = \sum_{\nu_1,\ldots,\nu_n} \alpha_{\nu_1,\ldots,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n}$ den bezüglich $\prec$ maximalen Term $X_1^{\mu_1} \cdots X_n^{\mu_n}$ mit der Eigenschaft $\alpha_{\mu_1,\ldots,\mu_n} \neq 0$ zu. Als Unterring R' wird der Polynomring $Q[X_1, \ldots, X_n]$ gewählt. Dieser ist gleichzeitig isomorph zum assoziierten graduierten Ring der beschriebenen graduierten Struktur. In diesem Sinne kann das Monom $\alpha_{\mu_1,\ldots,\mu_n} X_1^{\mu_1} \cdots X_n^{\mu_n}$ des $T(X)$-Grades $\varphi(a)$ mit dem Initialterm $\mathrm{in}(a)$ identifiziert werden. Außerdem kann in^* als die identische Abbildung auf der Menge aller Monome definiert werden und das Abschneiden einer Potenzreihe an einem vorgegebenen Potenzprodukt $X_1^{\nu_1} \cdots X_n^{\nu_n}$ geschieht in der üblichen Weise durch Weglassen aller Monome, die höchstens den $T(X)$-Grad $X_1^{\nu_1} \cdots X_n^{\nu_n}$ aufweisen. Die Anwendbarkeit der Sätze 6.7 und 6.8 verlangt, daß der Koeffizientenbereich Q ein effektiver linksnoetherscher Ring mit entscheidbarem Linksidealenthaltenseinsproblem und lösbarem Linkssyzygienproblem ist. Insbesondere kann es sich um einen effektiven Körper, zum Beispiel den der rationalen Zahlen, oder einen

effektiven Euklidischen Ring handeln. Außerdem muß die Ordnung $\prec$ entscheidbar sein, was beispielsweise für Ordnungen $\prec=\prec_{\mathfrak{A}}$ mit regulärer Matrix $\mathfrak{A}$ mit rationalen Einträgen der Fall ist.

6.2 Gröbnerbasen im Ring der ganzen Funktionen

Die Elemente $f \in R$ des Polynomrings $R = \mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[X]$ lassen sich vermöge der Vorschrift

$$f(\alpha_1, \ldots, \alpha_n) = \sigma_{\alpha_1,\ldots,\alpha_n}(f) \quad , \tag{6.3}$$

wobei $\sigma_{\alpha_1,\ldots,\alpha_n} : R \to \mathbb{K}$ den durch $X_i \mapsto \alpha_i$ definierten Ringhomomorphismus bezeichnet, als Funktionen $f : \mathbb{K}^n \to \mathbb{K}$ auffassen.

Für den Rest dieses Abschnitts werden wir stets $\mathbb{K} = \mathbb{C}$ annehmen und die obige Funktionsinterpretation so weit wie möglich auf Potenzreihen ausdehnen. Faßt man die rechte Seite als komplexe Reihe auf, dann beschreibt die Zuordnungsvorschrift

$$f(\alpha_1, \ldots, \alpha_n) = \sum_{\nu_1,\ldots,\nu_n} \beta_{\nu_1,\ldots,\nu_n} \alpha_1^{\nu_1} \cdots \alpha_n^{\nu_n}$$

in natürlicher Weise eine partielle n-stellige komplexe Funktion. Die Elemente des Definitionsbereichs von f sind genau die n-Tupel komplexer Zahlen, für die die Summe existiert. Die Frage nach Konvergenz und Summe der Reihe bedarf zunächst einmal einer fest vorgegebenen Wohlordnung der Exponentenvektoren $(\nu_1, \ldots, \nu_n)$. Unser Interesse gilt jedoch ausschließlich den *beständig konvergenten Potenzreihen*, das heißt den Potenzreihen $f \in \mathbb{C}[[X_1, \ldots, X_n]]$, die eine totale komplexe Funktion $f : \mathbb{C}^n \to \mathbb{C}$ beschreiben. Eine derartige Funktion f wird auch *ganze Funktion* genannt, sie konvergiert an jeder Stelle von $\mathbb{C}^n$ absolut und ist folglich in jedem beschränkten Gebiet von $\mathbb{C}^n$ gleichmäßig konvergent. Aus diesem Grund ist der Grenzwert der Partialsummenfolge gegenüber Umordnung der Summanden invariant, weshalb insbesondere die zugrundegelegte Wohlordnung der Exponentenvektoren irrelevant wird. Die Menge aller beständig konvergenten Potenzreihen aus S bildet einen Unterring, dieser heißt *Ring der ganzen Funktionen* und wird mit $E = \mathbb{C}\{\{X_1, \ldots, X_n\}\}$ bezeichnet. Ähnlich zum Polynomfall beschreibt die Abbildungsvorschrift $X_i \mapsto \alpha_i$ für beliebige $\alpha_i \in \mathbb{C}$ $(1 \leq i \leq n)$ einen Substitutionshomormorphismus $\sigma_{\alpha_1,\ldots,\alpha_n} : E \to \mathbb{C}$ und für beliebige $f \in E$ und $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ gilt Gleichung (6.3).

Die im Zusammenhang mit ganzen Funktionen betrachteten geometrischen Fragestellungen verlangen die Ausstattung von E mit der lokalen gleichmäßigen Konvergenz und wenn nicht explizit auf das Gegenteil hingewiesen wird, so werden wir E in Zukunft immer als toplogischen Ring in dieser Topologie ansehen. Die Krullsche Topologie und die Topologie der lokalen gleichmäßigen Konvergenz sind unvergleichbar, so ist es nicht erstaunlich, daß die in Abschnitt 6.1 vorgestellte Theorie der Standardbasen nicht zur Behandlung ganzer Funktionen geeignet ist. Der notwendige Übergang zum Abschluß eines Ideals und die Verlegung der Untersuchungen in den in der Krullschen Topologie kompletten Ring $S = \mathbb{C}[[X_1, \ldots, X_n]]$ ist nicht mit geometrischen Untersuchungen von

Nullstellengebilden vereinbar. Die Wertlosigkeit des Übergangs nach S wird bereits daran deutlich, daß der Ring S keine treue Erweiterung von E ist. So besitzt die Taylorreihe der Cosinusfunktion $\cos X_1$ Nullstellen, sie ist in E nicht invertierbar und erzeugt dort ein nichttriviales Ideal. Bei Einbettung in S wird die Cosinusreihe zur Einheit und Kontraktion des von ihr erzeugten Ideals nach E führt auf das triviale Ideal E mit leerem Nullstellengebilde.

Allgemein muß man feststellen, daß eine beliebige graduierte Struktur von E mit dem geordneten Wertemonoid $(T(X), \prec)$, wobei $\prec$ eine beliebige Monoidordnung mit der Eigenschaft $X_i \prec 1$ $(1 \leq i \leq n)$ ist, zum Aufbau von Divisionsalgorithmen ungeeignet ist, da die Reduktionssequenzen im allgemeinen nicht in der Topologie der lokalen gleichmäßigen Konvergenz konvergieren. Als Beispiel betrachte man $X_1 \bmod (X_1 - X_1^2)$, was die divergierende Folge $X_1, X_1^2, X_1^3, \ldots$ von Zwischenresten liefert.

Eine Fortsetzung einer wohlgeordneten $T(X)$-graduierte Struktur des Polynomrings R auf E ist ebensowenig möglich, da sich die Bewertung $\varphi = \mathrm{lpp}$ nicht zu einer Pseudobewertung auf ganz E fortsetzen läßt.

Da bereits der Koeffizientenkörper $\mathbb{C}$ überabzählbar und somit nicht effektiv ist, kann E erst recht keine effektive algebraische Struktur sein. Auch bei Einschränkung des Koeffiezientenbereichs auf den effektiven Körper der rationalen Zahlen entsteht noch ein überabzählbarer Unterring von E. Dennoch kann man ähnlich wie in Abschnitt 6.1 nach einem effektiven Unterring E' von E fragen, so daß man die Berechnung von Divisionsresten von Elementen aus E modulo Idealen von E durch algorithmisch ausführbare Berechnungen in E' mit vorgegebener Genauigkeit approximieren kann. Die Arbeit [ASTW] zeigt die theoretische Lösung dieser Fragestellung auf und [Ap95a] gibt Teilantworten auf das Approximationsproblem.

6.2.1 Ein Konvergenzkriterium für Reihen ganzer Funktionen

Für spätere Beweise benötigen wir ein Kriterium zum Nachweis, daß eine Reihe ganzer Funktionen in der Topologie der lokalen gleichmäßigen Konvergenz konvergiert. Dieses wollen wir hier kurz bereitstellen. Für Beweise und weitergehende Ausführungen wird auf [GR71] verwiesen.

Mit $\mathbb{R}_+$ bezeichnen wir die Menge der positiven reellen Zahlen und mit $S = \mathbb{C}[[X_1, \ldots, X_n]]$ den Ring der formalen Potenzreihen über den komplexen Zahlen. Für ein beliebiges n-Tupel $r = (r_1, \ldots, r_n) \in \mathbb{R}_+^n$ positiver reeller Zahlen definiert

$$\left\| \sum_{\nu_1,\ldots,\nu_n} \beta_{\nu_1,\ldots,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \right\|_r := \sum_{\nu_1,\ldots,\nu_n} |\beta_{\nu_1,\ldots,\nu_n}| r_1^{\nu_1} \cdots r_n^{\nu_n} \,, \tag{6.4}$$

eine Abbildung $\| \cdot \|_r \ : \ S \to \mathbb{R} \cup \{+\infty\}$. Für festes r ist $\| \cdot \|_r$ eine Norm auf der Menge $B_r := \{g \in S \ \mid \ \|g\|_r < +\infty\}$ aller formalen Potenzreihen g mit endlichem Funktionswert $\|g\|_r$ und B_r bildet eine analytische $\mathbb{C}$-Banachalgebra. Insbesondere erfüllt die Norm $\| \cdot \|_r$ für alle $f, g \in B_r$ die Dreiecksungleichung

$$\|f + g\|_r \leq \|f\|_r + \|g\|_r \quad . \tag{6.5}$$

Darüberhinaus gilt im Spezialfall $\mathrm{supp}(f) \cap \mathrm{supp}(g) = \emptyset$ stets die Gleichheit. $<$ bezeichne die Produktordnung der gewöhnlichen Kleinerordnung reeller Zahlen auf $\mathbb{R}_+^n$, also $r = (r_1, \ldots, r_n) < (s_1, \ldots, s_n) = s$ genau dann, wenn $r_i < s_i$ für alle $i = 1, \ldots, n$. Dann gilt $B_s \subset B_r$ für alle $r < s$. Eine Potenzreihe $g \in S$ wird *konvergent* genannt, falls es ein $r \in \mathbb{R}_+^n$ mit $g \in B_r$ gibt. $g \in B_r$ beschreibt eine in jedem Polyzylinder $Z_s = \{t = (t_1, \ldots, t_n) \in \mathbb{C}^n \mid |t_i| < s_i\}$ mit $\mathbb{R}_+^n \ni s = (s_1, \ldots, s_n) < r$ gleichmäßig konvergente Funktion. Für jede in der Banachtopologie von B_r konvergente Folge $g_1, g_2, \ldots$ von Potenzreihen $g_i \in B_r$ bilden die durch die g_i beschriebenen Funktionen eine im Polyzylinder Z_t gleichmäßig konvergente Folge stetiger Funktionen. Die beständig konvergenten Potenzreihen sind gerade die Elemente des Durchschnitts $E = \bigcap_{r \in \mathbb{R}_+^n} B_r$ und die auf E durch das System der in (6.4) definierten Seminormen $\|\cdot\|_r$ gegebene Topologie stimmt mit der Topologie der lokalen gleichmäßigen Konvergenz überein. Wir nennen eine Folge $(r_i)_{i=1,2,\ldots}$ von n-Tupeln $r_i = (\rho_{i,1}, \ldots, \rho_{i,n})$ positiver reeller Zahlen *komponentenweise bestimmt divergent*, falls für alle $1 \leq j \leq n$ die Beziehung $\lim_{i \to \infty} \rho_{i,j} = +\infty$ gilt.

Für eine beliebige Teilmenge $\mathcal{D} \subseteq T(X)$ von Potenzprodukten bildet die Menge $B_r(\mathcal{D})$ aller Potenzreihen aus B_r, in denen höchstens die Potenzprodukte aus $\mathcal{D}$ mit von Null verschiedenem Koeffizienten auftreten dürfen, einen in der Banachtopologie von B_r abgeschlossenen linearen Unterraum von B_r. Weiterhin ist die Menge $E(\mathcal{D})$ aller ganzen Funktionen, in denen nur Potenzprodukte aus $\mathcal{D}$ auftreten, ein abgeschlossener linearer Unterraum von E. Damit ergibt sich:

Lemma 6.9 *Sei $(r_i)_{i=1,2,\ldots}$ eine komponentenweise bestimmt divergente Folge von n-Tupeln positiver reeller Zahlen. Für jedes $t \in T(X)$ sei g_t ein Element von $E(\mathcal{D})$. Falls*

$$\sum_{t \in T(X)} \|g_t\|_{r_i} < +\infty\,, \qquad \textit{für alle} \qquad i = 1, 2, \ldots,$$

dann ist die Reihe $\sum_{t \in T(X)} g_t$ konvergent und ihre Summe liegt in $E(\mathcal{D})$.

6.2.2 Die Divisionsformel

Im Unterschied zu den Untersuchungen in den Abschnitten 5.2 und 6.1 ist es bei der Untersuchung des Ringes $E = \mathbb{C}\{\{X_1, \ldots, X_n\}\}$ der ganzen Funktionen unmöglich, eine geeignete graduierte Struktur auf E selbst zu finden. Eine graduierte Struktur des Unterrings $R = \mathbb{C}[X_1, \ldots, X_n]$ der Polynome wird sich aber bereits zum Aufbau einer Divisionsformel von $a \in E$ modulo eines Ideals IE mit polynomialem Erzeugendensystem $H \subset R$ als ausreichend erweisen.

Für n-Tupel $\nu = (\nu_1, \ldots, \nu_n)$ natürlicher Zahlen vereinbaren wir die Multiindexschreibweise $X_1^{\nu_1} \cdots X_n^{\nu_n} = X^\nu$ der Potenzprodukte der Menge $T = T(X)$. Jede formale Potenzreihe $a \in S$ läßt sich auf eindeutige Weise in der Form $a = \sum_{\nu \in \mathbb{N}^n} \alpha_\nu X^\nu$ darstellen. Die Menge $\mathrm{supp}(a) = \{X^\nu \in T \mid \alpha_\nu \neq 0\}$ der in a vorkommenden Potenzprodukte heißt der *Träger* der formalen Potenzreihe a. Durch entsprechende Einschränkung der Funktion supp auf die Unterringe E und R von S gelangt man zu den Begriffen des Trägers einer ganzen

Funktion beziehungsweise eines Polynoms. Zusätzlich führen wir wieder den Begriff des Monomträgers $\mathrm{Mon}(a) = \{\alpha_\nu X^\nu \in T \mid \alpha_\nu \neq 0\}$ der Potenzreihe $a = \sum_{\nu\in\mathbb{N}^n} \alpha_\nu X^\nu$ ein. Sei $\prec$ eine beliebige Monoidwohlordnung von T. Dann wird durch

$$\mathrm{lpp}(a) = \max_{\prec}(\mathrm{supp}(a))$$

eine partielle Funktion auf S erklärt, ihr Definitionsbereich ist genau die Teilmenge aller von Null verschiedenen Polynome. Im Falle seiner Existenz wird $\mathrm{lpp}(a)$ das *führende Potenzprodukt* und sein Koeffizient $\mathrm{lc}(a)$ der *Leitkoeffizient* von a genannt. Einschränkung von lpp auf R führt auf eine T-Bewertung des Polynomrings R. Derartige Bewertungen kommen in der klassischen Gröbnertheorie in Polynomringen zum Einsatz.

Sei $\mathfrak{R} = (R, T(X), \prec, \mathrm{lpp})$ eine graduierte Struktur des Polynomrings R mit einer Wohlordnung $\prec$ und der oben definierten Bewertung lpp. Der assoziierte graduierte Ring ist isomorph zu R und wir vereinbaren die identische Abbildung auf der Menge der Monome als Rückschnitt in^* der Initialfunktion. Entsprechend genügen $\mathrm{head}(a) = \mathrm{in}^*(\mathrm{in}(a)) = \mathrm{lc}(a)\mathrm{lpp}(a)$ und $\mathrm{tail}(a) = a - \mathrm{head}(a)$ den in Polynomringen üblichen Definitionen des Kopfes beziehungsweise des Restes eines von Null verschiedenen Polynoms a. Außerdem stimmt der oben eingeführte Begriff des Monomträgers $\mathrm{Mon}(a)$ für alle Polynome mit dem zu $\mathfrak{R}$ und in^* gehörigen überein.

Anwendung der in Kapitel 5 dargestellten Gröbnertheorie sichert für beliebige endliche Mengen $H = \{h_1, \ldots, h_k\} \subset R$ und beliebige Polynome a die Existenz einer Divisionsformel

$$a = \sum_{i=1}^{k} b_i h_i + b, \text{ mit} \tag{6.6}$$

$$\forall 1 \leq i \leq k \left(\mathrm{lpp}(b_i h_i) \preceq \mathrm{lpp}(a) \quad \wedge \quad \forall X^\nu \in \mathrm{supp}(b) \; : \; \mathrm{lpp}(h_i) \nmid X^\nu \right) .$$

Ist die Menge H sogar eine Gröbnerbasis des von ihr erzeugten Ideals I, so ist b das eindeutig bestimmte Element der Restklasse $a + I$ mit der Eigenschaft $\mathrm{supp}(b) \cap \mathrm{In}(I) = \emptyset$. $\mathrm{rem}_I : R \to R$ bezeichne die Funktion, die jedem Polynom $a \in R$ den Divisionsrest $b \in R$ modulo einer Gröbnerbasis H von I zuweist. Anliegen ist es, die Funktion rem_I stetig auf ganz E zu einer Restfunktion modulo des Erweiterungsideals IE fortzusetzen. Im Gegensatz zu b sind die in (6.6) auftretenden Kofaktoren b_i der h_i im allgemeinen selbst für Gröbnerbasen H nicht eindeutig bestimmt. Durch zusätzliche Einschränkungen läßt sich nicht nur ihre Eindeutigkeit erzwingen, sondern auch erreichen, daß die für $1 \leq i \leq k$ durch $a \mapsto b_i$ erklärten Abbildungen $\mathrm{q}_I^{(i)} : R \to R$ auf E stetig fortsetzbare Funktionen werden.

Sei $H = \{h_1, \ldots, h_k\}$ eine nicht das Nullelement enthaltende Gröbnerbasis von I bezüglich der graduierten Struktur $\mathfrak{R}$. Dabei nehmen wir $k \geq 1$ an, d.h. der Trivialfall $I = \{0\}$ wird ausgeschlossen. Wir fixieren eine Zerlegung $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ des aus den führenden Potenzprodukten aller Elemente von I bestehenden Monoidideals $\mathrm{lpp}(I) = \mathrm{lpp}(H) \circ T \subseteq T$ in paarweise disjunkte Teilmengen Δ_i mit der Eigenschaft $t \in \Delta_i \Longrightarrow \mathrm{lpp}(h_i) \mid t$ und verschärfen

die an die Divisionsformel (6.6) gestellten Anforderungen dahingehend, daß zusätzlich

$$\forall X^\nu \in \mathrm{supp}(b_i) \ : \ X^\nu \, \mathrm{lpp}(h_i) \in \Delta_i \tag{6.7}$$

gelten soll. Man überzeugt sich leicht von der Existenz geeigneter Polynome b und $b_1, \ldots, b_k$, welche gleichzeitig den Bedingungen (6.6) und (6.7) genügen. Kommen wir zum Nachweis der Eindeutigkeit der Lösung. Sei $b', b'_1, \ldots, b'_k$ ein zweiter Satz von den Bedingungen (6.6) und (6.7) genügenden Polynomen. Aus der Gröbnerbasiseigenschaft von H folgt sofort die Gleichheit $b = b'$ und somit auch

$$\sum_{i=1}^{k} b_i h_i = \sum_{i=1}^{k} b'_i h_i \quad . \tag{6.8}$$

Wir setzen $M := \{m \ | \ 1 \leq m \leq k \wedge b_m \neq b'_m\}$. Für alle $m \in M$ gilt $\mathrm{lpp}(b_m - b'_m) \in \mathrm{supp}(b_m) \cup \mathrm{supp}(b'_m)$ und mit (6.7) ergibt sich die Beziehung $\mathrm{lpp}(b_m - b'_m) \, \mathrm{lpp}(h_m) \in \Delta_m$. Demzufolge sind die führenden Potenzprodukte aller Summanden der Summe $\sum_{m \in M}(b_m - b'_m)h_m$ paarweise verschieden und da die Summe wegen (6.8) gleich Null sein muß, liegt $M = \emptyset$ vor. Zusammenfassend halten wir fest:

Lemma 6.10 *Seien $I \subseteq R$ ein vom Nullideal verschiedenes Polynomideal und $H = \{h_1, \ldots, h_k\} \not\ni 0$ eine Gröbnerbasis von I sowie $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ eine Zerlegung von $\mathrm{lpp}(I)$ mit der Eigenschaft $t \in \Delta_i \rightarrow \mathrm{lpp}(h_i) \mid t$ für alle $1 \leq i \leq k$ und alle $t \in T$.*

Dann existiert zu jedem $a \in R$ eine eindeutig bestimmte Lösung $(b, b_1, \ldots, b_k)$ der Gleichung $a = \sum_{i=1}^{k} b_i h_i + b$, so daß $\mathrm{lpp}(h_i) \nmid X^\mu$ und $X^\nu \, \mathrm{lpp}(h_i) \in \Delta_i$ für alle $1 \leq i \leq k$, $X^\mu \in \mathrm{supp}(b)$ sowie $X^\nu \in \mathrm{supp}(b_i)$.

Insbesondere werden durch die Vorschriften $a \mapsto b$ und $a \mapsto b_i$ auf wohldefinierte Weise lineare Operatoren $\mathrm{rem}_I : R \rightarrow R$ beziehungsweise $\mathrm{q}^{(i)}_{H,\Delta_H} : R \rightarrow R$ $(1 \leq i \leq k)$ festgelegt.

Für die anschließenden theoretischen Untersuchungen ist die konkrete Auswahl von H und Δ_H ohne Belang. Für praktische Zwecke erscheinen zwei Typen von Festsetzungen für H und Δ_H besonders erwähnenswert. Zum ersten kann man als H die reduzierte Gröbnerbasis auswählen, ihre Elemente beliebig numerieren und Δ_H rekursiv durch

$$\Delta_1 = \mathrm{lpp}(h_1) \circ T \ , \ \forall 1 < i \leq k \ : \ \Delta_i = (\mathrm{lpp}(h_i) \circ T) \setminus \bigcup_{j=1}^{i-1} \Delta_j \tag{6.9}$$

erklären. Diese Variante zeichnet sich besonders durch die kanonische Auswahl der reduzierten Gröbnerbasis aus. Eine zweite Möglichkeit besteht in der Verwendung einer reduzierten $\mathcal{D}$-involutiven Basis H und der Festsetzung der Mengen Δ_i als Mengen aller $\mathcal{D}$-Vielfachen von $\mathrm{lpp}(h_i)$ (siehe Kapitel 7). Zum einen entsteht dadurch eine weitere Abhängigkeit der Funktionen $\mathrm{q}^{(i)}_{H,\Delta_H}$, nämlich die von der partiellen Division $\mathcal{D}$. Zum anderen ergibt sich die Zerlegung Δ_H in natürlicherer Weise und experimentelle Rechnungen zu involutiven Basen nähren die Hoffnung, Effizienzvorteile gegenüber der Arbeit mit reduzierten Gröbnerbasen erzielen zu können.

Es folgt das Schlüssellemma der Division ganzer Funktionen modulo Polynomidealen.

Lemma 6.11 *Zu jeder endlichen Menge $F \subset R$ von Polynomen existiert eine komponentenweise bestimmt divergente Folge $(r_i)_{i=1,2,\ldots}$ von n-Tupeln positiver reeller Zahlen, so daß für alle $a \in R\backslash\{0\}$, $t \in T(X)$, $f \in F$ und $c \in \mathbb{C}$ mit*

$$ct \operatorname{head}(f) \in \operatorname{Mon}(a)$$

sowie alle $i = 1, 2, \ldots$ die Abschätzung

$$\|a - ctf\|_{r_i} + \|ct\|_{r_i} \leq \|a\|_{r_i} \tag{6.10}$$

erfüllt ist.

Beweis: Es existieren positive ganzzahlige Gewichte $g_1, \ldots, g_n$, so daß die Einschränkung der gemäß Beziehung (4.3) definierten gewichteten partiellen Gradordnung $\sqsubset$ auf die endliche Menge $\bigcup_{h\in F} \operatorname{supp}(h) \subset T(X)$ mit der entsprechenden Einschränkung von $\prec$ übereinstimmt (siehe [Ba82]). $\sqsubset$ hat für alle $h \in F$ die Eigenschaft, daß $\operatorname{lpp}(h)$ bezüglich $\sqsubset$ größtes Element von $\operatorname{supp}(h)$ ist. Für das Gesamtgewicht $\sum_{j=1}^{n} g_j i_j$ des Terms $t = X_1^{i_1} \cdots X_n^{i_n} \in T(X)$ führen wir die Bezeichnung $\mathrm{w}(t)$ ein. Man beachte, daß die Forderung der Übereinstimmung der Einschränkungen von $\prec$ und $\sqsubset$ auf $\bigcup_{h\in F} \operatorname{supp}(h) \subset T(X)$ aufgrund der Linearität von $\prec$ zur Folge hat, daß die Gesamtgewichte sämtlicher in F auftretenden Potenzprodukte paarweise verschieden sind. Insbesondere ist das Gesamtgewicht des führenden Potenzprodukts eines Elements $h \in F$ stets echt größer als das Gesamtgewicht eines beliebigen anderen in h vorkommenden Potenzprodukts. Wir setzen $s_i = (i^{g_1}, \ldots, i^{g_n})$. Dann existiert nach den obigen Überlegungen zu jedem Polynom $f \in F$ ein Index i_f, so daß

$$\|\operatorname{head}(f)\|_{s_i} = |\operatorname{lc}(f)| \cdot i^{\,\mathrm{w}(\operatorname{lpp}(f))} \geq \|\operatorname{tail}(f)\|_{s_i} + 1 \text{ für alle } i \geq i_f \quad . \tag{6.11}$$

Da F endlich ist, existiert das Maximum $i_0 = \max_{h\in F} i_h$. Im weiteren werden wir zeigen, daß die durch die Glieder $r_i = s_{i+i_0}$ gebildete Restfolge $(r_i)_{i=1,2,\ldots}$ den Anforderungen des Lemmas genügt. $a \in R\backslash\{0\}$, $t \in T(X)$, $f \in F$ und $c \in \mathbb{C}$ seien beliebige Elemente mit der Eigenschaft $u := ct \operatorname{head}(f) \in \operatorname{Mon}(a)$. Da die Träger von u und $a-u$ disjunkt sind, gilt für beliebige n-Tupel r positiver reeller Zahlen in der Dreiecksungleichung $\|a\|_r \leq \|u\|_r + \|a-u\|_r$ sogar die Gleichheit. Betrachten wir nun ein beliebiges festes $i \geq 1$. Einsetzen der entsprechenden Ungleichung (6.11) führt auf

$$\begin{aligned} \|a\|_{r_i} &= \|ct \operatorname{head}(f)\|_{r_i} + \|a-u\|_{r_i} \\ &= \|ct\|_{r_i} \|\operatorname{head}(f)\|_{r_i} + \|a-u\|_{r_i} \\ &\geq \|ct\|_{r_i} (\|\operatorname{tail}(f)\|_{r_i} + 1) + \|a-u\|_{r_i} \quad . \end{aligned} \tag{6.12}$$

Anwendung der Dreiecksungleichung (6.5) auf

$$a - ctf = a - ct(\operatorname{head}(f) + \operatorname{tail}(f)) = (a-u) - ct \operatorname{tail}(f)$$

und anschließendes Einsetzen von Ungleichung (6.12) ergibt

$$\begin{aligned} \|a - ctf\|_{r_i} &\leq \|a - u\|_{r_i} + \|ct \text{ tail}(f)\|_{r_i} \\ &= \|a - u\|_{r_i} + \|ct\|_{r_i} \| \text{ tail}(f)\|_{r_i} \\ &\leq \|a\|_{r_i} - \|ct\|_{r_i} \quad . \end{aligned}$$

Damit ist die Gültigkeit von Ungleichung (6.10) für alle $i = 1, 2, \ldots$ nachgewiesen. □

Folgerung 6.12 *Seien $F = \{f_1, \ldots, f_k\} \subset R$ eine endliche Polynommenge und $a, b, b_1, \ldots, b_k \in R$ Polynome mit den folgenden Eigenschaften:*

i) $\sum_{j=1}^{k} b_j f_j + b = a$,

ii) $\text{lpp}(f_j) \nmid t$ *für alle* $1 \leq j \leq k$ *und* $t \in \text{supp}(b)$,

iii) alle Terme $t \circ \text{lpp}(f_j)$ *mit* $1 \leq j \leq k$ *und* $t \in \text{supp}(b_j)$ *sind paarweise verschieden.*

Dann existiert eine komponentenweise bestimmt divergente Folge $(r_i)_{i=1,2,\ldots}$ von n-Tupeln positiver reeller Zahlen, so daß für alle $i = 1, 2, \ldots$ die Ungleichung

$$\|b\|_{r_i} + \sum_{j=1}^{k} \|b_j\|_{r_i} \leq \|a\|_{r_i} \tag{6.13}$$

gilt.

Beweis: Wir werden zeigen, daß jede Folge $(r_i)_{i=1,2,\ldots}$ von n-Tupeln positiver reeller Zahlen des in Lemma 6.11 konstruierten Typs geeignet ist.

Wir setzen $M = \{t \circ \text{lpp}(f_j) \mid 1 \leq j \leq k, t \in \text{supp}(b_j)\}$ und führen den Beweis der Aussage durch vollständige Induktion über die Mächtigkeit von M. Im Fall $M = \emptyset$ gilt $a = b$ und $b_1 = \cdots = b_k = 0$ und (6.13) ist trivialerweise erfüllt.

Sei $M \neq \emptyset$. Aus Voraussetzung *iii)* folgt die Existenz eindeutig bestimmter $1 \leq l \leq k$ und $s \in \text{supp}(b_l)$ mit $s \circ \text{lpp}(f_l) = \max_{\prec} M$. Sei $c \in \mathbb{C}$ der Koeffizient, mit dem s in b_l auftritt, mit anderen Worten $cs \in \text{Mon}(b_l)$. Wegen $s \circ \text{lpp}(f_l) \notin \text{supp}(b)$ gilt $cs \text{ head}(f_l) \in \text{Mon}(a)$. Anwendung von Lemma 6.11 ergibt

$$\|a - csf_l\|_{r_i} + \|cs\|_{r_i} \leq \|a\|_{r_i} \tag{6.14}$$

für alle $i = 1, 2, \ldots$. Auf $a - csf_l = b + \sum_{j=1}^{k} b'_j f_j$ mit $b'_j = b_j$ für alle $j \neq l$ und $b'_l = b_l - cs$ ist die Induktionsvoraussetzung anwendbar, also

$$\|b\|_{r_i} + \sum_{j=1}^{k} \|b'_j\|_{r_i} \leq \|a - csf_l\|_{r_i} \quad . \tag{6.15}$$

Mit Hilfe von (6.15) und (6.14) gelangt man zu der behaupteten Normabschätzung

$$\begin{aligned} \|b\|_{r_i} + \sum_{j=1}^{k} \|b_j\|_{r_i} &= \|b\|_{r_i} + \sum_{j=1}^{k} \|b'_j\|_{r_i} + \|cs\|_{r_i} \\ &\leq \|a - csf_l\|_{r_i} + \|cs\|_{r_i} \\ &\leq \|a\|_{r_i} \quad \text{für alle } i = 1, 2, \ldots \quad . \end{aligned}$$

□

Folgerung 6.13 *Sei* $\{0\} \subsetneq I \subseteq R$ *ein Polynomideal,* $H = \{h_1, \ldots, h_k\}$ *eine nicht das Nullpolynom enthaltende Gröbnerbasis von* I *und* $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ *eine zugehörige Zerlegung des Monoidideals* $\mathrm{lpp}(I)$.

Dann existiert eine komponentenweise bestimmt divergente Folge $(r_i)_{i=1,2,\ldots}$ *von* n*-Tupeln positiver reeller Zahlen, so daß für alle* $i = 1, 2, \ldots$ *und alle* $a \in R$ *die Ungleichungen*

$$\| \mathrm{rem}_I(a)\|_{r_i} + \sum_{j=1}^{k} \| \mathrm{q}^{(j)}_{H,\Delta_H}(a)\|_{r_i} \leq \|a\|_{r_i} \tag{6.16}$$

$$\| \mathrm{rem}_I(a)\|_{r_i} \leq \|a\|_{r_i} \tag{6.17}$$

$$\| \mathrm{q}^{(j)}_{H,\Delta_H}(a)\|_{r_i} \leq \|a\|_{r_i} \quad (j = 1, \ldots, k) \tag{6.18}$$

gelten.

Beweis: Bei (6.16) handelt es sich um einen Spezialfall von (6.13). Die Ungleichungen (6.17) und (6.18) sind triviale Folgerungen aus (6.16). □

Damit sind die vorbereitenden Untersuchungen auf dem Unterring der Polynome abgeschlossen und wir wenden uns der Konstruktion einer Divisionsformel ganzer Funktionen zu.

Definition 6.14 *Sei* $\{0\} \subsetneq I \subseteq R$ *ein Polynomideal,* $H = \{h_1, \ldots, h_k\}$ *eine nicht das Nullpolynom enthaltende Gröbnerbasis von* I *und* $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ *eine zugehörige Zerlegung des Monoidideals* $\mathrm{lpp}(I)$. *Dann werden die Operatoren* rem_I *und* $\mathrm{q}^{(j)}_{H,\Delta_H}$ $(j = 1, \ldots, k)$ *vermöge*

$$\mathrm{rem}_{IE}\left(\sum_{t\in T(X)} \beta_t t\right) := \sum_{t\in T(X)} \beta_t \, \mathrm{rem}_I(t)$$

$$\mathrm{q}^{(j)}_{HE,\Delta_H}\left(\sum_{t\in T(X)} \beta_t t\right) := \sum_{t\in T(X)} \beta_t \, \mathrm{q}^{(j)}_{H,\Delta_H}(t)$$

linear auf den Bereich E *der ganzen Funktionen fortgesetzt.*

Es erheben sich zwei Fragen, erstens nach der Wohldefiniertheit der obigen Fortsetzungen und zweitens inwieweit sie Anlaß zu einer Divisionsformel geben. Die entsprechenden Ergebnisse sind in dem folgenden Satz zusammengefaßt.

Satz 6.15 *Sei* $\{0\} \subsetneq I \subseteq R$ *ein Polynomideal,* $H = \{h_1, \ldots, h_k\}$ *eine nicht das Nullpolynom enthaltende Gröbnerbasis von* I *und* $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ *eine zugehörige Zerlegung des Monoidideals* $\mathrm{lpp}(I)$. $\mathcal{D}$ *bezeichne die Menge* $T(X)\setminus \mathrm{lpp}(I) = \{t \in T(X) \mid \mathrm{lpp}(h_1) \nmid t, \ldots, \mathrm{lpp}(h_k) \nmid t\}$ *aller Potenzprodukte, die in keinem Element von* I *führend sind. Weiterhin bezeichne* $E(\mathcal{D})$ *den linearen Unterraum aller ganzen Funktionen, deren Träger in* $\mathcal{D}$ *enthalten ist. Dann gelten folgende Beziehungen:*

i) die Operatoren rem_{IE} *und* $\mathrm{q}^{(j)}_{HE,\Delta_H}$, $j = 1, \ldots, k$, *sind auf ganz* E *wohldefiniert und stetig,*

ii) $im(\ \mathrm{rem}_{IE}) \subseteq E(\mathcal{D})$,

iii) $\forall a \in E\ :\ a = \sum_{j=1}^{k}\ \mathrm{q}^{(j)}_{HE,\Delta_H}(a)h_j + \ \mathrm{rem}_{IE}(a)$,

iv) $\mathrm{rem}_{IE}(a) = 0 \Longleftrightarrow a \in IE$,

v) $(a + IE) \cap E(\mathcal{D}) = \{\mathrm{rem}_{IE}(a)\}$.

Beweis: $(r_i)_{i=1,2,\ldots}$ sei eine bestimmt divergente Folge von n-Tupeln positiver reeller Zahlen des in Lemma 6.11 konstruierten Typs.
i) Aus (6.17) ergibt sich $\| \mathrm{rem}_I(t)\|_{r_i} \leq \|t\|_{r_i}$ für alle $t \in T(X)$ und $i = 1, 2, \ldots$. Sei $a = \sum_{t\in T(X)} \beta_t t$ eine beliebige ganze Funktion. Für alle $i = 1, 2, \ldots$ haben wir

$$\sum_{t\in T(X)} \| \mathrm{rem}_I(\beta_t t)\|_{r_i} = \sum_{t\in T(X)} |\beta_t|\ \| \mathrm{rem}_I(t)\|_{r_i} \leq \sum_{t\in T(X)} |\beta_t|\ \|t\|_{r_i} = \|a\|_{r_i} < \infty.$$

Mit Lemma 6.9 folgt schließlich

$$\mathrm{rem}_{IE}(a) = \sum_{t\in T(X)} \beta_t\ \mathrm{rem}_I(t) = \sum_{t\in T(X)} \mathrm{rem}_I(\beta_t t) \in E$$

und somit die Wohldefiniertheit von rem_{IE} auf ganz E. Weiterhin leitet man aus den obigen Ungleichungen und der Dreiecksungleichung die Gültigkeit von

$$\| \mathrm{rem}_{IE}(a)\|_{r_i} \leq \sum_{t\in T(X)} \| \mathrm{rem}_I(\beta_t t)\|_{r_i} \leq \|a\|_{r_i} \tag{6.19}$$

für alle $i = 1, 2, \ldots$ ab. Unter Berücksichtigung seiner Linearität folgt die Stetigkeit des Operators rem_{IE}.

Auf die gleiche Weise zeigt man mit Hilfe von (6.18) die Wohldefiniertheit und die Stetigkeit der Operatoren $\mathrm{q}^{(1)}_{HE,\Delta_H}, \ldots,\ \mathrm{q}^{(k)}_{HE,\Delta_H}$. Ebenso gilt für alle $j = 1, \ldots, k$ die Ungleichung

$$\| \mathrm{q}^{(j)}_{HE,\Delta_H}(a)\|_{r_i} \leq \sum_{t\in T(X)} \| \mathrm{q}^{(j)}_{H,\Delta_H}(\beta_t t)\|_{r_i} \leq \|a\|_{r_i} \tag{6.20}$$

ii) Wegen $\mathrm{rem}_I(t) \in E(D)$ für alle $t \in T(X)$ liefert Lemma 6.9 nicht nur $\mathrm{rem}_{IE}(a) \in E$, sondern sogar $\mathrm{rem}_{IE}(a) \in E(D)$.
iii) Sei $a = \sum_{t\in T(X)} \beta_t t \in E$ eine beliebige ganze Funktion. Die unter *i)* gezeigten Konvergenzen von Reihen ganzer Funktionen sichern die Zulässigkeit der folgenden Umformungen ab:

$$\begin{aligned}
\sum_{j=1}^{k} \mathrm{q}^{(j)}_{HE,\Delta_H}(a)h_j + \ \mathrm{rem}_{IE}(a) \quad &= \\
\sum_{j=1}^{k} \left(\sum_{t\in T(X)} \beta_t\ \mathrm{q}^{(j)}_{H,\Delta_H}(t) \right) h_j + \sum_{t\in T(X)} \beta_t\ \mathrm{rem}_I(t) \quad &= \\
\sum_{t\in T(X)} \beta_t \left(\sum_{j=1}^{k} \mathrm{q}^{(j)}_{H,\Delta_H}(t)h_j + \ \mathrm{rem}_I(t) \right) \quad &= \quad a \quad .
\end{aligned}$$

iv) Als triviale Konsequenz aus *iii)* ergibt sich $a \in IE$ für alle $a \in E$ mit $\mathrm{rem}_{IE}(a) = 0$.

Jedes Element a von IE ist Grenzwert einer Cauchy-Folge von Polynomen $g_l \in I$, $l = 1, 2, \ldots$. Aufgrund der Stetigkeit von rem_{IE} haben wir

$$\mathrm{rem}_{IE}(a) = \lim_{l\to\infty} \mathrm{rem}_{IE}(g_l) = \lim_{l\to\infty} \mathrm{rem}_I(g_l) = \lim_{l\to\infty} 0 = 0$$

und somit ist auch die Umkehrung $\mathrm{rem}_{IE}(a) = 0$ für alle $a \in IE$ nachgewiesen.

v) Aus *ii)* und *iii)* folgt $\mathrm{rem}_{IE}(a) \in (a + IE) \cap E(\mathcal{D})$. Sei $\hat{a} \in (a + IE) \cap E(\mathcal{D})$ beliebig. Wegen $\mathrm{supp}(\mathrm{rem}_{IE}(a) - \hat{a}) \subseteq \mathcal{D}$, also $\mathrm{rem}_I(t) = t$ für alle $t \in \mathrm{supp}(\mathrm{rem}_{IE}(a) - \hat{a})$, liegt die Gleichheit $\mathrm{rem}_{IE}(\mathrm{rem}_{IE}(a) - \hat{a}) = \mathrm{rem}_{IE}(a) - \hat{a}$ vor. Mittels *iv)* erhält man $\mathrm{rem}_{IE}(\mathrm{rem}_{IE}(a) - \hat{a}) = \mathrm{rem}_{IE}(a) - \hat{a} = 0$ und ist fertig. □

6.2.3 Approximationen

Die in Satz 6.15 dargestellten Resultate sind weitgehend von existentieller Natur. Dem Anliegen der vorliegenden Arbeit entsprechend, wenden wir uns nun der konstruktiven Seite der unter *iii)* angegebenen Divisionsformel zu. Genauer gesagt beschäftigen wir uns mit der Beantwortung der folgenden Frage: Angenommen, H ist Teilmenge eines effektiven Polynomrings $R' = \mathbb{K}[X] \subset R \subset E$, wie können dann die ganzen Funktionen $\mathrm{rem}_{IE}(a)$ und $\mathrm{q}^{(j)}_{HE,\Delta_H}(a)$ durch Polynome aus R' in vorgegebener Genauigkeit approximiert werden? Die Effektivität von R' ist gleichbedeutend mit der Effektivität des Koeffizientenkörpers $\mathbb{K} \subset \mathbb{C}$. Die Einschränkungen der Funktionen rem_{IE} und $\mathrm{q}^{(j)}_{HE,\Delta}$ auf den effektiven Unterring R' sind berechenbar. Adjunktion der imaginären Einheit zu einem beliebigen effektiven Körper $\mathbb{K} \subset \mathbb{C}$ führt stets wieder auf einen effektiven Körper. Daher können wir ohne Beschränkung der Allgemeinheit annehmen, daß $\mathbb{K}$ die imaginäre Einheit enthält. Dann existiert zu jeder ganzen Funktion a eine lokal gleichförmig gegen a konvergierende Folge von Polynomen aus R'. Unter Berücksichtigung der Stetigkeit der Operatoren läßt sich die Approximation von $\mathrm{rem}_{IE}(a)$ und $\mathrm{q}^{(j)}_{HE,\Delta}(a)$ in vorgegebener Genauigkeit somit auf die Konstuierbarkeit einer "genügend genauen" Approximation $\hat{a} \in R'$ von a reduzieren. Dem Funktionscharakter der Elemente $\mathrm{rem}_{IE}(a)$ und $\mathrm{q}^{(j)}_{HE,\Delta_H}(a)$ Rechnung tragend, stellt sich darüberhinaus die Frage nach der näherungsweisen Berechnung eines Funktionswertes an einer vorgegebenen Stelle $(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$. Da die Funktionswerte der Operatoren $\mathrm{q}^{(j)}_{HE,\Delta_H}(a)$ geometrisch uninteressant sind, werden wir uns in Bezug auf dieses Problem auf die Berechnung von Näherungen für $\mathrm{rem}_{IE}(a)(\alpha_1, \ldots, \alpha_n)$ beschränken.

Approximation von Quotienten und Divisionsrest

Um die Güte einer Näherung $\hat{a}$ von a quantitativ beziffern zu können, bedarf es einer Abschwächung der Topologie von E, so daß E mit der schwächeren Topologie einen metrischen Raum bildet. Dazu bieten sich zwei Alternativen an. Zum ersten fixiert man ein n-Tupel $r \in \mathbb{R}^n_+$ und verwendet den auf der

Relativtopologie der Banachtopologie von B_r basierenden Abstand

$$\mathrm{d}_r(\hat{a}, a) = \|\hat{a} - a\|_r \quad .$$

Zum zweiten kann die auf der Topologie der koeffizientenweisen Konvergenz aufbauende Abstandsdefinition

$$\mathrm{d}_{koeff}(\hat{a}, a) = \max_{t \in T(X)} |\beta_t| \quad , \text{ wobei } \hat{a} - a = \sum_{t \in T(X)} \beta_t t \quad ,$$

angewandt werden. Da jede Teilfolge $\beta_{t_1}, \beta_{t_2}, \ldots$ von Koeffizienten von $\hat{a} - a$ mit $t_1 \mid t_2 \mid \cdots$ gegen Null konvergiert, ist die Existenz des Maximums der Menge der Absolutbeträge der Koeffizienten von $\hat{a} - a$ in jedem Fall gesichert.

Der Abstandsbegriff ist umso geeigneter, je weniger stark die Topologie der lokalen gleichmäßigen Konvergenz abgeschwächt werden muß. Für n-Tupel $\mathbb{R}_+^n \ni r < s \in \mathbb{R}_+^n$ ist die von der Banachalgebra B_s induzierte Relativtopologie auf E mindestens so stark, wie die von B_r induzierte. Aus diesem Grund sind n-Tupel $r = (\rho_1, \ldots, \rho_n)$ mit sehr großen Koordinaten, genauer sehr großem $\min\{\rho_1, \ldots, \rho_n\}$, besonders günstig. Die Topologie der koeffizientenweisen Konvergenz ist für alle n-Tupel $r = (\rho_1, \ldots, \rho_n) \in \mathbb{R}_+^n$ schwächer als die Relativtopologie der Banachtopologie von B_r und falls $\rho_1, \ldots, \rho_n \geq 1$, so gilt offensichtlich sogar für alle $a, \hat{a} \in E$ die Ungleichung

$$\mathrm{d}_{koeff}(\hat{a}, a) \leq \mathrm{d}_r(\hat{a}, a) \quad . \tag{6.21}$$

Satz 6.16 *Seien $\{0\} \subsetneqq I \subseteq R$ ein Polynomideal, $H = \{h_1, \ldots, h_k\}$ eine nicht das Nullpolynom enthaltende Gröbnerbasis von I und Δ_H eine zugehörige Zerlegung des Monoidideals $\mathrm{lpp}(I)$. Weiterhin seien $g_1, \ldots, g_n$ positive ganze Zahlen, welche eine gewichtete partielle Gradordnung $\sqsubset$ definieren, deren Einschränkung auf $\bigcup_{i=1}^k \mathrm{supp}(h_i) \subset T(X)$ mit der von $\prec$ übereinstimmt. $\kappa \geq 1$ sei eine reelle Zahl mit der Eigenschaft, daß für alle $j = 1, \ldots, k$ die Ungleichung $\|\mathrm{head}(h_j)\|_{r_\kappa} \geq \|\mathrm{tail}(h_j)\|_{r_\kappa} + 1$, wobei r_κ das n-Tupel $(\kappa^{g_1}, \ldots, \kappa^{g_n})$ bezeichnet, erfüllt ist. Weiterhin seien $r = (\rho_1, \ldots, \rho_n)$ ein beliebiges n-Tupel positiver reeller Zahlen und $\psi \geq \kappa$ eine reelle Zahl mit $\rho_j \leq \psi^{g_j}$ für alle $j = 1, \ldots, n$. r_ψ bezeichne das n-Tupel $(\psi^{g_1}, \ldots, \psi^{g_n})$. Schließlich sei* op *einer der Operatoren* $\mathrm{q}^{(1)}_{HE,\Delta_H}, \ldots, \mathrm{q}^{(k)}_{HE,\Delta_H}$ *oder* rem_{IE}. *Dann gelten für alle ganzen Funktionen a und b die Beziehungen*

$$\mathrm{d}_{koeff}(\mathrm{op}(a), \mathrm{op}(b)) \leq \mathrm{d}_{r_\kappa}(\mathrm{op}(a), \mathrm{op}(b)) = \|\mathrm{op}(a - b)\|_{r_\kappa} \leq \|a - b\|_{r_\kappa} \tag{6.22}$$

und

$$\mathrm{d}_r(\mathrm{op}(a), \mathrm{op}(b)) \leq \mathrm{d}_{r_\psi}(\mathrm{op}(a), \mathrm{op}(b)) = \|\mathrm{op}(a - b)\|_{r_\psi} \leq \|a - b\|_{r_\psi} \quad . \tag{6.23}$$

Beweis: Zu (6.22): Die linke Ungleichung folgt aus $\kappa \geq 1$ und (6.21). Die Gleichheit ergibt sich aus der Abstandsdefinition und der Linearität des Operators op. Schließlich erhält man aus (6.19) beziehungsweise (6.20) die rechte Ungleichung.
Zu (6.23): Die linke Ungleichung folgt unmittelbar aus Voraussetzung $\rho_j \leq \psi^{g_j}$ und die rechte aus $\kappa \leq \psi$. □

Satz 6.16 zeigt einen Weg auf, wie die Beantwortung der Frage, welche Terme einer beständig konvergenten Potenzreihe a zum Zwecke der Division in vorgegebener Genauigkeit abgeschnitten werden dürfen, auf die näherungsweise Berechnung gewöhnlicher komplexer Reihen reduziert werden kann.

Die folgende Berechnungsvorschrift beschreibt einen näherungsweisen Divisionsalgorithmus. Dabei setzen wir voraus, daß die Koeffizienten aller Eingabedaten einem effektiven Unterkörper $\mathbb{K}$ der komplexen Zahlen angehören und daß es sich bei der von $\mathfrak{R}$ auf $R' = \mathbb{K}[X]$ induzierten graduierten Struktur $\mathfrak{R}' = (R', T(X), \prec, \mathrm{lpp})$ um eine effektive Gröbnerstruktur handelt. Für die Menge der zu $\mathbb{K}$ gehörigen, positiven reellen Zahlen vereinbaren wir die Symbolik $\mathbb{K}_+$. Weiterhin bezeichnet $\#(\mathrm{supp}(h))$ die Mächtigkeit des Trägers, also die Anzahl der Terme, eines Polynoms.

Aufruf: $(a_1, \ldots, a_k, \hat{a}) := \textsc{Divide}_{E,\mathfrak{R}'}(a, F, \epsilon, r)$
Eingaben: $F = \{f_1, \ldots, f_m\}$ Erzeugendensystem des Ideals $I \subseteq R'$,
$a = \sum_{t \in T(X)} \beta_t t \in \mathbb{K}[[X]] \cap E$, $\epsilon \in \mathbb{K}_+$, $r = (\rho_1, \ldots, \rho_n) \in \mathbb{K}_+^n$
Ausgaben: $a_1, \ldots, a_k, \hat{a} \in R'$ mit

$$\mathrm{d}_r\left(\hat{a},\ \mathrm{rem}_{IE}(a)\right) < \epsilon \text{ und } \mathrm{d}_r\left(a_j,\ \mathrm{q}^{(j)}_{HE,\Delta_H}(a)\right) < \epsilon\ (1 \leq j \leq k) \quad ,$$

wobei $H = \{h_1, \ldots, h_k\}$ die reduzierte Gröbnerbasis von I bezüglich $\mathfrak{R}'$ und Δ_H die in (6.9) definierte Zerlegung von $\mathrm{lpp}(I)$ sind.

Berechne die reduzierte Gröbnerbasis $H = \{h_1, \ldots, h_k\}$ von I bezüglich $\mathfrak{R}'$

Berechne positive ganzzahlige Gewichte $g_1, \ldots, g_n$, so daß die davon definierte gewichtete Gradordnung $\sqsubset$ auf $\bigcup_{j=1}^k \mathrm{supp}(h_j)$ mit $\prec$ übereinstimmt.

$\omega := \max\left\{|c| \mid \exists t \in T(X) : ct \in \bigcup_{j=1}^k \mathrm{Mon}(h_j)\right\}$

$\lambda := \max_{j=1}^k \#(\mathrm{supp}(h_j))$

Berechne das minimale ganzzahlige $\psi \geq \omega\lambda$ mit $\rho_j \leq \psi^{g_j}$ für alle $j = 1, \ldots, n$

$r_\psi := (\psi^{g_1}, \ldots, \psi^{g_n})$

Berechne ein $\alpha \in \mathbb{K}_+$ mit $|\alpha - \|a\|_{r_\psi}| < \frac{\epsilon}{2}$

$\beta := 0$, $b := 0$, $l := 0$

while $|\alpha - \beta| \geq \frac{\epsilon}{2}$ **do**

$\beta := \beta + \sum_{\mathrm{w}(t)=l} |\beta_t| \psi^l$

$b := b + \sum_{\mathrm{w}(t)=l} \beta_t t$

$l := l + 1$

$(a_1, \ldots, a_k, \hat{a}) := \textsc{Divide}_{R'}(b, H)$

return$(a_1, \ldots, a_k, \hat{a})$

Die gerufene Funktion $\text{DIVIDE}_{R'}$ ist eine Instanz des in Abschnitt 5.2 eingeführten Divisionsalgorithmus DIVIDE_R, angewandt auf die graduierte Struktur $\mathfrak{R}'$ und ausgestattet mit einer Unterfunktion DIVIDE_G, welche die Gültigkeit der Forderung (6.7) absichert.

Die Korrektheit der Vorschrift folgt nahezu unmittelbar aus Ungleichung (6.23) von Satz 6.16. Wir beschränken uns auf einige zusätzliche Erklärungen ausgewählter Stellen. $\kappa = \omega\lambda$ ist eine positive reelle Zahl größer oder gleich 1 und eine einfache Abschätzung bestätigt für alle $j = 1, \ldots, k$ die Gültigkeit von $\|\text{head}(h_j)\|_{r_\kappa} \geq \|\text{tail}(h_j)\|_{r_\kappa} + 1$, wobei $r_\kappa = (\kappa^{g_1}, \ldots, \kappa^{g_n})$. Somit genügen κ, ψ und r den Voraussetzungen von Satz 6.16 und es gilt Ungleichung (6.23). Schließlich verbleibt noch der Nachweis von $\|a - b\|_{r_\psi} < \epsilon$. Nach Konstruktion haben b und $a - b$ vor jedem Durchlauf der **while**-Schleife die Gestalt $b = \sum_{\text{w}(t)<l} \beta_t t$ beziehungsweise $a - b = \sum_{\text{w}(t)\geq l} \beta_t t$. Aufgrund der Disjunktheit der Träger von b und $a - b$ sind die Normen von b und $a - b$ additiv. Es folgt $\|a\|_{r_\psi} = \|(a - b) + b\|_{r_\psi} = \|a - b\|_{r_\psi} + \|b\|_{r_\psi} = \|a - b\|_{r_\psi} + \beta$. Somit $\|a - b\|_{r_\psi} = \|a\|_{r_\psi} - \beta = (\|a\|_{r_\psi} - \alpha) + (\alpha - \beta) = |(\|a\|_{r_\psi} - \alpha) + (\alpha - \beta)| \leq |\|a\|_{r_\psi} - \alpha| + |\alpha - \beta| < \epsilon$. Die obigen Schlußfolgerungen basieren wesentlich darauf, daß die β_t die exakten Koeffizienten der ganzen Funktion a sind, denn gingen nur genäherte Koeffizienten in die Konstruktion von b ein, so wären die Träger von a und $a - b$ nicht disjunkt und es gelänge im allgemeinen nicht, die Norm von $a - b$ nach oben abzuschätzen.

Da alle Komponenten von ψ größer oder gleich 1 sind, ist ϵ gleichzeitig obere Schranke für die betragsmäßige Abweichung der Koeffizienten der ganzen Funktionen $\text{q}^{(1)}_{HE,\Delta_H}, \ldots, \text{q}^{(k)}_{HE,\Delta_H}$ und $\text{rem}_{IE}(a)$.

Wenden wir uns nun dem Terminationsverhalten der Berechnungsvorschrift zu. Der Unterring $A = \mathbb{K}[[X]] \cap E$ ist überabzählbar, daher ist bestenfalls eine Einschränkung der Funktion $\text{DIVIDE}_{E,\mathfrak{R}'}$ auf eine gödelisierbare Teilmenge $A' \subsetneq A$ berechenbar. Die Elemente $a \in A'$ müssen so beschaffen sein, daß zu einem beliebig vorgegebenem Potenzprodukt $t \in T(X)$ der zugehörige Koeffizient β_t von a berechnet werden kann. Im wesentlichen bedeutet diese Forderung die Berechenbarkeit des Polynoms $\sum_{\text{w}(t)<l} \beta_t t$ zu beliebig vorgegebenem Gesamtgewicht l. Betrachten wir also die Berechenbarkeit der Einschränkung auf eine derartige Menge A'. Mit Ausnahme der Berechnung des Wertes α sind dann alle Schritte der Vorschrift berechenbar. Wenn α berechnet werden kann, so bricht auch die anschließende Abbarbeitung der **while**-Schleife nach endlich vielen Schritten ab. Die Berechnung von α entspricht der Approximation der Summe der gewöhnlichen komplexen Reihe $\sum_{l=0}^{\infty}(\sum_{\text{w}(t)=l} |\beta_t|)\psi^l$ und ist der numerischen Mathematik zuzurechnen. Auf Bedingungen und Methoden seiner Lösung soll hier nicht eingegangen werden.

Alternativ zur Berechenbarkeitsuntersuchung der Einschränkung der Funktion $\text{DIVIDE}_{E,\mathfrak{R}'}$ auf eine gödelisierbare Menge A' kann auch ihre relative Berechenbarkeit bezüglich einer Funktion $\mu : E \times \mathbb{K}_+ \to \mathbb{K}[X]$ mit $\text{d}_{r_\psi}(a, \mu(a, \epsilon)) < \epsilon$ betrachtet werden. Auf dieser Grundlage könnte das gesamte Programmfragment

Berechne ein $\alpha \in \mathbb{K}_+$ mit $|\alpha - \|a\|_{r_\psi}| < \frac{\epsilon}{2}$
$\beta := 0$, $b := 0$, $l := 0$

while $|\alpha - \beta| \geq \frac{\epsilon}{2}$ **do**

$\beta := \beta + \sum_{\mathrm{w}(t)=l} |\beta_t| \psi^l$

$b := b + \sum_{\mathrm{w}(t)=l} \beta_t t$

$l := l + 1$

einfach durch

$b := \mu(a, \epsilon)$

ersetzt und die Eingabespezifikation $a \in \mathbb{K}[[X]] \cap E$ zu $a \in E$ abgeschwächt werden. Während die erstgewählte Variante durchsichtiger ist und bereits gewisse Teillösungen der Berechenbarkeit von μ umfaßt, hinterläßt die zweite Variante die größere Berechenbarkeitslücke, stellt aber gleichzeitig den allgemeineren Zugang dar.

Bei den in Abschnitt 6.1 durchgeführten Untersuchungen in der Krullschen Topologie reichte zur näherungsweisen Berechnung der Bestandteile einer Divisionsformel bereits die Eingabe von Näherungen der Elemente des Erzeugendensystems F in der gewünschten Genauigkeit aus. Dieser Sachverhalt beruht auf der Stetigkeit der Quotienten und des Restes bei Division von $a \in S$ modulo $I \subseteq S$ in a und den Elementen des Erzeugendensystems F von I. Es erhebt sich die Frage, ob eine ähnliche Stetigkeit auch im Ring der ganzen Funktionen vorliegt. Zu beliebigen $h_1, h_2 \in \mathbb{C}\{\{X_1\}\}$ und beliebiger reeller Zahl $\epsilon > 0$ existieren Polynome $\widetilde{h_1}, \widetilde{h_2} \in \mathbb{C}[X_1]$ mit $\mathrm{d}_{koeff}(h_1, \widetilde{h_1}) < \epsilon$ und $\mathrm{d}_{koeff}(h_2, \widetilde{h_2}) < \epsilon$ sowie $ggT(\widetilde{h_1}, \widetilde{h_2}) = 1$. Mehr noch, es gibt Folgen von Polynomen, die in der Topologie der lokalen gleichmäßigen Konvergenz gegen h_1 beziehungsweise h_2 konvergieren, so daß die beiden Polynome mit gleichem Index jeweils teilerfremd sind. Somit läßt jede ganze Funktion bei Division modulo eines in E von zwei Polynomen mit gleichem Index erzeugten Ideals den Rest 0. Haben jedoch h_1 und h_2 eine gemeinsame Nullstelle, dann gibt es eine nicht dem Ideal $(h_1, h_2)\mathbb{C}\{\{X_1\}\}$ angehörige ganze Funktion a und diese kann bei Division modulo $(h_1, h_2)\mathbb{C}\{\{X_1\}\}$ nicht den Rest 0 lassen. Folglich sind die Operatoren rem_{IE} und $\mathrm{q}^{(j)}_{HE,\Delta_H}$ nicht in den Elementen der reduzierten Gröbnerbasis H und erst recht nicht in den Elementen des Erzeugendensystems F stetig. Daher kann weder von der Forderung der exakten Vorgabe der Elemente von F abgerückt werden, noch ist eine stetige Fortsetzung der Operatoren rem_{IE} und $\mathrm{q}^{(j)}_{HE,\Delta_H}$ auf nicht von Polynomen erzeugte Ideale von E möglich.

Man beachte einen wesentlichen Unterschied zur Forderung der genauen Vorgabe der Koeffizienten von a. Die Operatoren rem_{IE} und $\mathrm{q}^{(j)}_{HE,\Delta_H}$ sind in a stetig, das heißt kleine Störungen an den Koeffizienten von a führen zu kleinen Störungen an den Koeffizienten von $\mathrm{rem}_{IE}(a)$ beziehungsweise $\mathrm{q}^{(j)}_{HE,\Delta_H}(a)$. Das Problem besteht nur im Treffen quantitativer Aussagen über die Größe der Abweichung von der exakten Lösung. Dagegen kann bei kleinsten Störungen der Koeffizienten des Erzeugendensystem F nicht einmal eine qualitative Aussage über den Abstand zur exakten Lösung getroffen werden.

Approximation von Funktionswerten des Divisionsrests

Wenden wir uns jetzt der Frage nach der näherungsweisen Berechnung des Funktionswertes der ganzen Funktion $\mathrm{rem}_{IE}(a)$ an einer Stelle $(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ zu. Wir werden die Lösung dieses Problems auf die im vorangegangenen Abschnitt beschriebene Approximation von Divisionsresten zurückführen.

Für $\alpha_1 = \cdots = \alpha_n = 0$ ist der Funktionswert $\mathrm{rem}_{IE}(a)(0, \ldots, 0)$ gleich dem Absolutglied der ganzen Funktion $\mathrm{rem}_{IE}(a)$. Mittels $\textsc{Divide}_{E,\mathfrak{R}'}$ kann ein Polynom bestimmt werden, dessen Koeffizienten, also insbesondere auch das Absolutglied, betragsmäßig um höchstens ϵ von den entsprechenden Koeffizienten von $\mathrm{rem}_{IE}(a)$ abweichen. Darüberhinaus läßt sich die Berechnung des Funktionswertes $\mathrm{rem}_{IE}(a)(\alpha)$ an einer beliebigen Stelle $\alpha = (\alpha_1, \ldots, \alpha_n)$ durch Entwicklung von $\mathrm{rem}_{IE}(a)$ an der Stelle α auf eine Funktionswertberechnung im Nullpunkt reduzieren.

Die Potenzreihenentwicklung der ganzen Funktion $\mathrm{rem}_{IE}(a)$ an der Stelle α erhält man, indem man $\mathrm{rem}_{IE}(a)$ dem durch $X_i \mapsto X_i - \alpha_i$, $i = 1, \ldots, n$, definierten Automorphismus $\iota_\alpha : E \to E$ unterwirft. Die Vorgabe eines Polynoms h mit $\mathrm{d}_{koeff}(\mathrm{rem}_{IE}(a), h) < \epsilon$ läßt im allgemeinen keine Aussage über die Größe des Abstands $\mathrm{d}_{koeff}\left(\iota_\alpha\left(\mathrm{rem}_{IE}(a)\right), \iota_\alpha(h)\right)$ zu. Um die vorbereitende Approximation von $\mathrm{rem}_{IE}(a)$ zu umgehen, bliebe die Möglichkeit, den Automorphismus vor der Division auf das Ideal IE und die ganze Funktion a anzuwenden. Allerdings bereitet die Transformation von a Schwierigkeiten. So ist es im allgemeinen unmöglich, die exakten Koeffizienten von $\iota_\alpha(a)$ zu bestimmen und die Eingabespezifikationen der Berechnungsvorschrift $\textsc{Divide}_{E,\mathfrak{R}'}$ sind nicht erfüllt.

Wir führen einen zweiten Satz von Variablen $Y = \{Y_1, \ldots, Y_n\}$ ein und bilden die Polynomringe $R_Y = \mathbb{C}[Y]$ und $R_{X,Y} = \mathbb{C}[X, Y] \cong R[Y]$ sowie die Ringe $E_Y = \mathbb{C}\{\{Y\}\}$ und $E_{X,Y} = \mathbb{C}\{\{X, Y\}\}$ der ganzen Funktionen in den Variablen $Y_1, \ldots, Y_n$ beziehungsweise $X_1, \ldots, X_n, Y_1, \ldots, Y_n$. Die Monoide $T(X)$ und $T(Y)$ sind vermöge $X_i \mapsto Y_i$ in natürlicher Weise zueinander isomorph. $\prec_Y$ sei die von der Monoidordnung $\prec$ von $T(X)$ auf $T(Y)$ induzierte Monoidordnung, das heißt die Monoidordnung, bei welcher der obige Isomorphismus auch Isomorphismus der geordneten Monoide $(T(X), \prec)$ und $(T(Y), \prec_Y)$ ist. Wir betrachten $T(X)$ und $T(Y)$ als Untermonoide von $T(X, Y)$ und definieren auf $T(X, Y)$ eine Eliminationsordnung $\prec_{X,Y}$, deren Einschränkungen auf $T(X)$ mit $\prec$ und auf $T(Y)$ mit $\prec_Y$ übereinstimmen. Unter einer Eliminationsordnung verstehen wir dabei eine Monoidwohlordnung $\prec_{X,Y}$ von $T(X, Y)$ mit der Eigenschaft $t \prec_{X,Y} s$ für alle $t \in T(Y)$ und $s \notin T(Y)$. Wir ordnen den Polynomringen R_Y und $R_{X,Y}$ die graduierten Strukturen $\mathfrak{R}_Y = (R_Y, T(Y), \prec_Y, \mathrm{lpp})$ beziehungsweise $\mathfrak{R}_{X,Y} = (R_{X,Y}, T(X, Y), \prec_{X,Y}, \mathrm{lpp})$ zu. Sei J das von der Menge

$$F = \{X_1 - Y_1 + \alpha_1, \ldots, X_n - Y_n + \alpha_n\} \tag{6.24}$$

in $R_{X,Y}$ erzeugte Polynomideal. Man sieht leicht, daß es sich bei F um die reduzierte Gröbnerbasis von J bezüglich der graduierten Struktur $\mathfrak{R}_{X,Y}$ handelt. Vermöge der Abbildungsvorschrift $X_i \mapsto Y_i - \alpha_i$, $(i = 1, \ldots, n)$, wird ein Isomorphismus $\tau_\alpha : E \to E_Y$ definiert. Unter Berücksichtigung der Isomorphie der geordneten Wertemonoide von $\mathfrak{R}$ und $\mathfrak{R}_Y$ ergibt sich, daß für alle von Null

verschiedenen Polynome $g \in R$ die Gleichheit

$$\mathrm{lpp}\,(\tau_\alpha(\mathrm{head}(g))) = \mathrm{lpp}(\tau_\alpha(g)) \tag{6.25}$$

vorliegt. Bei natürlicher Einbettung von E_Y in $E_{X,Y}$ ergibt sich die Gleichheit

$$g(\alpha) = \tau_\alpha(g)(0,\ldots,0) = \mathrm{rem}_{JE_{X,Y}}(g)(0,\ldots,0) \quad . \tag{6.26}$$

Lemma 6.17 *Sei $I \subseteq R$ ein Ideal und H eine Gröbnerbasis von I bezüglich der graduierten Struktur $\mathfrak{R}$. Dann ist $\tau_\alpha(H) = \{\tau_\alpha(h) \mid h \in H\}$ eine Gröbnerbasis des Bildes $\tau_\alpha(I)$ von I unter dem Isomorphismus τ_α bezüglich der graduierten Struktur $\mathfrak{R}_Y$. Ist H reduzierte Gröbnerbasis, so ist auch $\tau_\alpha(H)$ eine solche.*

Beweis: Sei $0 \neq g \in \tau_\alpha(I)$. Da H Gröbnerbasis ist, existiert eine Darstellung $\tau_\alpha^{-1}(g) = \sum_{h\in H} p_h h$, wobei für alle $h \in H$ mit $p_h h \neq 0$ die Ungleichung $\mathrm{lpp}(p_h h) \preceq \mathrm{lpp}\left(\tau_\alpha^{-1}(g)\right)$ erfüllt ist. Anwendung von τ_α führt auf $g = \sum_{h\in H} \tau_\alpha(p_h)\tau_\alpha(h)$ und aus (6.25) folgt $\mathrm{lpp}(\tau_\alpha(p_h)\tau_\alpha(h)) \preceq_Y \mathrm{lpp}(g)$ für alle $h \in H$ mit $\tau_\alpha(p_h)\tau_\alpha(h) \neq 0$. Das beweist die Gröbnerbasiseigenschaft von $\tau_\alpha(H)$.

Weiterhin folgt aus (6.25) unmittelbar, daß $\mathrm{lpp}(\tau_\alpha(H))$ das minimale Erzeugendensystem des Monoidideals $\mathrm{lpp}(\tau_\alpha(I)) \subseteq T(Y)$ ist, falls $\mathrm{lpp}(H)$ minimales Erzeugendensystem von $\mathrm{lpp}(I) \subseteq T(X)$ war. Außerdem hat $\tau_\alpha(h)$ den gleichen führenden Koeffizienten wie h. Schließlich ist jedes Potenzprodukt aus $\mathrm{supp}(\tau_\alpha(h))$ Teiler eines Elements aus dem Bild von $\mathrm{supp}(h)$ unter dem natürlichen Isomorphimus von $T(X)$ nach $T(Y)$. Diese drei Eigenschaften sichern, daß reduzierte Gröbnerbasen von der Abbildung τ_α wieder in reduzierte Gröbnerbasen überführt werden. □

Lemma 6.18 *Sei $I \subseteq R$ ein Ideal des Polynomrings $R = \mathbb{C}[X]$ und H eine Gröbnerbasis von I bezüglich der graduierten Struktur $\mathfrak{R} = (R, T(X), \prec, \mathrm{lpp})$. Dann ist $\tau_\alpha(H) \cup F$, wobei F die in (6.24) angegebene Gröbnerbasis ist, eine Gröbnerbasis des Ideals $J + IR_{X,Y}$ bezüglich der graduierten Struktur $\mathfrak{R}_{X,Y}$.*

Beweis: Nach dem vorangegangenen Lemma ist $\tau_\alpha(H)$ eine Gröbnerbasis des Ideals $\tau_\alpha(I)$. Da die führenden Potenzprodukte der Elemente von $\tau_\alpha(H)$ nur von $Y_1,\ldots,Y_n$ und die von F nur von $X_1,\ldots,X_n$ abhängen, wird für alle $h \in H$ und $f \in F$ die Beziehung $ggT(\mathrm{lpp}(\tau_\alpha(h)), \mathrm{lpp}(f)) = 1$ erfüllt. Folglich gilt nach dem ersten Buchbergerschen Kriterium (siehe [Bu85]), daß jedes zu einem kritischen Paar $(\tau_\alpha(h), f) \in \tau_\alpha(H) \times F$ gehörige S-Polynom $\mathrm{head}(f)\tau_\alpha(h) - \mathrm{head}(\tau_\alpha(h))f$ bei Division modulo $\{\tau_\alpha(h), f\} \subseteq \tau_\alpha(H) \cup F$ den Rest 0 läßt. Da $\tau_\alpha(H)$ und F Gröbnerbasen sind, lassen die S-Polynome der kritischen Paare aus $\tau_\alpha(H) \times \tau_\alpha(H)$ beziehungsweise $F \times F$ bei Division modulo $\tau_\alpha(H) \cup F$ ebenfalls den Rest 0. Also ist $\tau_\alpha(H) \cup F$ eine Gröbnerbasis bezüglich der graduierten Struktur $\mathfrak{R}_{X,Y}$. Das von $\tau_\alpha(H) \cup F$ in $R_{X,Y}$ erzeugte Ideal ist $J + \tau_\alpha(I)R_{X,Y} = J + IR_{X,Y}$. □

Man überzeugt sich leicht davon, daß $\tau_\alpha(H) \cup F$ für minimale Gröbnerbasen H eines echten Ideals $\{0\} \subsetneqq I \subsetneqq R$ ebenfalls eine minimale Gröbnerbasis ist. Sind alle führenden Potenzprodukte der Elemente von H mindestens vom Totalgrad zwei, so folgt aus der Reduziertheit von H auch die Reduziertheit von $\tau_\alpha(H) \cup F$.

Satz 6.19 *Seien $a \in E$ eine ganze Funktion, I ein Ideal von $R = \mathbb{C}[X]$ und $\alpha = (\alpha_1, \ldots, \alpha_n)$ ein Punkt des Raumes $\mathbb{C}^n$. Weiterhin seien J das durch die in (6.24) angegebene Menge F in $R_{X,Y}$ erzeugte Polynomideal und τ_α der durch $X_i \mapsto Y_i - \alpha_i$, $(i = 1, \ldots, n)$, erklärte Isomorphismus von E nach E_Y. Dann gilt die Gleichheit*

$$\tau_\alpha\left(\mathrm{rem}_{IE}(a)\right) = \mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right) = \mathrm{rem}_{(J+IR_{X,Y})E_{X,Y}}(a) \tag{6.27}$$

Beweis: Zunächst überzeugt man sich leicht von der Gültigkeit der Beziehung $\tau_\alpha(b) = \mathrm{rem}_{JE_{X,Y}}(b)$ für beliebige ganze Funktionen $b \in E$, somit bleibt nur die zweite Gleichheit nachzuweisen.

Aus $a - \mathrm{rem}_{IE}(a) \in IE$ und $\mathrm{rem}_{IE}(a) - \mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right) \in JE_{X,Y}$ ergibt sich $a - \mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right) \in (IE)E_{X,Y} + JE_{X,Y} = (IR_{X,Y} + J)E_{X,Y}$. Nach Satz 6.15 ist $\mathrm{rem}_{(J+IR_{X,Y})E_{X,Y}}(a)$ die eindeutig bestimmte ganze Funktion in den Variablen $X_1, \ldots, X_n, Y_1, \ldots, Y_n$, welche kongruent zu a modulo $(J + IR_{X,Y})E_{X,Y}$ ist und deren Träger kein dem Monoidideal $\mathrm{lpp}(J + IR_{X,Y}) \subset T(X,Y)$ angehöriges Potenzprodukt enthält. Wir werden zeigen, daß $\mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right)$ ebenfalls kein dem Monoidideal $\mathrm{lpp}(J + IR_{X,Y})$ angehöriges Potenzprodukt enthält. Nach Lemma 6.18 wird das Monoidideal $\mathrm{lpp}(J + IR_{X,Y})$ von den Variablen X und den führenden Potenzprodukten der Elemente von $\tau_\alpha(H)$ erzeugt. Für jedes Elemente $t \in \mathrm{supp}(\mathrm{rem}_{IE}(a))$ und jedes $h \in H$ gilt $\mathrm{lpp}(h) \nmid t$. Für beliebiges $b \in E_{X,Y}$ gilt $\mathrm{supp}(\mathrm{rem}_{JE_{X,Y}}(b)) \subseteq T(Y)$ und zu jedem $Y^\nu \in \mathrm{supp}(\mathrm{rem}_{JE_{X,Y}}(b))$ existiert ein $Y^{\nu_1}X^{\nu_2} \in \mathrm{supp}(b)$, so daß $Y^\nu \mid Y^{\nu_1+\nu_2}$. Wendet man das auf den Spezialfall $b = \mathrm{rem}_{IE}(a)$ an und beachtet dabei $\mathrm{supp}(\mathrm{rem}_{IE}(a)) \subseteq T(X) \setminus \mathrm{lpp}(H) \circ T(X)$, so zieht $Y^\nu \in \mathrm{supp}\left(\mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right)\right)$ die Existenz eines $X^\mu \in \mathrm{supp}(\mathrm{rem}_{IE}(a))$ mit $Y^\nu \mid Y^\mu$ und $\mathrm{lpp}(h) \nmid X^\mu$ für alle $h \in H$ nach sich. Mit Lemma 6.17 ergibt sich $\mathrm{lpp}(\tau_\alpha(h)) \nmid Y^\nu$ für alle $h \in H$. Damit ist bewiesen, daß $\mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right)$ eine modulo $(J + IR_{X,Y})E_{X,Y}$ zu a kongruente ganze Funktion mit

$$\mathrm{supp}\left(\mathrm{rem}_{JE_{X,Y}}\left(\mathrm{rem}_{IE}(a)\right)\right) \cap \mathrm{lpp}(J + IR_{X,Y}) = \emptyset$$

ist. Damit ist auch die zweite Gleichheit in (6.27) bewiesen. □

Folgerung 6.20 *Für beliebige Polynomideale $I \subseteq R$, ganze Funktionen $a \in E$ und $\alpha \in \mathbb{C}^n$ gilt die Gleichung*

$$\mathrm{rem}_{IE}(a)(\alpha) = \tau_\alpha\left(\mathrm{rem}_{IE}(a)\right)(0, \ldots, 0) = \mathrm{rem}_{(J+IR_{X,Y})E_{X,Y}}(a)(0, \ldots, 0) \tag{6.28}$$

Beweis: Die Behauptung folgt unmittelbar aus Satz 6.19 und Gleichung (6.26). □

Zu jedem Punkt $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ kann mit Hilfe von $\textsc{Divide}_{E_{X,Y}, \mathfrak{R}'_{X,Y}}$ für die rechte Seite eine Näherung beliebig vorgegebener Genauigkeit $\epsilon \in \mathbb{K}_+$ berechnet werden. Ein für praktische Belange wichtiger Fakt besteht darin, daß die Berechnung der reduzierten Gröbnerbasis des Ideals $J + IR_{X,Y}$ keine

Probleme in sich birgt, wie Lemma 6.18 und die daran anschließenden Bemerkungen belegen. In der Tat ist es nicht einmal notwendig, die Transformation der Gröbnerbasis tatsächlich auszuführen. Es reicht aus, obere Schranken für die zu $F \cup \tau_\alpha(H)$ gehörigen Werte ω und λ aus Algorithmus $\textsc{Divide}_{E_{X,Y},\Re'_{X,Y}}$ zu ermitteln. Damit kann die Funktion a so abgeschnitten werden, daß ein Polynom $b \in \mathbb{K}[X]$ entsteht, dessen Divisionsrest modulo $(J + IR_{X,Y})E_{X,Y}$ ein Absolutglied hat, welches betragsmäßig um höchstens ϵ von dem Absolutglied des Restes $\mathrm{rem}_{(J+IR_{X,Y})E_{X,Y}}(a)$ abweicht. Unter Ausnutzung von (6.27) kann dann die Restbildung mit Hilfe des mittleren Ausdrucks erfolgen, wozu die bereits bekannten Gröbnerbasen H und F von I und J ausreichen.

Kapitel 7

Involutive Basen

Die in diesem Kapitel vorgestellte Methode der involutiven Basen bietet einen alternativen Divisionsalgorithmus zum Entscheiden des Idealenthaltenseinsproblems in ausgewählten graduierten Strukturen.

Der historische Hintergrund wird von der Konstruktion involutiver Systeme im Zusammenhang mit der Lösung von Systemen partieller Differentialgleichungen gebildet (siehe [Ja29],[Th37] und [Po78]). Zharkov und Blinkov nutzten eine Dualität zwischen partiellen Differentialgleichungssystemen und Systemen algebraischer Gleichungen, um diese Methoden auf polynomiale Fragestellungen anzuwenden (siehe [ZB93]). In diesem Zusammenhang prägten sie den Begriff der *involutiven Basis* eines Polynomideals. Ein vielversprechender Ansatz zur Entwicklung eines allgemeinen Begriffs involutiver Basen wurde durch Gerdt und Blinkov in [GB96] vorgestellt. Die von ihnen vorgeschlagene axiomatische Theorie weist jedoch in allen bisherigen Fassungen des Papiers noch gravierende Mängel auf. Inwieweit diese behoben werden können, bleibt abzuwarten.

In dieser Arbeit nehmen wir einen rein algebraischen Aufbau einer allgemeinen Theorie involutiver Basen vor. Die Vorteile gegenüber dem axiomatischen Ansatz von Gerdt und Blinkov bestehen in einer wesentlich umfangreicheren Konstruktivität sowie einer größeren Wahlfreiheit während der Berechnungen, welche zur Anpassung an das betrachtete Ideal verwendet werden kann. In [Ap96] wurde bewiesen, daß das Axiomensystem von Gerdt und Blinkov nicht alle hier betrachteten involutiven Divisionen überdeckt. Andererseits gibt es auch Grund zur Annahme, daß die hier entwickelte Theorie nicht alle von Gerdt und Blinkov untersuchten involutiven Divisionen behandeln kann. In Abschnitt 7.4.2 werden wir näher darauf eingehen.

Ähnlich der Theorie der Gröbnerbasen besteht auch das Anliegen der involutiven Basen darin, ein Erzeugendensystem zu finden, dessen Gröbnerfiltrierung mit der durch die Ringfiltrierung induzierten Filtrierung des Ideals übereinstimmt. Daraus folgt insbesondere, daß jede involutive Basis auch Gröbnerbasis ist. Der genaue Zusammenhang beider Theorien ist nach wie vor nicht vollständig erforscht. Heuristische Untersuchungen an Hand von Testläufen zeigen, daß die involutive Methode wenigstens in einer Reihe von Beispielen kürzere Rechenzeiten und geringeren Speicherplatzbedarf aufweist (siehe [ZB93],[Ni96]). Damit sind die involutiven Basen gerade aus Anwendungssicht

heraus zukunftsträchtig. Allerdings wird die Hoffnung dadurch gedämpft, daß keine Verbesserung der Zeit- und Speicherkomplexität zu erwarten ist. Ausgehend von den Ergebnissen von Mayr und Meyer (siehe [MaMe82]) wiesen Möller und Mora eine in der Anzahl der Unbestimmten doppelt exponentielle kleinste obere Schranke für das Wachstum des Maximalgrads bei Übergang von einem beliebigen Erzeugendensystem zu einer reduzierten Gröbnerbasis nach (siehe [MöMo84]). Diese Schranke kann für die hier in Frage stehenden speziellen Gröbnerbasen natürlich nicht kleiner werden.

Auch aus theoretischer Sicht bieten die involutiven Basen interessante Ansatzpunkte. So zeigte sich in [Ap96], daß die Redundanz der involutiven Basen einen geradlinigen Algorithmus zur Berechnung der Hilbertfunktion eines Ideals liefert. Außerdem beinhaltet die involutive Methode in Analogie zur Gröbnertheorie in Gruppenalgebren einen Sättigungsschritt. Damit ergibt sich möglicherweise ein neuer Ansatz der Kopplung algebraischer Methoden mit Mitteln der Termersetzungstheorie.

7.1 Der Verband der partiellen Divisionen

Die Vielfachenrelation eines Monoids Γ kann durch die Familie $(\mathrm{Id}_\Gamma(\gamma))_{\gamma\in\Gamma}$ der von $\gamma \in \Gamma$ erzeugten Monoidideale $\mathrm{Id}_\Gamma(\gamma)$ charakterisiert werden, denn $\mathrm{Id}_\Gamma(\gamma)$ umfaßt gerade alle Vielfachen von γ. Vermöge der Beziehung $\gamma \mid \omega \Longleftrightarrow \omega \in \mathrm{Id}_\Gamma(\gamma)$ beschreibt die obige Familie ebenso die Teilbarkeitsrelation von Γ. Auf diesem Zusammenhang baut der Begriff der partiellen Divisionen auf. Dabei lassen wir nur noch ausgewählte Multiplikatoren für die Elemente von Γ zu. Von den zulässigen Multiplikatoren eines Elements $\gamma \in \Gamma$ wird verlangt, daß ihre Gesamtheit einen direkten Faktor von Γ bildet.

Unsere Untersuchungen beschränken sich auf noethersche kommutative wohlgeordnete Monoide Γ. Diese besitzen ein eindeutig bestimmtes minimales Erzeugendensystem $X = \{X_1, \ldots, X_n\}$ und jeder ihrer direkten Faktoren wird als Monoid von einer Teilmenge $Y \subseteq X$ erzeugt. Erzeugt die Teilmenge $Y \subseteq X$ einen direkten Faktor Ω von Γ, so erzeugt auch $X\backslash Y$ einen direkten Faktor Ω' von Γ und das Produkt $\Gamma = \Omega \circ \Omega'$ ist direkt. Im allgemeinen erzeugt jedoch nicht jede Teilmenge $Y \subseteq X$ einen direkten Faktor von Γ. Nur im Falle des von X frei erzeugten kommutativen Monoids $\Gamma = T(X)$ ist ein Untermonoid genau dann direkter Faktor von Γ, wenn es von einer Teilmenge $Y \subseteq X$ erzeugt wird.

Definition 7.1 *Sei Γ ein kommutatives Monoid mit minimalem Erzeugendensystem X und $Y = (Y_\gamma)_{\gamma\in\Gamma}$ eine Familie von Teilmengen $Y_\gamma \subseteq X$, die direkte Faktoren $\Omega_\gamma = \langle Y_\gamma\rangle$ von Γ erzeugen.*

Dann wird die Familie $\mathcal{D} = (\gamma\circ\Omega_\gamma)_{\gamma\in\Gamma}$ die von Y erzeugte partielle Division *von Γ genannt. Ein Element $\omega \in \gamma\circ\Omega_\gamma$ heißt $\mathcal{D}$-*Vielfaches *von γ. Entsprechend bezeichnen wir γ in dieser Situation als $\mathcal{D}$-*Teiler *von ω und schreiben dafür $\gamma \mid_{\mathcal{D}} \omega$.*

Sei $\Delta \subseteq \Gamma$ eine Menge von Monoidelementen und $\sqsubset$ eine lineare Ordnung von Δ. Die partielle Division $\mathcal{D} = (D_\gamma)_{\gamma\in\Gamma}$ wird zulässig *auf $(\Delta, \sqsubset)$ genannt, falls für alle $\delta, \delta' \in \Delta$ mit $\delta' \sqsubset \delta$ eine der Bedingungen* i) *$D_{\delta'} \subseteq D_\delta$ oder*

ii) $D_\delta \cap \mathrm{Id}_\Gamma(\delta') = \emptyset$ *zutrifft. Die Menge aller auf* $(\Delta, \sqsubset)$ *zulässigen partiellen Divisionen wird mit* $\mathbb{D}_{(\Delta,\sqsubset)}$ *bezeichnet.*

Darüberhinaus nennen wir $\mathcal{D}$ *auf* Δ zulässig, *falls eine lineare Ordnung* $\sqsubset$ *von* Δ *existiert, für welche* $\mathcal{D}$ *auf* $(\Delta, \sqsubset)$ *zulässig ist. Entsprechend bezeichnen wir die Menge aller auf* Δ *zulässigen partiellen Divisionen mit* $\mathbb{D}_\Delta$.

Leicht zu beweisende Aussagen über zulässige partielle Divisionen sind:

i) Für beliebige Mengen $\Delta \subseteq \Sigma \subseteq \Gamma$ von Monoidelementen und eine beliebige lineare Ordnung $\sqsubset$ auf Σ gilt die Beziehung $\mathbb{D}_{(\Sigma,\sqsubset)} \subseteq \mathbb{D}_{(\Delta,\sqsubset|_\Delta)}$.

ii) $\mathbb{D}_\emptyset$ umfaßt alle partiellen Divisionen.

iii) Sei Δ eine durch $\sqsubset$ linear geordnete Teilmenge von Γ. Falls es Elemente $\delta, \delta' \in \Delta$ mit $\delta \neq \delta'$ und $\delta' \mid \delta$ gibt, welche zueinander in der Relation $\delta' \sqsubset \delta$ stehen, so ist die Menge $\mathbb{D}_{(\Delta,\sqsubset)}$ aller auf der geordneten Menge $(\Delta, \sqsubset)$ zulässigen partiellen Divisionen leer.

Zum Beweis der dritten Aussage betrachten wir eine beliebige partielle Division $\mathcal{D} = (D_\gamma)_{\gamma\in\Gamma}$. Zum einen kann wegen $\delta' \notin Id_\Gamma(\delta) \supseteq D_\delta$ nicht die Inklusion $D_{\delta'} \subseteq D_\delta$ gelten. Zum anderen haben wir $\delta \in D_\delta \cap \mathrm{Id}_\Gamma(\delta') \neq \emptyset$ und folglich ist $\mathcal{D}$ nicht zulässig auf $(\Delta, \sqsubset)$.

Auf der Menge aller partiellen Divisionen werden die folgenden binären Relationen eingeführt:

Definition 7.2 *Seien* $\mathcal{D} = (D_\gamma)_{\gamma\in\Gamma}$ *und* $\mathcal{C} = (C_\gamma)_{\gamma\in\Gamma}$ *zwei partielle Divisionen und* $\Delta \subseteq \Gamma$ *eine Menge von Monoidelementen.*

Falls für alle $\delta \in \Delta$ *die Gleichheit* $D_\delta = C_\delta$ *zutrifft, so nennen wir* $\mathcal{D}$ *und* $\mathcal{C}$ Δ-äquivalent *(Schreibweise:* $\mathcal{D} \equiv_\Delta \mathcal{C}$*).*

Im Falle der Gültigkeit der Enthaltenseinsrelationen $D_\gamma \subseteq C_\gamma$ *für alle* $\gamma \in \Gamma$ *wird* $\mathcal{C}$ *als* Verfeinerung *von* $\mathcal{D}$ *bezeichnet (Schreibweise:* $\mathcal{D} \leq \mathcal{C}$*).*

$\equiv_\Delta$ ist für jedes $\Delta \subseteq \Gamma$ eine Äquivalenzrelation. Die Verfeinerungsrelation $\leq$ ist eine reflexive Halbordnung und die Menge aller partiellen Divisionen bildet mit ihr einen Verband $(\mathbb{D}_\emptyset, \leq)$.

Sei $\Delta \subseteq \Gamma$ eine beliebige Menge von Monoidelementen und $\mathbb{D}_\emptyset / \equiv_\Delta$ die Menge der Restklassen partieller Divisionen modulo der Δ-Äquivalenz. Jede Restklasse $[\mathcal{D}]_{\equiv_\Delta} \in \mathbb{D}_\emptyset / \equiv_\Delta$ besitzt ein größtes Element $\max[\mathcal{D}]_{\equiv_\Delta}$ bezüglich $\leq$. Genauer gilt für jedes $\mathcal{D} = (D_\gamma)_{\gamma\in\Gamma} \in \mathbb{D}_\emptyset$ die Beziehung $\max[\mathcal{D}]_{\equiv_\Delta} = (C_\gamma)_{\gamma\in\Gamma}$ mit $C_\delta = D_\delta$ für alle $\delta \in \Delta$ und $C_\gamma = \gamma \circ \Gamma$ für alle $\gamma \notin \Delta$. Die Verfeinerungshalbordnung induziert vermöge

$$[\mathcal{D}]_{\equiv_\Delta} \leq_{\equiv_\Delta} [\mathcal{C}]_{\equiv_\Delta} :\Longleftrightarrow \exists \mathcal{D}', \mathcal{C}' \ : \ \mathcal{D} \equiv_\Delta \mathcal{D}' \wedge \mathcal{C} \equiv_\Delta \mathcal{C}' \wedge \mathcal{D}' \leq \mathcal{C}'$$

eine Verbandshalbordnung $\leq_{\equiv_\Delta}$ auf der Restklassenstruktur $\mathbb{D}_\emptyset / \equiv_\Delta$. Offensichtlich gilt genau dann $[\mathcal{D}]_{\equiv_\Delta} \leq_{\equiv_\Delta} [\mathcal{C}]_{\equiv_\Delta}$, wenn $\max[\mathcal{D}]_{\equiv_\Delta} \leq \max[\mathcal{C}]_{\equiv_\Delta}$ zutrifft. Die Abbildung $[\mathcal{D}]_{\equiv_\Delta} \mapsto \max[\mathcal{D}]_{\equiv_\Delta}$ beschreibt einen starken Ordnungsmonomorphismus von $(\mathbb{D}_\emptyset / \equiv_\Delta, \leq_{\equiv_\Delta})$ in $(\mathbb{D}_\emptyset, \leq)$.

Betrachten wir die Menge $\mathbb{D}_\Delta / \equiv_\Delta \subseteq \mathbb{D}_\emptyset / \equiv_\Delta$ der Restklassen aller auf Δ zulässigen partiellen Divisionen modulo der Δ-Äquivalenz. Diese ist gegenüber

der Bildung von Infima beliebiger nichtleerer Teilmengen abgeschlossen. Eine analoge Aussage für Suprema trifft jedoch im allgemeinen nicht zu. Daher ist $\mathbb{D}_\Delta / \equiv_\Delta$ nur ein unterer Unterhalbverband von $\mathbb{D}_\emptyset / \equiv_\Delta$.

7.2 Involutive Basen graduierter Strukturen

Das Konzept der partiellen Divisionen eines noetherschen kommutativen Monoids Γ läßt sich zunächst auf homogene Problemstellungen in Γ-graduierten Ringen und dann auf graduierte Strukturen anwenden.

Definition 7.3 *Sei Γ ein noethersches kommutatives Monoid, G ein Γ-graduierter Ring und $\mathcal{D}$ eine partielle Division von Γ. Weiterhin sei $H \subset G$ eine Menge von Null verschiedener homogener Elemente.*

Ein von Null verschiedenes homogenes Element $a \in G$, welches dem von $\{h \in H \mid \deg_\Gamma(h) \mid_\mathcal{D} \deg_\Gamma(a)\}$ erzeugten Ideal angehört, nennen wir eine $\mathcal{D}$-Kombination von H. Per definitionem ist das Nullelement stets $\mathcal{D}$-Kombination von H. Die Menge aller endlichen Summen von $\mathcal{D}$-Kombinationen von H wird mit $\mathrm{Dom}_\mathcal{D}(H)$ bezeichnet und der $\mathcal{D}$-Bereich von H genannt. Falls $\mathcal{D}$ auf der Menge $\deg_\Gamma(H)$ zulässig ist und der $\mathcal{D}$-Bereich von H das gesamte von H erzeugte Ideal I von G umfaßt, dann nennen wir H ein $\mathcal{D}$-Erzeugendensystem von I.

Analog werden die Begriffe des $\mathcal{D}$-Links- beziehungsweise $\mathcal{D}$-Rechtsbereichs sowie des $\mathcal{D}$-Erzeugendensystems eines einseitigen Ideals von G eingeführt.

Definition 7.4 *Seien $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur mit noetherschem wohlgeordnetem kommutativem Wertemonoid $(\Gamma, \prec)$ und $\mathcal{D}$ eine partielle Division von Γ. Eine Teilmenge F des Ideals $I \subseteq R$ heißt eine* $\mathcal{D}$-involutive Basis[1] *von I bezüglich $\mathfrak{R}$, falls die Menge $\mathrm{in}(F)$ der Initialterme aller Elemente von F ein $\mathcal{D}$-Erzeugendensystem des Initialideals $\mathrm{In}(I)$ von I ist.*

Analog führt man unter Bezugnahme auf die einseitigen Initialideale $\mathrm{LIn}(I)$ beziehungsweise $\mathrm{RIn}(I)$ auch $\mathcal{D}$-involutive Basen bezüglich $\mathfrak{R}$ für einseitige Ideale $I \subseteq R$ ein.

Gemäß der obigen Definition weist eine $\mathcal{D}$-involutive Basis F bezüglich $\mathfrak{R}$ zwei wesentliche Eigenschaften auf. Zum ersten muß die involutive Division $\mathcal{D}$ auf der Menge $\deg_\Gamma(\mathrm{in}(F))$ der Grade ihrer Initialterme zulässig sein und zum zweiten muß der $\mathcal{D}$-Bereich ihrer Initialterme gleich ihrem Initialideal sein. Es bestehen die folgenden offensichtlichen Zusammenhänge:

Bemerkung 7.5

i) Wegen $\mathrm{Dom}_\mathcal{D}(\mathrm{in}(F)) \subseteq \mathrm{In}(F) \subseteq \mathrm{In}(I)$ ist jede $\mathcal{D}$-involutive Basis F eines Ideals I bezüglich $\mathfrak{R}$ erst recht eine Gröbnerbasis von I bezüglich $\mathfrak{R}$.

[1] Der Begriff der *involutiven Basis* lehnt sich an Zharkov/Blinkov an und stellt eine Verallgemeinerung des in [ZB93] vorgestellten Konzepts dar.

ii) Seien F eine $\mathcal{D}$-involutive Basis bezüglich $\mathfrak{R}$ und $\mathcal{C}$ eine auf $\deg_\Gamma(\mathrm{in}(F))$ zulässige Verfeinerung von $\mathcal{D}$. Dann ist F auch $\mathcal{C}$-involutive Basis bezüglich $\mathfrak{R}$.

Aus *i)* ergibt sich unmittelbar, daß jede $\mathcal{D}$-involutive Basis F von I das Ideal I erzeugt. Für $\mathcal{D}$-involutive Basen F zweiseitiger Ideale kann die im Divisionsalgorithmus $\textsc{Div}_R$ gerufene Funktion $\textsc{Divide}_G$ (siehe Seite 61) durch eine Funktion $\textsc{pDivide}_G$ der folgenden Spezifikation ausgetauscht werden und der dabei entstehende Algorithmus $\textsc{pDiv}_R$ (mit $\mathcal{D}$ als zusätzlichem Argument) beschreibt ebenfalls einen Nullsimplifikator für R/I.

Aufruf: $(p_1,\ldots,p_l,q_1,\ldots,q_l,A,r_1,\ldots,r_l) := \textsc{pDivide}_G(a,H,\mathcal{D})$
Eingaben: a homogenes Element von G,
$H=\{h_1,\ldots,h_m\}$ endliche Menge homogener Elemente von G, $0\notin H$
$\mathcal{D}$ auf $\{\deg_\Gamma(h_1),\ldots,\deg_\Gamma(h_m)\}$ zulässige partielle Division.
Ausgaben: $p_1,\ldots,p_l,q_1,\ldots,q_l,A$ homogen, $1\le r_1,\ldots,r_l\le m$, wobei
$a=\sum_{i=1}^{l} p_i h_{r_i} q_i + A$,
$\deg_\Gamma(h_{r_i}) \mid_{\mathcal{D}} \deg_\Gamma(a)$, $\deg_\Gamma(p_i)\circ\deg_\Gamma(h_{r_i})\circ\deg_\Gamma(q_i)=\deg_\Gamma(a)$ $(i=1,\ldots,l)$
und $A=0 \iff a\in \mathrm{Dom}_{\mathcal{D}}(H)$.

Entsprechendes gilt im einseitigen Fall. Eine mögliche Berechnungsvorschrift für $\textsc{pDivide}_G$ ist

$H' = \{h_i \mid 1\le i\le m, \deg_\Gamma(h_i)\mid_{\mathcal{D}} \deg_\Gamma(a)\}$
$(p_1,\ldots,p_l,q_1,\ldots,q_l,A,r_1,\ldots,r_l) := \textsc{Divide}_G(a,H')$
return$(p_1,\ldots,p_l,q_1,\ldots,q_l,A,r_1,\ldots,r_l)$

Dabei beziehen sich die durch $\textsc{Divide}_G$ ausgegebenen Indizes $r_1,\ldots,r_l$ auf die ursprüngliche Numerierung von H. An dieser Berechnungsvorschrift erkennt man sofort, daß die Entscheidbarkeit des Enthaltenseinsproblems endlich erzeugter homogener Ideale des assoziierten graduierten Rings G und die Entscheidbarkeit des $\mathcal{D}$-Teilbarkeitsproblems von Γ die Berechenbarkeit der Funktion $\textsc{pDivide}_G$ nach sich zieht. Ebenso wie im Gröbnerfall kann der Definitionsbereich des Nullsimplifikators $\textsc{pDiv}_R$ auf beliebige endliche Erzeugendensysteme F erweitert werden. Auch hier beschreibt der enstehende Divisionsalgorithmus $\textsc{pDivide}_R$ für Mengen F die keine $\mathcal{D}$-involutive Basis sind, keinen Nullsimplifikator modulo des von F erzeugten Ideals. Der verallgemeinerte Divisionsalgorithmus $\textsc{pDivide}_R$ bildet wiederum die Grundlage für den Test auf und die Konstruktion von $\mathcal{D}$-involutiven Basen. Sei $F\subset R$ eine endliche Teilmenge von Null verschiedener Elemente des Ringes R und $\mathcal{D}$ eine auf $\varphi(F)=\deg_\Gamma(\mathrm{in}(F))$ zulässige partielle Division. Wir führen die Funktion $\mathrm{Nf}_{\mathcal{D},F} : R\to R$ ein, welche jedem Element $g\in R$ den Rest $\hat{a}\in R$ bei der Division $\textsc{pDivide}_R(g,F,\mathcal{D})$ zuordnet. Die Bezeichnung Nf soll an den Terminus einer *Normalform* modulo $\mathcal{D}$ und F erinnern. Die wesentlichen Eigenschaften von $\mathrm{Nf}_{\mathcal{D},F}(g)$ bestehen darin, daß

i) im Falle $\mathrm{Nf}_{\mathcal{D},F}(g) \neq 0$ für alle $f \in F$ die Beziehung $\varphi(f) \nmid_{\mathcal{D}} \varphi(\mathrm{Nf}_{\mathcal{D},F}(g))$ gilt und daß

ii) eine Darstellung $\mathrm{Nf}_{\mathcal{D},F}(g) - g = \sum_{j=1}^{k} u_j f_j v_j$ existiert, wobei $u_j, v_j \in R$, $f_j \in F$ sowie $\varphi(f_j) \mid_{\mathcal{D}} \varphi(u_j) \circ \varphi(f_j) \circ \varphi(v_j) \preceq \varphi(g)$ für alle $j = 1, \ldots, k$.

Bei aller Ähnlichkeit der Theorien der $\mathcal{D}$-involutiven und der Gröbnerbasen bestehen jedoch auch wesentliche Unterschiede. So besitzt ein Ideal zu vorgegebenem $\mathcal{D}$ im allgemeinen keine $\mathcal{D}$-involutive Basis. Selbst ein Erzeugendensystem F von I mit der wesentlich schwächeren Eigenschaft, daß $\mathcal{D}$ auf $\deg_\Gamma(\mathrm{in}(F))$ zulässig ist, braucht nicht notwendigerweise zu existieren.

Bei vorgegebener endlicher Menge F drängt sich eine Reihe interessanter Problemstellungen auf:

i) Ist die Frage, ob F eine $\mathcal{D}$-involutive Basis ist, für vorgegebenes $\mathcal{D}$ entscheidbar?

ii) Gibt es eine partielle Division $\mathcal{D}$, für welche das von F erzeugte Ideal I eine endliche $\mathcal{D}$-involutive Basis besitzt?

iii) Falls ja, kann man eine derartige partielle Division $\mathcal{D}$ und eine zugehörige endliche $\mathcal{D}$-involutive Basis von I berechnen?

Während man im Gröbnerfall gerade dann auf Schwierigkeiten stößt, wenn ein homogenes Element Vielfaches mehrerer Initialterme von Elementen aus F ist, stehen wir nun vor dem umgekehrten Problem. Es kann Vielfache von Elementen von F geben, deren Initialterm einen Grad aufweist, der keinen Grad eines Initialterms eines Elementes von F zum $\mathcal{D}$-Teiler hat. Der Algorithmus zum Test, ob F eine $\mathcal{D}$-involutive Basis ist, wird gerade an diesem neuen Typ kritischer Situationen ansetzen.

7.3 Involutive Basen in effektiven Algebren von auflösbarem Typ

Sei $\mathfrak{R} = (R, T(X), \prec, \mathrm{lpp})$ eine effektive Linksgröbnerstruktur der Algebra R von auflösbarem Typ in den Variablen $X = \{X_1, \ldots, X_n\}$ über dem Körper $\mathbb{K}$. Die Bestandteile von $\mathfrak{R}$ sind wie in Abschnitt 5.1 erklärt, im weiteren bezeichnen wir $T(X)$ kurz mit T. Die Multiplikation des Monoids T der Potenzprodukte wird mit $\circ$ bezeichnet. Sofern die Potenzprodukte als Element von R angesehen werden, so wird $\cdot$ oder kein Operationszeichen als Multiplikationssymbol verwendet. Quotienten und kleinste gemeinsame Vielfache von Potenzprodukten beziehen sich immer auf die Monoidoperation $\circ$.

Satz 7.6 *Sei F eine Menge von Null verschiedener Elemente und I das von F erzeugte Linksideal von R. Die von $(Y_u)_{u \in T}$ erzeugte partielle Division $\mathcal{D} = (D_u)_{u \in T}$ sei auf der durch $\sqsubset$ linear geordneten Menge $(\mathrm{lpp}(F), \sqsubset)$ der führenden Potenzprodukte der Elemente von F zulässig. Die führenden Potenzprodukte der Elemente von F seien paarweise nicht $\mathcal{D}$-Teiler voneinander. Dann sind die folgenden Eigenschaften zueinander äquivalent:*

i) *F ist eine $\mathcal{D}$-involutive Basis bezüglich $\mathfrak{R}$.*

ii) *Für alle $f \in F$ und $x \in X \backslash Y_{\mathrm{lpp}(f)}$ besitzt das Produkt xf eine Darstellung $xf = \sum_{i=1}^{k} c_i t_i f_i$ mit den Eigenschaften $0 \neq c_i \in \mathbb{K}$, $t_i \in T$, $f_i \in F$, $\mathrm{lpp}(f_i) \mid_D t_i \circ \mathrm{lpp}(f_i)$ für alle $i = 1, \ldots, k$ und $t_{i+1} \circ \mathrm{lpp}(f_{i+1}) \prec t_i \circ \mathrm{lpp}(f_i)$ für alle $i = 1, \ldots, k-1$.*

iii) *Für alle $f \in F$ und $x \in X \setminus Y_{\mathrm{lpp}(f)}$ existiert ein $f' \in F \setminus \{f\}$ mit $\mathrm{lpp}(f') \sqsubset \mathrm{lpp}(f)$, so daß zwischen den Elementen von F eine Relation der Gestalt $xf - ctf' = \sum_{i=1}^{k} h_i f_i$, wobei $0 \neq c \in \mathbb{K}$, $t \in T$, $0 \neq h_i \in R$, $f_i \in F$ sowie $\mathrm{lpp}(h_i) \circ \mathrm{lpp}(f_i) \prec x \circ \mathrm{lpp}(f) = t \circ \mathrm{lpp}(f')$ für alle $i = 1, \ldots, k$, besteht.*

iv) *F ist eine Gröbnerbasis von I bezüglich $\mathfrak{R}$ und es gilt $X \circ \mathrm{lpp}(F) \subseteq \bigcup_{f \in F} D_{\mathrm{lpp}(f)}$.*

Beweis: *i) $\Rightarrow$ ii)* trivial, Anwendung von pDIVIDE$_R$ liefert die gesuchte Darstellung von xf.
ii) $\Rightarrow$ iii) Sei $xf = \sum_{i=1}^{k} c_i t_i f_i$ die Darstellung aus *ii)*. Insbesondere gilt $\mathrm{in}(xf) = \mathrm{in}(c_1 t_1 f_1)$ und $\mathrm{lpp}(f_1) \mid_{\mathcal{D}} x \circ \mathrm{lpp}(f)$. Letzteres impliziert $x \circ \mathrm{lpp}(f) \in D_{\mathrm{lpp}(f_1)} \cap \mathrm{Id}_T(\mathrm{lpp}(f)) \neq \emptyset$. Der Fall $\mathrm{lpp}(f) = \mathrm{lpp}(f_1)$ ist wegen $x \circ \mathrm{lpp}(f) \in D_{\mathrm{lpp}(f_1)} \setminus D_{\mathrm{lpp}(f)}$ ausgeschlossen. Angenommen, es würde $\mathrm{lpp}(f) \sqsubset \mathrm{lpp}(f_1)$ gelten. Dann müßte mit Notwendigkeit der Fall $D_{\mathrm{lpp}(f)} \subset D_{\mathrm{lpp}(f_1)}$ vorliegen. Das ist ein Widerspruch zur Voraussetzung, daß kein führendes Potenzprodukt $\mathcal{D}$-Vielfaches eines anderen sein darf. Also kann $f' = f_1$ gewählt werden und einfaches Umstellen liefert die in *iii)* geforderte Relation.
iii) $\Rightarrow$ i) Für jeden Term $t \in \mathrm{Id}_T(\mathrm{lpp}(F))$ definieren wir die (nicht leere) Menge $G_t = \{g \in F : \mathrm{lpp}(g) \mid t\}$. Da nach Voraussetzung kein führendes Potenzprodukt eines Elementes von F $\mathcal{D}$-Vielfaches eines anderen sein darf, sind die führenden Potenzprodukte der Elemente von F insbesondere paarweise verschieden. Also enthält jede Menge G_t ein eindeutig bestimmtes Element $g_t \in G$ mit bezüglich $\sqsubset$ minimalem führenden Potenzprodukt und wir setzen $v_t := \frac{t}{\mathrm{lpp}(g_t)} \in T$. Angenommen, es gilt $\mathrm{lpp}(g_t) \nmid_{\mathcal{D}} t$. Dann besitzt v_t einen Teiler $y \in X \setminus Y_{\mathrm{lpp}(g_t)}$. Aus *iii)* folgt die Existenz eines Elementes $g \in F$ mit $\mathrm{lpp}(g) \sqsubset \mathrm{lpp}(g_t)$ sowie $\mathrm{lpp}(g) \mid (y \circ \mathrm{lpp}(g_t)) \mid t$, im Widerspruch zur Konstruktion von g_t. Damit erhalten wir

$$v_t \in \langle Y_{\mathrm{lpp}(g_t)} \rangle \tag{7.1}$$

für alle $t \in \mathrm{Id}_T(\mathrm{lpp}(F))$. Unser nächstes Ziel ist es, für alle $f \in G_t$ die Beziehung

$$c_{t,f} u_{t,f} f - v_t g_t \in \widehat{\mathcal{F}}_t^{(F)}, \tag{7.2}$$

wobei $c_{t,f} \in \mathbb{K}$, $u_{t,f} \in T$ sowie $\mathrm{in}(c_{t,f} u_{t,f} f) = \mathrm{in}(v_t g_t)$ gelten und $\mathfrak{F}^{(F)} = \left(\mathcal{F}_t^{(F)}\right)_{t \in T}$ die durch F bestimmte Gröbnerfiltrierung von I ist, nachzuweisen. Die Endlichkeit von G_t erlaubt einen Induktionsbeweis über $\mathrm{lpp}(f)$ bezüglich $\sqsubset$. Ist $\mathrm{lpp}(f)$ minimal, so gilt $f = g_t$, $c_{t,f} = 1$ sowie $u_{t,f} = v_t$ und die Gültigkeit von (7.2) ist offensichtlich. Betrachten wir den Fall $\mathrm{lpp}(g_t) \sqsubset \mathrm{lpp}(f)$. Nach

Voraussetzung gilt $\mathrm{lpp}(g_t) \notin D_{\mathrm{lpp}(f)}$ und folglich $D_{\mathrm{lpp}(f)} \cap \mathrm{Id}_T(\mathrm{lpp}(g_t)) = \emptyset$. Demnach besitzt $u_{t,f}$ einen Teiler $y \in X \setminus Y_{\mathrm{lpp}(f)}$. Aus *iii)* folgt die Existenz von $f' \in F$, $d \in \mathbb{K}$ und $w \in T$ mit den Eigenschaften $\mathrm{lpp}(f') \sqsubset \mathrm{lpp}(f)$ und $yf - dwf' \in \widehat{\mathcal{F}}^{(F)}_{y \circ \mathrm{lpp}(f)}$. Also $u'yf - du'wf' \in \widehat{\mathcal{F}}^{(F)}_t$, wobei $u' \in T$ mit $u' \circ y = u_{t,f}$. Anwendung der Induktionsvoraussetzung auf f' und Einsetzen führt schließlich auf die Enthaltenseinsrelation (7.2). Wir betrachten ein beliebiges $h \in I$ und setzen $t := \min_{\prec} \left\{ s \in T \ : \ h \in \mathcal{F}^{(F)}_s \right\}$. h besitzt eine Darstellung $h = \sum_{i=1}^{k} d_i u_i f_i$ mit $d_i \in \mathbb{K} \setminus \{0\}$, $u_i \in T$, $f_i \in F$ und $u_i \circ \mathrm{lpp}(f_i) \preceq t$ für alle $i = 1, \ldots, k$. Sei $J = \{i \mid 1 \leq i \leq k \wedge u_i \circ \mathrm{lpp}(f_i) = t\}$. Dann gilt $h - \sum_{i \in J} d_i u_i f_i \in \widehat{\mathcal{F}}^{(F)}_t$. Einsetzen der Beziehungen (7.2) führt auf $h - \sum_{i \in J} d'_i v_t g_t \in \widehat{\mathcal{F}}^{(F)}_t$, wobei $d'_i := \frac{d_i}{c_{t,f_i}}$ $(i \in J)$. Aus $h \notin \widehat{\mathcal{F}}^{(F)}_t$ folgt $d := \sum_{i \in J} d'_i \neq 0$ und aus Gradgründen muß $\mathrm{lpp}(h) = \mathrm{lpp}(v_t g_t)$ gelten. Mit (7.1) schließen wir auf $\mathrm{lpp}(g_t) \mid_{\mathcal{D}} \mathrm{lpp}(h)$ und erhalten letztendlich, daß F eine $\mathcal{D}$-involutive Basis ist.
Der Nachweis der Gültigkeit der Implikationen *i)* $\Rightarrow$ *iv)* $\Rightarrow$ *iii)* ist trivial und vervollständigt den Beweis. □

Die äquivalente Eigenschaft *ii)* $\mathcal{D}$-involutiver Basen bildet die Grundlage für den Algorithmus *IBTEST* zum Nachweis der Eigenschaft eines Erzeugendensystems eines Linksideals, $\mathcal{D}$-involutive Basis zu sein. Ähnlich der Buchbergerschen Idee der S-Polynome, von denen er zeigen konnte, daß die Nullreduzierbarkeit dieser endlichen Menge spezieller Idealelemente bereits die Nullreduzierbarkeit sämtlicher Idealelemente nach sich zieht, erweist sich auch hier der Nachweis, daß für jede der endlich vielen *Prolongationen* xf mit $f \in F$ und $x \in X \setminus Y_{\mathrm{lpp}(f)}$ die Gleichheit $\mathrm{Nf}_{\mathcal{D},F}(xf) = 0$ gilt, als konstruktiver Test.

Aufruf: $\hat{a} := \mathrm{IBTest}(F, \mathcal{D})$
Eingaben: F endliches Erzeugendensystem des Linksideals I, $0 \notin F$
$\mathcal{D}$ auf $\mathrm{lpp}(F) = \{\mathrm{lpp}(f) \mid f \in F\}$ zulässige partielle Division.
Ausgaben: $\hat{a} \in I$ mit $\hat{a} = 0$ falls F eine $\mathcal{D}$-involutive Basis von I ist und
$\mathrm{lpp}(f) \nmid_{\mathcal{D}} \mathrm{lpp}(\hat{a})$ für alle $f \in F$ sonst.

Berechne eine minimale Menge $K \subseteq F$ mit $\mathrm{lpp}(K) = \mathrm{lpp}(F)$
$H := \{g \in K \mid \forall f \in K \setminus \{g\} \ : \ \mathrm{lpp}(f) \nmid_{\mathcal{D}} \mathrm{lpp}(g)\}$
$L := \{(1, h) \mid h \in F \setminus H\} \cup \{(y, h) \mid h \in H \wedge y \in X \wedge \mathrm{lpp}(h) \nmid_{\mathcal{D}} y \circ \mathrm{lpp}(h)\}$
while $L \neq \emptyset$ **do**
  Wähle $(u, h) \in L$ mit $u \circ \mathrm{lpp}(h)$ minimal bezüglich $\prec$
  $L := L \setminus \{(u, h)\}$
  $\hat{a} := \mathrm{Nf}_{\mathcal{D},H}(uh)$
  if $\hat{a} \neq 0$ **then return**$(\hat{a})$
return(0)

Der Gröbnertheorie folgend liegt es nahe, das Erzeugendensystem F im Falle des Mißerfolgs durch das Element $\hat{a}$ zu ergänzen und den Test zu wiederholen. Das ist jedoch nicht ohne weiteres möglich, da $\mathcal{D}$ im allgemeinen auf der erweiterten Menge $\mathrm{lpp}(F) \cup \{\mathrm{lpp}(\hat{a})\}$ der führenden Potenzprodukte nicht zulässig zu sein

braucht. Im wesentlichen gibt es zwei Möglichkeiten, diese Schwierigkeit zu beheben. Zum einen können wir fordern, daß $\mathcal{D}$ auf ganz T zulässig sein soll.

Aufruf: $H := \text{InvBas1}(F, \mathcal{D})$
Eingaben: F endliches Erzeugendensystem des Linksideals I, $0 \notin F$
$\mathcal{D}$ auf T zulässige partielle Division.
Ausgaben: H endliche $\mathcal{D}$-involutive Basis von I.

$H := F$
$\hat{a} := \text{IBTest}(H, \mathcal{D})$
while $\hat{a} \neq 0$ **do**
$H := H \cup \{\hat{a}\}$
$\hat{a} := \text{IBTest}(H, \mathcal{D})$
return(H)

Die Korrektheit ist offensichtlich. Termination ist im allgemeinen leider nicht zu erwarten. Das klassische Beispiel dieses Vorgehens ist die Pommaretmethode (siehe [ZB93], [Ap95b]). Im Zusammenhang mit der Behandlung dieser Methode werden wir in Abschnitt 7.4.2 noch einmal auf InvBas1 zurückkommen.

Bisher fragten wir bei vorgegebenen $\mathcal{D}$ und F nach einer $\mathcal{D}$-involutiven Basis des Linksideals I. Eine Alternative besteht darin, nur F vorzugeben und nach einer $\mathcal{D}$-involutiven Basis des Linksideals I bezüglich einer beliebigen partiellen Division $\mathcal{D}$ zu fragen. Dieser Weg wurde in [Ap96] beschritten.

Aufruf: $(H, \mathcal{D}) := \text{InvBas2}(F)$
Eingaben: F endliches Erzeugendensystem des Linksideals I, $0 \notin F$
Ausgaben: $\mathcal{D}$ partielle Division
H endliche $\mathcal{D}$-involutive Basis von I.

$H := F$
Wähle $\mathcal{D} \in \mathbb{D}_{\text{lpp}(H)}$
$\hat{a} := \text{IBTest}(H, \mathcal{D})$
while $\hat{a} \neq 0$ **do**
$H := H \cup \{\hat{a}\}$
Wähle $\mathcal{D} \in \mathbb{D}_{\text{lpp}(H)}$
$\hat{a} := \text{IBTest}(H, \mathcal{D})$
return$(H, \mathcal{D})$

Die Korrektheit der Methode ist wiederum offensichtlich. Das Terminationsverhalten hängt stark von der Auswahl der partiellen Divisionen $\mathcal{D}$ in den einzelnen Schritten ab. Wir werden in Abschnitt 7.5 näher darauf eingehen. Vorher müssen wir zunächst noch einige Fakten über partielle Potenzproduktdivisionen bereitstellen.

7.4 Partielle Divisionen im Monoid der Potenzprodukte

Wir betrachten den Spezialfall des Monoids $T = T(X)$ der Potenzprodukte in den Unbestimmten $X = \{X_1, \ldots, X_n\}$. Bis auf Isomorphie beziehen sich auch die klassischen Untersuchungen involutiver Systeme im Zusammenhang mit der Lösung von Systemen partieller Differentialgleichungen (siehe [Ja29],[Th37] und [Po78]) auf dieses Monoid. Dabei steht das Potenzprodukt $X_1^{i_1} \cdots X_n^{i_n}$ für die partielle Ableitung $\frac{\partial^{i_1+\cdots+i_n}}{\partial X_1^{i_1} \cdots \partial X_n^{i_n}}$. Janet, Thomas und Pommaret entwickelten jeweils Regeln, in Richtung welcher Variablen die Ableitungen einer Differentialgleichung fortzusetzen sind und in welcher nicht. Auf diese Weise wird für jede Gleichung des Differentialgleichungssystems eine Zerlegung der Variablenmenge X in zwei disjunkte Mengen vorgenommen, wobei eine der beiden Mengen leer sein darf und ihre Vereinigung X ergeben muß. Die Zerlegung hängt in jedem Fall von der höchsten in der Gleichung vorkommenden Ableitung ab. Zusätzlich kann sie aber auch noch von den höchsten Ableitungen aller anderen zum System gehörigen partiellen Differentialgleichungen abhängen. Die höchsten Ableitungen sind nach Übersetzung der partiellen Ableitungen in Potenzprodukte in Bezug auf eine vorgegebene zulässige Termordnung $\prec$ zu bestimmen.

Die Einteilung in fortzusetzende und nicht weiter fortzusetzende Variablen steht in engem Zusammenhang zu einer partiellen Division von T. Sei $\Delta \subset T$ die Menge der zu den höchsten Ableitungen einer endlichen Menge von Differentialgleichungen gehörigen Potenzprodukte. Für $t \in \Delta$ sei $Y_t \subseteq X$ die Menge von Variablen, in deren Richtung die zu t gehörige Gleichung nicht weiter abgeleitet zu werden braucht. Dann beschreibt $(Y_t)_{t\in\Delta}$ eine Äquivalenzklasse partieller Divisionen modulo $\equiv_\Delta$. $(Z_t)_{t\in T}$ mit $Z_t = T$ für alle $t \notin \Delta$ und $Z_t = Y_t$ für alle $t \in \Delta$ erzeugt die bezüglich der Verfeinerungshalbordnung maximale partielle Division dieser Äquivalenzklasse. Die so definierten partiellen Divisionen werden sich immer als zulässig auf Δ erweisen und vereinbart man für die Auswahl der zulässigen partiellen Divisionen, daß stets auf einen fest vorgegebenen Typ, das heißt Janet, Thomas oder Pommaret, zugegriffen werden muß, dann geht Algorithmus InvBas2 gerade in die von Janet, Thomas beziehungsweise Pommaret verwendeten Methoden über. In [Ap96] wurde gezeigt, daß jeder der drei Divisionstypen eine ausgezeichnete Stellung im Verband der partiellen Divisionen einnimmt.

Wir führen die Bezeichungen $\deg(t) = \sum_{j=1}^n i_j$ und $\deg_j(t) = i_j$ für den Totalgrad beziehungsweise den Grad in X_j des Potenzprodukts $t = X_1^{i_1} \cdots X_n^{i_n}$ ein. Für die der Zulässigkeit partieller Divisionen zugrunde liegende Ordnung $\sqsubset$ kann wenigstens für die klassischen involutiven Divisionen stets die reverse lexikographische Ordnung $\lhd$ gewählt werden. Diese ist durch

$$X_1^{i_1} \cdots X_n^{i_n} \lhd X_1^{j_1} \cdots X_n^{j_n} :\Longleftrightarrow \exists 1 \leq k \leq n \; : \; (i_k > j_k \wedge \forall 1 \leq l < k \; : \; (i_l = j_l)) \tag{7.3}$$

definiert.

7.4.1 Zulässigkeitskriterien

Sei $\mathcal{D}$ eine beliebige partielle Division über dem Monoid $T = T(X)$ der Potenzprodukte in X, $\mathfrak{R} = (R, T, \prec, \mathrm{lpp})$ eine effektive Linksgröbnerstruktur der Algebra R von auflösbarem Typ, $I \subseteq R$ ein Linksideal und $F \subset I$ ein endliches Erzeugendensystem. Eine notwendige Voraussetzung dafür, daß F eine $\mathcal{D}$-involutive Basis von I sein kann, ist die Zulässigkeit von $\mathcal{D}$ auf der Menge $\mathrm{lpp}(F)$ der führenden Potenzprodukte von F. Bevor der Test IBTest ausgeführt werden kann, hat dieser Zulässigkeitsnachweis zu erfolgen.

Wir kommen daher zur Entscheidung der Frage $\mathcal{D} \in \mathbb{D}_U$? für eine gegebene partielle Division $\mathcal{D} \in \mathbb{D}_\emptyset$ und eine gegebene endliche Teilmenge $U \subset T$. Außerdem fragen wir nach der Möglichkeit einer konstruktiven Beschreibung der Menge $\mathbb{D}_U$. Die Beantwortung dieser Fragen läßt sich auf einfache Untersuchungen von Potenzproduktidealen in einem Polynomring $S = k[X]$ in den Unbestimmten X über einem beliebigen Körper k zurückführen. Für Ideale $I, J, K \subseteq S$ und Unterpolynomringe $S' = k[Y]$ mit $Y \subseteq X$ vereinbaren wir die abkürzenden Schreibweisen $I + J : K := I + (J : K)$ und $I \circ J \cap S' := (I \circ J) \cap S'$, wobei $\circ$ für eine beliebige Idealoperation steht. Insbesondere schreiben wir $I + J : K \cap S'$ anstelle von $(I + (J : K)) \cap S'$.

Satz 7.7 *Seien $\mathcal{D} = (D_t)_{t \in T}$ die von $(Y_t)_{t \in T}$ erzeugte partielle Division und $(U, \sqsubset)$ eine endliche linear geordnete Menge von Potenzprodukten. Für jedes $t \in U$ erklären wir folgende drei Potenzproduktmengen:*

$$\begin{aligned} A_t &= \{X_i \in X \mid \exists v \in U : (t \sqsubset v \wedge t \in D_v \wedge X_i \notin Y_v)\} \\ B_t &= \{v \in U \mid v \sqsubset t \wedge v \notin \mathrm{Id}_T(t)\} \\ C_t &= \{v \in U \mid v \sqsubset t \wedge D_v \not\subseteq t \circ \langle Y_t \cup \{X_i \in X \mid \deg_i(t) < \deg_i(v)\}\rangle\} \end{aligned} \tag{7.4}$$

Dann sind die folgenden Bedingungen zueinander äquivalent:

i) $\mathcal{D}$ ist zulässig für $(U, \sqsubset)$,

ii) für alle $t \in U$ ist Y_t eine unabhängige Menge des Potenzproduktideals $(A_t) + (B_t) : (t) \subseteq S$,

iii) für alle $t \in U$ ist Y_t eine unabhängige Menge des Potenzproduktideals $(A_t) + (C_t) : (t) \subseteq S$.

Sind alle Mengen Y_t mit $t \in U$ maximal unabhängig für das entsprechende Potenzproduktideal $(A_t) + (B_t) : (t)$, so ist die die Äquivalenzklasse $[\mathcal{D}]_{\equiv_U}$ ein maximales Element von $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$ bezüglich $\leq_{\equiv_U}$.

Ist umgekehrt $[\mathcal{D}]_{\equiv_U}$ ein bezüglich $\leq_{\equiv_U}$ maximales Element von $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$, so sind alle Mengen Y_t mit $t \in U$ maximal unabhängig für $(A_t) + (C_t) : (t)$.

Beweis: *i) $\Rightarrow$ iii)* Sei $\mathcal{D}$ zulässig für $(U, \sqsubset)$. Angenommen, es existieren Potenzprodukte $t \in U$ und $u \in T$ mit $u \in (A_t) + (C_t) : (t) \cap k[Y_t]$. Dann gilt $ut \in D_t$. Würde $u \in (A_t)$ vorliegen, so gäbe es ein Potenzprodukt $v \in U$ mit den Eigenschaften $t \sqsubset v$, $t \in D_v$ und $u \notin \langle Y_v\rangle$. Wir hätten $ut \in D_t \setminus D_v$ und im Widerspruch zu Definition 7.1 könnte weder $D_t \subseteq D_v$ noch $D_v \cap \mathrm{Id}_T(t) = \emptyset$

zutreffen. Also bleibt nur die Möglichkeit $u \in (C_t) : (t)$. Somit gilt $ut \in (C_t)$ und nach Konstruktion von C_t muß ein $v \in U$ mit den Eigenschaften $v \sqsubset t$, $D_v \not\subseteq t \circ \langle Y_t \cup \{X_i \in X \mid \deg_i(t) < \deg_i(v)\}\rangle$ sowie $ut \in \mathrm{Id}_T(v)$ existieren. Also weder $D_t \cap \mathrm{Id}_T(v) = \emptyset$ noch $D_v \subseteq D_t$ im Widerspruch zu Definition 7.1. Folglich war bereits die Annahme der Existenz eines Potenzproduktes in irgendeinem der Durchschnitte $(A_t) + (C_t) : (t) \cap k[Y_t]$ mit $t \in U$ falsch und wir sind fertig.

iii) $\Rightarrow$ *ii)* Diese Beweisrichtung ist wegen der offensichtlichen Gültigkeit der Beziehung $B_t \subseteq C_t$ für alle $t \in U$ trivial.

ii) $\Rightarrow$ *i)* Wir setzen voraus, daß für alle $t \in U$ die Relation $(A_t) + (B_t) : (t) \cap k[Y_t] = \{0\}$ gilt. Seien t und v beliebige Potenzprodukte aus U mit $v \sqsubset t$. Wir untersuchen den Durchschnitt $D_t \cap \mathrm{Id}_T(v)$. Beginnen wir mit dem Fall $v \notin \mathrm{Id}_T(t)$. Dann gilt $v \in B_t$ und somit $\frac{kgV(t,v)}{t} \in (B_t) : (t)$. Demzufolge haben wir $\frac{kgV(t,v)}{t} \notin \langle Y_t \rangle$ und folglich $kgV(t,v) \notin D_t$. Es ergibt sich $w \notin D_t$ für alle $w \in \mathrm{Id}_T(kgV(t,v))$ und demzufolge $D_t \cap \mathrm{Id}_T(v) = \emptyset$. Betrachten wir nun die noch verbleibende Möglichkeit $v \in \mathrm{Id}_T(t)$. Angenommen, es existiert ein Potenzprodukt $w \in D_t \cap \mathrm{Id}_T(v)$. Aus $\frac{w}{t} \in \langle Y_t \rangle$ und $\frac{v}{t} \mid \frac{w}{t}$ schließen wir auf die Gültigkeit von $\frac{v}{t} \in \langle Y_t \rangle$. Somit gilt $v \in D_t$ und aus der Konstruktion von A_v ergibt sich die Inklusion $X \setminus Y_t \subseteq A_v$. Mit $(A_v) + (B_v) : (v) \cap k[Y_v] = \{0\}$ erhalten wir $Y_v \subseteq Y_t$ und daher $D_v \subseteq D_t$. Damit ist nachgewiesen, daß für beliebige $v, t \in U$ eine der beiden möglichen Zulässigkeitsbedingungen partieller Divisionen zutrifft.

Kommen wir nun zum Beweis der hinreichenden und der notwendigen Bedingung für die Maximalität von $[\mathcal{D}]_{\equiv_U}$.
Für alle $t \in U$ seien die Bedingungen $(A_t) + (B_t) : (t) \cap k[Y_t] = \{0\}$ sowie $(A_t) + (B_t) : (t) \cap k[Z] \supsetneq \{0\}$ für alle echten Obermengen $Y_t \subsetneq Z \subseteq X$ erfüllt.

Angenommen, es gäbe eine echte Verfeinerung $\mathcal{D}' \in \mathbb{D}_{(U,\sqsubset)}$ mit $[\mathcal{D}]_{\equiv_U} <_{\equiv_U} [\mathcal{D}']_{\equiv_U}$. Seien $(Y'_t)_{t\in T}$ das Erzeugendensystem von $\mathcal{D}'$ und A'_t sowie B'_t die zu D' gehörigen Potenzproduktmengen der in (7.4) beschriebenen Gestalt. $v \in U$ sei ein Potenzprodukt von minimalem Grad, für welches die echte Inklusion $Y_v \subsetneq Y'_v$ vorliegt. Da v von minimalem Grad gewählt war, gilt für alle zu U gehörigen Teiler w von v die Gleichheit $Y_w = Y'_w$ und somit $A_v = A'_v$. Die Definition der Mengen B_v hängt nicht von $\mathcal{D}$ ab, also $B_v = B'_v$ für alle $v \in U$. Aufgrund der Zulässigkeitannahme für $\mathcal{D}'$ ergibt sich aus dem ersten Teils des Satzes die Gleichheit $(A'_v) + (B'_v) : (v) \cap k[Y'_v] = \{0\}$. Das steht im Widerspruch zu der an $\mathcal{D}$ gestellten Voraussetzung $(A_v) + (B_v) : (v) \cap k[Y'_v] \supsetneq \{0\}$.

Sei nun $\mathcal{D}$ ein bezüglich der Verfeinerungshalbordnung maximales Element der Menge $\mathbb{D}_{(U,\sqsubset)}$. Ziel ist es zu zeigen, daß für alle $t \in U$ und $y \in X \setminus Y_t$ die Unbestimmten $Y_t \cup \{y\}$ eine abhängige Menge des Potenzproduktideals $(A_t) + (C_t) : (t)$ bilden.

Angenommen, es existieren Elemente $t \in U$ und $y \in X \setminus Y_t$ mit $(A_t) + (C_t) : (t) \cap k[Y_t \cup \{y\}] = \{0\}$. Wir bezeichnen die von $(Y'_u)_{u\in T}$, wobei $Y'_t = Y_t \cup \{y\}$ und $Y'_u = Y_u$ für alle $u \neq t$, erzeugte partielle Division mit $\mathcal{D}' = (D'_u)_{u\in T}$. Offensichtlich ist $\mathcal{D}'$ eine echte Verfeinerung von $\mathcal{D}$. Wir werden nun den Nachweis führen, daß $\mathcal{D}'$ ebenfalls zulässig auf der geordneten Menge $(U, \sqsubset)$ ist.

Wir betrachten zwei beliebige Potenzprodukte $u, v \in U$ mit $v \sqsubset u$. Im Falle $t \notin \{u, v\}$ übertragen sich die Relationen $D'_v = D_v \subseteq D_u = D'_u$ oder $D'_u \cap \mathrm{Id}_T(v) = D_u \cap \mathrm{Id}_T(v) = \emptyset$ von $\mathcal{D}$ auf $\mathcal{D}'$.

Sei $v = t$. Offensichtlich zieht die Gültigkeit von $D_u \cap \mathrm{Id}_T(t) = \emptyset$ die von $D'_u \cap \mathrm{Id}_T(t) = D_u \cap \mathrm{Id}_T(t) = \emptyset$ nach sich. Es verbleibt die Untersuchung des Falls $D_t \subseteq D_u$. Aus $X \setminus Y_u \subseteq A_t$ und $(A_t) \cap k[Y_t \cup \{y\}] = \{0\}$ können wir $y \in Y_u$ schlußfolgern. Daher gilt $D'_t \subseteq D_u = D'_u$.

Schließlich bleibt noch die Untersuchung des Falls $u = t$. Falls $D_v \subseteq D_t$ vorliegt, so folgt sofort $D'_v = D_v \subseteq D_t \subset D'_t$. Im verbleibenden Fall $D_t \cap \mathrm{Id}_T(v) = \emptyset$ unterscheiden wir zwei Unterfälle.
a) Sei $v \in C_t$. Aus $(C_t) : (t) \cap k[Y_t \cup \{y\}] = \{0\}$ folgt $tw \notin (C_t) \supseteq (v)$ für alle $w \in \langle Y_t \cup \{y\}\rangle$. Somit $D'_t \cap \mathrm{Id}_T(v) = \emptyset$.
b) Sei nun $v \notin C_t$. Im Fall $D'_t \cap \mathrm{Id}_T(v) \neq \emptyset$ muß $\{X_i \mid \deg_i(t) < \deg_i(v)\} \subseteq Y_t \cup \{y\}$ gelten. Folglich $D'_v = D_v \subseteq t \circ \langle Y_t \cup \{X_i \mid \deg_i(t) < \deg_i(v)\}\rangle \subseteq t \circ \langle Y_t \cup \{y\}\rangle = D'_t$.

Zusammenfassend haben wir gezeigt, daß die Annahme der Existenz von Elementen $t \in U$ und $y \in X \setminus Y_t$ mit $(A_t) + (C_t) : (t) \cap k[Y_t \cup \{y\}] = \{0\}$ im Widerspruch zur vorausgesetzten Maximalität von $\mathcal{D}$ die Existenz einer ebenfalls auf $(U, \sqsubset)$ zulässigen echten Verfeinerung $\mathcal{D}'$ von $\mathcal{D}$ nach sich zieht. □

Wir weisen darauf hin, daß die angegebene hinreichende Bedingung für die Maximalität von $[\mathcal{D}]_{\equiv_U}$ nicht notwendig und die angegebene notwendige Bedingung nicht hinreichend ist. Die erste Aussage erkennt man an folgendem einfachen Beispiel. Sei $t_1 = X_1^2 \sqsubset t_2 = X_2 \sqsubset t_3 = X_1$ die Anordnung der Elemente von U und $\mathcal{D}$ die von $Y_{t_1} = \{X_1, X_2\}$, $Y_{t_2} = \{X_2\}$ sowie $Y_{t_3} = \emptyset$ bis auf U-Äquivalenz erzeugte partielle Division. Durch Nachrechnen überzeugt man sich von der Zulässigkeit von $\mathcal{D}$ auf $(U, \sqsubset)$. Obwohl $(A_{t_3}) + (B_{t_3}) : (t_3) = (X_2)$ die unabhängige Menge X_1 aufweist und Y_{t_3} damit nicht maximal ist, kann $\mathcal{D}$ trotzdem nicht verfeinert werden, ohne die Zulässigkeit der partiellen Division zu verlieren. Zur zweiten Aussage betrachten wir die Anordnung $t_1 = X_1X_2^2X_3 \sqsubset t_2 = X_1^2X_2X_4 \sqsubset t_3 = X_1X_2$. $Y_{t_1} = \{X_1, X_2, X_3, X_4\} = X$, $Y_{t_2} = \{X_1, X_2, X_4\}$, $Y_{t_3} = \{X_3, X_4\}$ beschreibt bis auf U-Äquivalenz eine auf $(U, \sqsubset)$ zulässige partielle Division $\mathcal{D}$. Es gilt $(A_{t_3}) + (C_{t_3}) : (t_3) = (X_2X_3, X_1X_4)$ und Y_{t_3} ist maximale unabhängige Menge dieses Ideals. Ebenso sind Y_{t_2} und Y_{t_1} maximal unabhängig für die entsprechenden Ideale. Dennoch erzeugt auch $Y'_{t_1} = Y_{t_1}$, $Y'_{t_2} = Y_{t_2}$, $Y'_{t_3} = \{X_1, X_2, X_3, X_4\}$ eine auf $(U, \sqsubset)$ zulässige partielle Division, welche $\mathcal{D}$ offensichtlich verfeinert.

Bedingung *ii)* erlaubt das geradlinige Generieren der Menge $\mathbb{D}_U / \equiv_U$ aller auf U zulässigen partiellen Divisionen für beliebige endliche Mengen U. Wir beginnen zunächst mit der Berechnung von $\mathbb{D}_{(U,\sqsubset)} / \equiv_U$ für eine feste lineare Ordnung $\sqsubset$ der endlichen Menge U. Der Funktionsname PARTDIVORD steht für zulässige partielle Divisionen auf geordneten Mengen. Eine endliche Familie $Y = (Y_t)_{t \in U}$, wobei $Y_t \subseteq X$, kann als Erzeugendensystem einer Äquivalenzklasse $[\mathcal{D}]_{\equiv_U}$ modulo der U-Äquivalenz $\equiv_U$ aufgefaßt werden.

Aufruf: $\mathbb{D} :=$ PARTDIVORD(U, Y, j)
Eingaben: $U = \{u_1, \ldots, u_m\} \subset T$
$Y = (Y_{u_i})_{u_i \in U_{j-1}}$, $Y_{u_i} \subseteq X$ $(1 \leq i < j)$, $\mathcal{D} \in \mathbb{D}_{(U_{j-1}, \sqsubset)}$

$j \in \{1, 2, \ldots, m, m+1\}$
Ausgaben: $\mathbb{D} = \{[\mathcal{D}]_{\equiv_U}\}$ falls $j = m+1$
$\mathbb{D} = \left\{[\mathcal{C}]_{\equiv_U} \in \mathbb{D}_{(U,\sqsubset)} / \equiv_U \mid \mathcal{C} \equiv_{U_{j-1}} \mathcal{D}\right\}$ sonst.

Die in der Spezifikation verwendeten Bezeichnungen U_l und $\sqsubset$ sind durch $U_l = \{u_i \mid i = 1, \ldots, l\}$ beziehungsweise $u_i \sqsubset u_l \Longleftrightarrow i > l$ erklärt. $\mathcal{D}$ bezeichnet einen beliebigen Repräsentanten der von der Eingabefamilie Y erzeugten Äquivalenzklasse modulo $\equiv_{U_{j-1}}$. Die Elemente der Ausgabemenge werden durch endliche Erzeugendensysteme dargestellt.

if $j = m+1$ **then return**$(\{Y\})$
$\mathbb{D} := \emptyset$
$i := j - 1$
while $i > 0$ und $u_j \notin u_i \circ \langle Y_{u_i} \rangle$ **do** $i := i - 1$
if $i > 0$ **then** $A := X \backslash Y_{u_i}$ **else** $A := \emptyset$
$B := \left\{ \frac{kgV(u_l, u_j)}{u_j} \mid u_j \nmid u_l \wedge j < l \leq m \right\}$
for each $Z \subseteq X$ **such that** $(A) + \sqrt{(B)} \cap k[Z] = \{0\}$ **do**
    $Y_{u_j} := Z$, $Y := (Y_{u_i})_{u_i \in U_j}$
    $\mathbb{D} := \mathbb{D} \cup$ PartDivOrd$(U, Y, j+1)$
return$(\mathbb{D})$

Der Aufruf von PartDivOrd mit den Parametern $U = \{u_1, \ldots, u_m\}$, der leeren Familie Y und $j = 1$ berechnet gerade die Menge $\mathbb{D}_{(U,\sqsubset)} / \equiv_U$, wobei jedes Element der Menge durch ein endliches Erzeugendensystem beschrieben wird. Es besteht eine natürliche Bijektion zwischen den Mengen der linearen Ordnungen und der Permutationen der Menge U. Durch Umnumerieren der Potenzprodukte läßt sich mit Hilfe der Funktion PartDivOrd zu jeder linearen Ordnung $\sqsubset_\pi$ von U die Menge $\mathbb{D}_{(U,\sqsubset_\pi)} / \equiv_U$ berechnen. Durch Vereinigung der endlich vielen auf diese Weise gewonnenen Mengen berechnet man schließlich die Menge $\mathbb{D}_U / \equiv_U$ aller auf U zulässigen partiellen Divisionen. Im Anschluß an Definition 7.1 stellten wir fest, daß es im Falle der Existenz zweier Potenzprodukte $u_i, u_l \in U$ mit $u_l \sqsubset u_i$ und $u_l \mid u_i$ keine auf $(U, \sqsubset)$ zulässige partielle Division geben kann. Der Algorithmus trägt dem dadurch Rechnung, daß die Menge B beim Versuch der zulässigen Erweiterung auf die Menge $\{u_j \in U \mid u_i \sqsubseteq u_j\}$ das Potenzprodukt 1 enthält. Damit ist jede Teilmenge $\emptyset \subseteq Z \subseteq X$ abhängig für $(A) + \sqrt{(B)}$ und wie erwartet, wird keine zulässige partielle Division gefunden.

Kommen wir zum Nachweis, daß der Algorithmus den an die Funktion PartDivOrd gestellten Anforderungen genügt. Zunächst einmal überzeugt man sich leicht von der Termination des Algorithmus und der Berechenbarkeit aller Teilschritte. Im Fall $j = m+1$ ist die Gültigkeit der Ausgabespezifikationen offensichtlich. Der Korrektheitsbeweis im Fall $1 \leq j \leq m$ basiert auf der Äquivalenz der Bedingungen *i)* und *ii)* aus Satz 7.7.

Für $1 \leq l < j$ stimmen die in Satz 7.7 eingeführten Potenzproduktmengen A_{u_l} und B_{u_l} aller in der Ausgabemenge enthalten partiellen Divisionen mit denen der durch die Eingabefamilie Y erzeugten partiellen Division überein. Man beachte, für das Gleichbleiben der Mengen A_{u_l} ist die Eigenschaft, daß das

neu hinzugenommene Element u_j bezüglich $\sqsubset$ kleiner als alle bisherigen Potenzprodukte ist, bedeutsam. Da auch die jeweiligen Erzeugendensysteme Y_{u_l} unverändert bleiben, überträgt sich die Gültigkeit der in Satz 7.7*(ii)* formulierten Zulässigkeitsbedingung von der Ein- auf die Ausgabe. Als nächstes werden wir nachweisen, daß die beim rekursiven Aufruf von PARTDIVORD übergebenen Argumente ebenfalls den Eingabespezifikationen genügen. Falls dieser Nachweis gelingt, so folgt mittels vollständiger Induktion über $m - j$ die Zulässigkeit der Elemente der Ausgabemenge auf ganz $(U, \sqsubset)$.

Seien also U, Y und $j + 1$ die an PARTDIVORD übergebenen Argumente. $\mathcal{D}$ bezeichne einen Repräsentanten der von Y erzeugten Restklasse partieller Divisionen modulo $\equiv_{U_j}$. Wir haben die Gültigkeit von $(A_{u_j}) + (B_{u_j}) : (u_j) \cap k[Y_{u_j}] = \{0\}$ für die zu $\mathcal{D}$ gehörigen Mengen A_{u_j}, B_{u_j} und Y_{u_j} zu zeigen. Wenn u_j kein $\mathcal{D}$-Vielfaches eines Potenzproduktes mit Index kleiner j ist, so wurde der Variablen A vor dem entsprechenden Unteraufruf der Wert $\emptyset$ zugewiesen. Andernfalls hatte A das Komplement der Menge Y_{u_i}, wobei u_i der bezüglich $\sqsubset$ kleinste $\mathcal{D}$-Teiler von u_j ist, als Wert. $A \subseteq A_{u_j}$ ist offensichtlich. Überlegen wir uns nun, daß zwangsläufig Gleichheit gelten muß. Angenommen, u_j ist $\mathcal{D}$-Vielfaches zweier verschiedener Elemente $u_i \sqsubset u_{i'}$. Dann sind die Mengen der $\mathcal{D}$-Vielfachen von u_i und $u_{i'}$ nicht disjunkt und aus der Eingabespezifikation der rufenden Instanz läßt sich $u_i \circ \langle Y_{u_i} \rangle \subset u_{i'} \circ \langle Y_{u_{i'}} \rangle$ ableiten. Insbesondere gelten damit $Y_{u_i} \subseteq Y_{u_{i'}}$ und $X \setminus Y_{u_{i'}} \subseteq A$. Die vor dem Unteraufruf gebildete Menge B ist ein Erzeugendensystem des Ideals $(B_{u_j}) : (u_j)$, also ist $\sqrt{(B)}$ das Radikalideal von $(B_{u_j}) : (u_j)$. Eine Menge Z ist genau dann unabhängige Menge für $(A_{u_j}) + (B_{u_j}) : (u_j)$, wenn es unabhängige Menge von $(A) + \sqrt{(B)}$ ist. Folglich ist $\mathcal{D}$ auf $(U_j, \sqsubset)$ zulässig.

Gemäß der obigen Überlegungen haben wir damit gezeigt, daß jedes Element der Ausgabemenge auf $(U, \sqsubset)$ zulässig ist. Da Z in jedem Schritt des Algorithmus alle unabhängigen Mengen von $(A) + \sqrt{(B)}$ durchläuft, sind umgekehrt auch alle auf $(U, \sqsubset)$ zulässigen und zur Eingabe U_{j-1}-äquivalenten partiellen Divisionen Element der Ausgabemenge. □

Der beschriebene Algorithmus zur Konstruktion der auf $(U, \sqsubset)$ zulässigen partiellen Divisionen arbeitet rekursiv über der Mächtigkeit von U. Die Ordnung $\sqsubset$ sei so beschaffen, daß kein Element von U ein größeres teilt. Dann wird durch die Hinzunahme der Potenzprodukte in absteigender Ordnung erreicht, daß stets zulässige Erweiterungen existieren und daß kein Überprüfen der Zulässigkeitsbedingungen für bereits früher hinzugefügte Potenzprodukte erforderlich ist. Würde man bei jeder Hinzunahme eines weiteren Potenzprodukts immer nur die maximalen unabhängigen Mengen Z betrachten, also nur die maximalen Elemente der Menge $\left\{ [\mathcal{C}]_{\equiv_{U_j}} \in \mathbb{D}_{(U_j,\sqsubset)} / \equiv_{U_j} \mid \mathcal{C} \equiv_{U_{j-1}} \mathcal{D} \right\}$ berechnen, so würde man letztendlich nur maximale Elemente von $\mathbb{D}_{(U,\sqsubset)} / \equiv_U$ erhalten. Allerdings werden auf diese Weise nicht alle maximalen auf $(U, \sqsubset)$ zulässigen partiellen Divisionen generiert und daher kann nicht auf die Berücksichtigung nicht maximaler unabhängiger Mengen Z verzichtet werden.

Den maximalen Elementen von $\mathbb{D}_{(U,\sqsubset)} / \equiv_U$ kommt eine besondere Bedeutung zu. Beispielsweise sei an die Aussage zu Beginn von Abschnitt 7.2 erinnert, wonach eine $\mathcal{D}$-involutive Basis auch $\mathcal{C}$-involutive Basis für jede zulässige Verfei-

nerung $\mathcal{C}$ von $\mathcal{D}$ ist. Die Wahrscheinlichkeit dafür, daß ein Ideal überhaupt eine involutive Basis besitzt, ist somit für maximale zulässige partielle Divisionen besonders hoch. Auch ist der Aufwand der Testfunktion IBTest im Fall $\mathcal{D} < \mathcal{C}$ für $\mathcal{C}$ höchstens so groß wie für $\mathcal{D}$. Später werden wir noch sehen, daß die zusätzliche Forderung der Maximalität in den Auswahlschritten $\mathcal{D} \in \mathbb{D}_{\mathrm{lpp}(H)}$ die Termination von Algorithmus InvBas2 garantiert. Schließlich ist es bei Kenntnis aller maximalen Elemente von $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$ problemlos möglich, die gesamte Menge zu erzeugen. Aus all diesen Gründen liegt es nahe, für eine gegebene endliche linear geordnete Potenzproduktmenge $(U,\sqsubset)$ und eine gegebene auf $(U,\sqsubset)$ zulässige partielle Division $\mathcal{D}$ danach zu fragen, ob *a)* $[\mathcal{D}]_{\equiv_U}$ ein maximales Element der Menge $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$ ist und *b)* wie eine maximale zulässige Verfeinerung $\mathcal{C} \in \mathbb{D}_{(U,\sqsubset)}$ von $\mathcal{D}$ berechnet werden kann. Beide Aufgaben sind aufgrund der Endlichkeit von $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$ prinzipiell lösbar. Aussage *iii)* aus Satz 7.7 bietet die Möglichkeit der Schaffung schneller Algorithmen zur suboptimalen Lösung beider Fragestellungen. Wir nennen die von $(Y_t)_{t\in T}$ erzeugte Restklasse $[\mathcal{D}]_{\equiv_U}$ *submaximal* in $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$, falls die Mengen Y_t für alle $t \in U$ maximal unabhängig für die in Satz 7.7 definierten Potenzproduktideale $(A_t)+(C_t):(t)$ sind. Es folgt ein Algorithmus zur Berechnung submaximaler Verfeinerungen zulässiger partieller Divisionen.

Aufruf: $Z :=$ SubMaxVerf(Y,U)
Eingaben: $Y = (Y_{u_i})_{u_i\in U}$ Erzeugendensystem von $[\mathcal{D}]_{\equiv_U} \in \mathbb{D}_{(U,\sqsubset)}/\equiv_U$
$U = \{u_1,\ldots,u_m\} \subset T$, geordnet vermöge $u_m \sqsubset u_{m-1} \sqsubset \cdots \sqsubset u_1$
Ausgaben: $Z = (Z_{u_i})_{u_i\in U}$ Erzeugendensystem von $[\mathcal{C}]_{\equiv_U}$ mit
$[\mathcal{D}]_{\equiv_U} \leq_{\equiv_U} [\mathcal{C}]_{\equiv_U}$ und $[\mathcal{C}]_{\equiv_U}$ submaximal in $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$

Z := Y
for $i := 1$ **to** m **do**
  $j := i-1$
  while $j > 0$ und $u_i \notin u_j \circ \langle Z_{u_j}\rangle$ **do** $j := j-1$
  if $j > 0$ **then** $A := X \backslash Z_{u_j}$ **else** $A := \emptyset$
  $C := \{\frac{kgV(u_i,u_r)}{u_i} \mid i < r \leq m \quad \wedge$
    $u_r \circ \langle Z_{u_r}\rangle \not\subset u_i \circ \langle Z_{u_i} \cup \{X_l \mid \deg_l(u_i) < \deg_l(u_r)\}\rangle\}$
  while $\exists y \in X \setminus Z_{u_i} : (A) + \sqrt{(C)} \cap k[Z_{u_i} \cup \{y\}] = \{0\}$ **do**
    $W :=$ maximale Menge mit den Eigenschaften
      $(A) + \sqrt{(C)} \cap k[W] = \{0\}$ und $Z_{u_i} \subseteq W$
    $Z_{u_i} := W$
    $C := \{\frac{kgV(u_i,u_r)}{u_i} \mid i < r \leq m \quad \wedge$
      $u_r \circ \langle Z_{u_r}\rangle \not\subset u_i \circ \langle Z_{u_i} \cup \{X_l \mid \deg_l(u_i) < \deg_l(u_r)\}\rangle\}$
$Z := \left(Z_{u_j}\right)_{u_j\in U}$
return(Z)

Die Termination des Algorithmus ist offensichtlich. Jeder Schritt der Berechnungsvorschrift ist berechenbar. Überzeugen wir uns nun von der Korrektheit des Algorithmus. Wir zeigen, daß die Familie Z zu jedem Zeitpunkt eine auf $(U,\sqsubset)$ zulässige Verfeinerung von $\mathcal{D}$ erzeugt. Bei Initialisierung von Z ist die

Bedingung nach Eingabespezifikation erfüllt. Jeder elementare Verfeinerungsschritt besteht im Vergrößern einer der Variablenmengen Z_{u_i} zu einer Menge W mit $(A) + \sqrt{(C)} \cap k[W] = \{0\}$. Ähnlich wie beim vorangegangenen Algorithmus zeigt man $\forall V \subseteq X \ : \ (A) + \sqrt{(C)} \cap k[V] = \{0\} \Longleftrightarrow (A_{u_i}) + (C_{u_i}) : (u_i) \cap k[V] = \{0\}$, wobei A_{u_i} und C_{u_i} die zu Z gehörigen Potenzproduktmengen aus Satz 7.7 sind. Durch Anwendung der Argumente aus dem letzten Teil des Beweises von Satz 7.7 erhält man schließlich, daß die Zulässigkeit der von Z erzeugten partiellen Division bei Ersetzen von Z_{u_i} durch W bestehen bleibt.

Nun muß noch die Submaximalität der von Z erzeugten partiellen Division nachgewiesen werden. Aus der Zulässigkeit folgt, daß zu jedem Zeitpunkt für alle $j = 1, \ldots, m$ die Beziehung $(A_{u_j}) + (C_{u_j}) : (u_j) \cap k[Z_{u_j}] = \{0\}$ gilt. Unmittelbar nach dem i-ten Durchlauf der **for**-Schleife gilt darüberhinaus die echte Inklusion $(A_{u_i}) + (C_{u_i}) : (u_i) \cap k[Z_{u_i} \cup \{y\}] \supsetneqq \{0\}$ für alle $y \in X \setminus Z_{u_i}$. Dabei ist zu beachten, daß die in der zweiten **while**-Schleife vorgenommene iterierte Vergrößerung von Z_{u_i} tatsächlich erforderlich ist, da das Vergrößern von Z_{u_i} zu einer Verkleinerung der Menge C_{u_i} führen kann. Infolgedessen ist W nicht notwendigerweise maximale unabhängige Menge des zur verfeinerten partiellen Division gehörigen Ideals $(A'_{u_i}) + (C'_{u_i}) : (u_i)$. Wir werden nun zeigen, daß die am Ende des i-ten Durchlaufs erreichte Maximalität der Menge Z_{u_i} dann aber für den weiteren Verlauf der Berechnung Bestand hat. Ersetzen von Z_{u_i} durch eine Obermenge $W \supseteq Z_{u_i}$ wirkt sich nicht auf die Mengen A_{u_j} mit $j < i$ aus und die Mengen C_{u_j} werden dabei höchstens größer. Folglich gilt $(A_{u_j}) + (C_{u_j}) : (u_j) \subseteq (A'_{u_j}) + (C'_{u_j}) : (u_j)$, wobei sich die ungestrichenen Mengen auf die partielle Division vor dem i-ten Durchlauf und die gestrichenen Mengen auf die verfeinerte Division nach dem i-ten Durchlauf der **for**-Schleife beziehen. Somit impliziert $(A_{u_j}) + (C_{u_j}) : (u_j) \cap k[V] \supsetneqq \{0\}$ erst recht $(A'_{u_j}) + (C'_{u_j}) : (u_j) \cap k[V] \supsetneqq \{0\}$. Also sind nach dem i-ten Durchlauf der **for**-Schleife alle Mengen Z_{u_j} mit $1 \leq j \leq i$ maximale unabhängige Mengen der entsprechenden Potenzproduktideale. Insbesondere liegt nach dem m-ten Durchlauf Submaximalität vor. □

Ist man an einer maximalen zulässigen Verfeinerung $\mathcal{C}$ einer partiellen Division $\mathcal{D} \in \mathbb{D}_{(U,\sqsubset)}$ interessiert, so kann der Aufwand stark reduziert werden, indem man zunächst eine submaximale Verfeinerung von $\mathcal{D}$ mittels des obigen Algorithmus berechnet und diese dann mit Hilfe kombinatorischer Suche bis hin zur Maximalität verfeinert.

Bei Anwendung von Algorithmus InvBas2 zur Berechnung involutiver Basen werden sich bereits submaximale partielle Divisionen als ausreichend erweisen, um die Termination zu erzwingen. Es wird uns hier jedoch nicht gelingen, einen exakten Aufwandsvergleich zwischen Rechnungen basierend auf submaximalen beziehungsweise maximalen partiellen Divisionen anzustellen. Es sind folgende gegenläufige Tendenzen zu verzeichnen. Ist $\mathcal{D}$ eine maximale und $\mathcal{C} < \mathcal{D}$ eine submaximale partielle Division, so wird der Rechenaufwand der Funktion IBTest bei Verwendung von $\mathcal{D}$ häufig geringer ausfallen als bei Verwendung von $\mathcal{C}$. Außerdem ist die Chance einer positiven Antwort größer. Andererseits kann der Aufwand, um $\mathcal{C}$ maximal zu verfeinern, zu hoch sein, um daraus einen Nutzen zu ziehen. Weiterhin steht die Frage, wie oft die

durch SubMaxVerf berechnete submaximale Verfeinerung bereits maximal ist. Denn nur wenn das in praktischen Anwendungen nicht "zu häufig" der Fall ist, dann kann sich der zusätzliche Aufwand für den anschließenden Maximierungsschritt überhaupt lohnen.

7.4.2 Pommaretdivision

Sei $T = T(X)$ das von $X = \{X_1, \ldots, X_n\}$ frei erzeugte kommutative Monoid und π eine Permutation von $\{1, \ldots, n\}$.

Ein Teiler $u \in T$ von $v \in T$ wird π-*Pommaretteiler* genannt, falls ein $1 \leq i \leq n$ existiert, so daß $u \in T(X_{\pi(1)}, \ldots, X_{\pi(i)})$ und $\frac{v}{u} \in T(X_{\pi(i)}, \ldots, X_{\pi(n)})$ gelten. Entsprechend wird v in diesem Fall als π-*Pommaretvielfaches* von u bezeichnet. Die partielle Division $\mathcal{P} = (P_t)_{t \in T}$, wobei P_t für alle $t \in T$ die Menge aller π-Pommaretvielfachen von t ist, wird π-*Pommaretdivision* genannt. Im Falle der identischen Permutation π werden wir auf die Angabe von π verzichten. Setzen wir von nun an die identische Permutation π voraus. $\lhd$ bezeichnet die in (7.3) definierte reverse lexikographische Ordnung. Das Erzeugendensystem $Y_{\mathcal{P}} = (Y_{\mathcal{P},t})_{t \in T}$ der Pommaretdivision $\mathcal{P}$ ordnet jedem Potenzprodukt der Gestalt $t = X_1^{j_1} \cdots X_i^{j_i}$ mit $j_i > 0$ die Menge $Y_{\mathcal{P},t} = \{X_i, \ldots, X_n\}$ zu. Außerdem gilt $Y_{\mathcal{P},1} = X$. Es folgt eine Reihe wichtiger Eigenschaften der Pommaretdivision.

Lemma 7.8 *Für alle $t \in T$ ist $Y_{\mathcal{P},t}$ eine maximale unabhängige Menge des zur Pommaretdivision gehörigen Potenzproduktideals $(A_t) + (B_t) : (t)$ aus Satz 7.7.*

Beweis: Der Fall $t = 1$ ist wegen $A_1 = B_1 = \emptyset$ trivial. Betrachten wir nun $t = X_1^{j_1} \cdots X_i^{j_i}$ mit $j_i > 0$. Da für alle Teiler u von t die Relation $Y_{\mathcal{P},u} \supseteq \{X_i, \ldots, X_n\}$ gilt, haben wir

$$A_t \subseteq \{X_1, \ldots, X_{i-1}\} \quad . \tag{7.5}$$

Aus Beziehung (7.3) folgt für beliebiges $u \lhd t$ die Existenz eines $1 \leq l \leq n$ mit $\deg_l(u) > \deg_l(t)$ und $\forall 1 \leq j < l \ : \ \deg_j(u) = \deg_j(t)$. Falls u darüberhinaus kein Vielfaches von t ist, so muß außerdem $l < i$ gelten. Daher enthält $\frac{kgV(u,t)}{t}$ für alle $u \lhd t$ mit $t \nmid u$ wenigstens eine der Variablen $X_1, \ldots, X_{i-1}$ und es ergibt sich $(B_t) : (t) \subseteq (X_1, \ldots, X_{i-1})$. Wegen $\left\{ \frac{X_l t}{X_i} \mid l < i \right\} \subset B_t$ folgt sogar die Gleichheit

$$(B_t) : (t) = (X_1, \ldots, X_{i-1}) \quad . \tag{7.6}$$

Aus (7.5) und (7.6) schließen wir auf $(A_t) + (B_t) : (t) = (X_1, \ldots, X_{i-1})$ und $Y_{\mathcal{P},t} = \{X_i, \ldots, X_n\}$ ist die einzige maximale unabhängige Menge von Variablen für dieses Ideal. □

Folgerung 7.9 *Die Pommaretdivision $\mathcal{P}$ ist zulässig auf $(T, \lhd)$ und sie ist ein maximales Element von $\mathbb{D}_{(T,\lhd)}$.*

Beweis: Die Gültigkeit beider Behauptungen folgt unmittelbar aus Satz 7.7 und Lemma 7.8. □

Satz 7.10 *Sei $\sqsubset$ eine beliebige lineare Ordnung von T mit den Eigenschaften $X_1 \sqsubset X_2 \sqsubset \cdots \sqsubset X_n$ und $u \sqsubset v \Longleftrightarrow uw \sqsubset vw$ für alle $u, v, w \in T$. Dann wird jede auf $(T, \sqsubset)$ zulässige partielle Division $\mathcal{D}$ durch die Pommaretdivision $\mathcal{P}$ verfeinert.*

Beweis: Sei $Y = (Y_t)_{t \in T}$ das Erzeugendensystem von $\mathcal{D}$. Angenommen, es existiert ein $u \in T$ mit $Y_u \not\subseteq Y_{\mathcal{P},u}$. Dann muß es $1 \leq j < i \leq n$ mit $X_j \in Y_u$ und $X_i \mid u$ geben. Aus den Eigenschaften von $\sqsubset$ läßt sich die Gültigkeit von $v := X_j \circ \frac{u}{X_i} \sqsubset X_i \circ \frac{u}{X_i} = u$ ableiten. Offensichtlich ist u kein Teiler von v und somit impliziert die Zulässigkeit von $\mathcal{D}$ die Beziehung $u \circ \langle Y_u \rangle \cap \mathrm{Id}_T(v) = \emptyset$. Das steht aber im Widerspruch zu $X_i v = X_j u \in u \circ \langle Y_u \rangle$. □

Satz 7.11 *Die Pommaretdivision ist ein maximales Element der Menge aller auf ganz T zulässigen partiellen Divisionen.*

Beweis: Angenommen, es gäbe eine echte Verfeinerung $\mathcal{D} = (D_t)_{t \in T} \in \mathbb{D}_T$ von $\mathcal{P}$. Wir betrachten ein Potenzprodukt $v \in T$ von minimalem Grad, für welches eine echte Inklusion $P_v \subsetneqq D_v$ besteht. Weiterhin sei $X_i \in X$ eine Unbestimmte mit $X_i v \in D_v \setminus P_v$. Es existiert ein (eindeutig bestimmter) Index j mit $1 \leq i < j \leq n$ und $v \in T(X_1, \ldots, X_j) \setminus T(X_1, \ldots, X_{j-1})$, Insbesondere ist dann v durch X_j teilbar. v ist Pommaretvielfaches und damit erst recht $\mathcal{D}$-involutives Vielfaches von $\frac{v}{X_j}$. Aus der Zulässigkeit von $\mathcal{D}$ auf T ergibt sich $D_v \subset D_{\frac{v}{X_j}}$ und somit $X_i v \in D_{\frac{v}{X_j}}$. Da $\frac{v}{X_j}$ von kleinerem Grad als v ist, liegt die Gleichheit $P_{\frac{v}{X_j}} = D_{\frac{v}{X_j}}$ vor. Aufgrund der Enthaltenseinsbeziehung $X_i v \in P_{\frac{v}{X_j}}$ muß $\frac{v}{X_j} \in T(X_1, \ldots, X_i)$ gelten. Demzufolge ist $X_i v$ Pommaretvielfaches und erst recht $\mathcal{D}$-involutives Vielfaches von $\frac{X_i v}{X_j} \in T(X_1, \ldots, X_i) \subset T(X_1, \ldots, X_j)$. $X_i v$ ist also ein gemeinsames $\mathcal{D}$-involutives Vielfaches von v und $\frac{X_i v}{X_j}$. Wegen $\frac{X_i v}{X_j} \nmid v$ und $v \nmid \frac{X_i v}{X_j}$ steht das im Widerspruch zur Zulässigkeit von $\mathcal{D}$ auf T. □

Die vorangegangenen Sätze unterstreichen die Bedeutung der π-Pommaretdivisionen in der Menge der auf ganz T zulässigen partiellen Divisionen. Man stellt fest, daß die Menge aller partiellen Divisionen $\mathcal{D}$, für die eine mit der Monoidstruktur von T verträgliche lineare Ordnung $\sqsubset$ existiert, so daß $\mathcal{D}$ auf $(T, \sqsubset)$ zulässig ist, genau $n!$ maximale Elemente, nämlich gerade die π-Pommaretdivisionen, besitzt.

Ein Polynomideal besitzt im allgemeinen keine endlichen involutiven Basen vom Pommarettyp (siehe [ZB93]). Aus Satz 7.10 und Bemerkung 7.5 folgt, daß sich diese Eigenschaft wenigstens auf alle die partiellen Divisionen überträgt, die für eine Monoidordnung $\sqsubset$ auf $(T, \sqsubset)$ zulässig sind. In [Ap95b] wurde die Frage nach der Existenz endlicher involutiver Basen vom Pommarettyp diskutiert. Es wurde bewiesen, daß jedes Ideal durch eine Zariski-offene Menge linearer Variablentransformationen in ein Polynomideal mit endlicher Pommaretbasis überführt wird. Mall zeigte, daß die Ideale unter derartigen Variablentransformationen sogar in eine solche Position gebracht werden, in welcher die reduzierte $\mathcal{P}$-involutive Basis mit der reduzierten Gröbnerbasis übereinstimmt (siehe [Mal95]). Außerdem wurde in [Ap95b] nachgewiesen, daß die Berechnungsvorschrift InvBas1 für $\mathcal{D} = \mathcal{P}$ und bei Verwendung einer geeigneten

Auswahlstrategie im Unteralgorithmus IBTest genau im Falle der Existenz endlicher $\mathcal{P}$-involutiver Basen des von F erzeugten Linksideals terminiert.

Aus praktischer Sicht ist die Tatsache, daß jedes Ideal nach generischer linearer Variablentransformation eine durch InvBas1 berechenbare endliche $\mathcal{P}$-Basis besitzt, leider wenig hilfreich. Aufgrund der wenigstens exponentiellen Speicherkomplexität der Algorithmen zur Berechnung involutiver Basen stellen erfolgreiche Anwendungen die Ausnahme dar. Besteht das Erzeugendensystem F aus dichtbesetzten Polynomen, so besteht bereits bei kleinen Graden und Variablenanzahlen kaum noch Aussicht auf Erfolg.

Es existieren auf T zulässige partielle Divisionen, welche durch keine π-Pommaretdivision verfeinert werden. Betrachten wir dazu ein Beispiel. Sei $X = \{X_1, X_2\}$. Wir zerlegen die Menge $T = T(X)$ aller Potenzprodukte in X in drei disjunkte Teilmengen $T_{X_2} = T(X_2)$, $T_{X_1} = X_1 \circ T(X_1)$ und $T_{X_1X_2} = \mathrm{Id}_T(X_1X_2)$. Die Ordnung $\sqsubset$ soll den Bedingungen *i)* $\forall s \in \{X_2, X_1, X_1X_2\}$: $\sqsubset|_{T_s} = \lhd|_{T_s}$ und *ii)* $T_{X_1X_2} \sqsubset T_{X_1} \sqsubset T_{X_2}$, wobei per definitionem $T_s \sqsubset T_u :\Leftrightarrow \forall v \in T_s, w \in T_u \ : \ v \sqsubset w$, genügen. Wir definieren die Mengen $Y_1 = Y_{X_1} = X$, $Y_u = \{X_2\}$ für alle $u \in T_{X_2} \setminus \{1\}$, $Y_v = \{X_1\}$ für alle $v \in T_{X_1} \setminus \{X_1\}$ und schließlich $Y_w = Y_{\mathcal{P}, \frac{w}{X_1X_2}}$ für alle $w \in T_{X_1X_2}$. Dann erzeugt die Familie $Y = (Y_t)_{t \in T}$ eine auf $(T, \sqsubset)$ zulässige partielle Division, welche durch keine Pommaretdivision verfeinert wird. Die Frage, ob es eine auf T zulässige partielle Division $\mathcal{D}$ gibt, so daß jedes Linksideal von R eine endliche $\mathcal{D}$-involutive Basis besitzt, bleibt damit offen. Eine kürzlich von Blinkov und Gerdt beschriebene partielle Division legt die Vermutung der Existenz derartiger $\mathcal{D}$ nahe. Allerdings scheint es, als würde diese Division (Division II aus [GB97]) unseren Zulässigkeitsanforderungen auf T nicht genügen. Unser in Definition 7.1 gegebener Zulässigkeitsbegriff überdeckt möglicherweise nicht die gesamte Bandbreite der in [GB96] axiomatisierten involutiven Divisionen.

Unter Ausnutzung der regulären Gestalt unendlicher reduzierter $\mathcal{P}$-involutiver Basen gelang es in [Ap98], die Methode InvBas1 so durch eine Abbruchbedingung zu ergänzen, daß im Falle des Anhaltens stets eine abgeschnittene $\mathcal{P}$-involutive Basis des von F erzeugten Linksideals I ausgegeben wird. Diese abgeschnittene $\mathcal{P}$-involutive Basis ist bereits Gröbnerbasis von I. Außerdem wird die Methode durch diese Abbruchbedingung algorithmisch, das heißt, die Abarbeitung hält bei beliebiger zulässiger Eingabe an.

7.4.3 Janetdivision

Im Gegensatz zur π-Pommaretdivision ist die π-Janetdivision nicht einfach eine partielle Division im Sinne von Definition 7.1, sondern eine ganze Familie $\iota_\pi = \left(\mathcal{J}_\pi^{(V)}\right)_{V \subseteq T}$ partieller Divisionen mit der Eigenschaft $\mathcal{J}_\pi^{(V)} \in \mathbb{D}_{(V, \sqsubset_\pi)}$ für alle Teilmengen $V \subseteq T$.

Soweit nicht explizit auf das Gegenteil hingewiesen wird, nehmen wir im weiteren an, daß π die identische Permutation ist und verzichten auf die Angabe von π in den Bezeichnungen. Die Verallgemeinerung auf beliebige Permutationen π von $\{1, \ldots, n\}$ ist offensichtlich. $\lhd$ bezeichnet wiederum die in (7.3) definierte reverse lexikographische Ordnung.

Bei festgehaltener Potenzproduktmenge $V \subseteq T$ ordnen wir jedem $v \in V$ die Variablenmenge

$$Y_{\mathcal{J}^{(V)},v} = \left\{ X_i \mid \neg\exists u \in V \ \left(\deg_i u > \deg_i v \wedge \forall 1 \leq j < i \ \deg_j u = \deg_j v\right)\right\}$$

zu. Die *Janetdivision $\mathcal{J}^{(V)}$ über der Trägermenge V* (bezüglich der Ordnung $\lhd$) wird als das bezüglich der Verfeinerungshalbordnung maximale Element der von der Familie

$$Y_{\mathcal{J}^{(V)}} = \left(Y_{\mathcal{J}^{(V)},v}\right)_{v\in V}$$

erzeugten Restklasse partieller Divisionen modulo $\equiv_V$ definiert. Wenn V aus dem Kontext heraus klar ist, dann werden wir die $\mathcal{J}^{(V)}$-involutiven Vielfachen beziehungsweise $\mathcal{J}^{(V)}$-involutiven Teiler von $v \in V$ auch einfach als *Janetvielfache* beziehungsweise *Janetteiler* von v bezeichnen.

Lemma 7.12 *Für alle Teilmengen $V \subseteq T$ ist die Janetdivision $\mathcal{J}^{(V)}$ über der Trägermenge V zulässig auf $(V, \lhd)$. Darüberhinaus sind alle Mengen $J_v^{(V)}$ mit $v \in V$ paarweise disjunkt.*

Beweis: Seien A_v und B_v die in Satz 7.7 eingeführten Mengen von Potenzprodukten. Man überzeugt sich leicht von der Gültigkeit von

$$J_v^{(V)} \cap V = \{v\} \ . \tag{7.7}$$

Damit gilt für alle $v \in V$ die Beziehung $A_v = \emptyset$. Wir halten ein beliebiges $v \in V$ fest. Zu jedem Potenzprodukt $u \in T$, welches in der reversen lexikographischen Ordnung $\lhd$ kleiner als v ist, existiert ein Index $1 \leq i_u \leq n$ mit $\deg_{i_u}(u) > \deg_{i_u}(v)$ und $\deg_j(u) = \deg_j(v)$ für alle $1 \leq j < i_u$. Für $u \in B_v$ ergibt sich $X_{i_u} \notin Y_{\mathcal{J}^{(V)},v}$ und folglich haben wir $t \notin \left\langle Y_{\mathcal{J}^{(V)},v}\right\rangle$ für alle $t \in (B_v) : (v)$. Damit ist $Y_{\mathcal{J}^{(V)},v}$ eine unabhängige Menge des Potenzproduktideals $(A_v) + (B_v) : (v)$ und aus Satz 7.7 erhalten wir die Zugehörigkeit $\mathcal{J}^{(V)} \in \mathbb{D}_{(V,\lhd)}$. Schließlich impliziert Gleichung (7.7), daß die Mengen der Janetvielfachen der Elemente von V paarweise disjunkt sind. □

Wählt man in InvBas2 in jedem Schritt die Janetdivision über der Trägermenge $\mathrm{lpp}(H)$ aus, so erhält man die Janetmethode. Diese besitzt praktische Vorzüge gegenüber der Pommaret- und der unten noch folgenden Thomasmethode, denn einerseits terminiert sie immer und andererseits arbeitet sie relativ effizient, da die Janetdivisionen für eine Vielzahl endlicher Trägermengen V "nahezu maximal" unter allen auf V zulässigen partiellen Divisionen sind. Neben den in Satz 7.7 beschriebenen Mengen A_v, B_v und C_v führen wir für alle $v \in V$ die Menge $L_v = \{v \in V \mid v \lhd u\}$ ein. Mittels ähnlicher Argumente wie im Beweis von Lemma 7.12 zeigt man, daß $Y_{\mathcal{J}^{(V)},v}$ für alle $v \in V$ eine unabhängige Menge des Ideals $(A_v) + (L_v) : (v) = (L_v) : (v)$ ist. Die für praktische Anwendungen günstige Eigenschaft besteht darin, daß $Y_{\mathcal{J}^{(V)},v}$ für eine Vielzahl endlicher Mengen V sogar maximale unabhängige Menge von $(L_v) : (v)$ ist. Das folgende Gegenbeispiel belegt jedoch, daß es sich dabei nicht um eine allgemeingültige Eigenschaft handelt. Sei $V =$

$\{X_1X_3, X_1X_2^2X_4, X_1^2X_2^2\}$. Dann haben wir $Y_{\mathcal{J}^{(V)},X_1X_3} = \{X_3, X_4\}$ und auch die echte Obermenge $\{X_1, X_3, X_4\} \supsetneq Y_{\mathcal{J}^{(V)},X_1X_3}$ ist unabhängig für $(L_{X_1X_3})$: $(X_1X_3) = (X_1X_2^2, X_2^2X_4) = (X_1, X_4) \cap (X_2^2)$. Diese Tatsache berechtigt zur Hoffnung, daß sich InvBas2 gegenüber der Janetmethode noch weiter verbessern läßt. So ist zu vermuten, daß es von Vorteil sein könnte, die Janetdivision über der Trägermenge $\mathrm{lpp}(H)$ mit Hilfe des Algorithmus SubMaxVerf submaximal zu verfeinern. In Abschnitt 7.5 werden wir noch einmal vertieft auf diese Problematik eingehen.

7.4.4 Thomasdivision

Ähnlich der Janetdivision trägt die *Thomasdivision* den Charakter einer Familie $\tau = \left(\mathcal{T}^{(V)}\right)_{V\subseteq T}$ partieller Divisionen. $\mathcal{T}^{(V)}$ wird die *Thomasdivision über der Trägermenge* V genannt. Das Erzeugendensystem ihrer Restklasse modulo $\equiv_V$ wird von den Mengen

$$Y_{\mathcal{T}^{(V)},v} = \{X_i \mid \forall u \in V : \deg_i(u) \leq \deg_i(v)\}$$

gebildet. Im Unterschied zu Pommaret- und Janetdivision hängt die Thomasdivision nicht zusätzlich von einer Variablenpermutation π ab. Zwischen Thomas- und Janetdivision besteht der Zusammenhang

$$\mathcal{T}^{(V)} = \inf_{\pi} \mathcal{J}^{(V,\pi)} ,$$

wobei π sämtliche Permutationen der Menge $\{1, \ldots, n\}$ durchläuft, $\mathcal{J}^{(V,\pi)}$ die π-Janetdivision über der Trägermenge V bezeichnet und inf für die Bildung des Infimums bezüglich der Verfeinerungshalbordnung steht. Aus diesem Zusammenhang folgt unmittelbar $\mathcal{T}^{(V)} \in \mathbb{D}_{(V,\lhd)}$ für alle Potenzproduktmengen $V \subseteq T$ sowie die paarweise Disjunktheit der $\mathcal{T}^{(V)}$-Vielfachenmengen der Elemente von V. Aus den dargelegten Zusammenhängen ist zu vermuten, daß die Thomasmethode bei praktischen Rechnungen Effizienznachteile gegenüber der Janetmethode besitzt. Auf der anderen Seite ist sie aber von entscheidender theoretischer Bedeutung, denn der folgende Satz und das daran anschließende Lemma bilden die Grundlage des Terminationsbeweises einer allgemeinen Variante von Algorithmus InvBas2.

Satz 7.13 *Seien $V \subseteq T$ und $\sqsubset$ eine beliebige lineare Ordnung von V. Dann ist jede submaximale partielle Division $\mathcal{D} \in \mathbb{D}_{(V,\sqsubset)}$ eine Verfeinerung von $\mathcal{T}^{(V)}$.*

Beweis: Für geordnete Mengen $(V, \sqsubset)$, welche Elemente $u \neq v$ mit $v \sqsubset u$ und $v \mid u$ enthalten, ist die Aussage des Satzes wegen $\mathbb{D}_{(V,\sqsubset)} = \emptyset$ trivialerweise richtig.

Im weiteren beschränken wir uns auf die Betrachtung geordneter Mengen $(V, \sqsubset)$, die solche Elemente u und v nicht enthalten. Seien $\mathcal{D} \in \mathbb{D}_{(V,\sqsubset)}$ eine submaximale partielle Division und $Y = (Y_t)_{t\in T}$ ihr Erzeugendensystem. Die Bezeichnungen A_v und C_v beziehen sich auf die zu $\mathcal{D}$ gehörigen Potenzproduktmengen aus Satz 7.7. Aufgrund der Annahmen über $\sqsubset$ enthält C_v

keine Teiler von v und es gilt $(C_v) : (v) \subsetneqq k[X]$. Aus der Definition der Thomasdivision ergibt sich für beliebige $v \in V$ und $X_i \in Y_{\mathcal{T}^{(V)},v}$ die Beziehung $\forall u \in V \ : \ X_i \nmid \frac{kgV(u,v)}{v}$. Folglich besitzt $(C_v) : (v)$ ein Erzeugendensystem aus $k[X \setminus Y_{\mathcal{T}^{(V)},v}]$ und $Y_{\mathcal{T}^{(V)},v}$ ist Teilmenge jeder maximalen unabhängigen Menge Z des Ideals $(C_v) : (v)$.

Betrachten wir nun eine beliebige Variable $X_i \in A_v$ und weisen dafür die Beziehung

$$X_i \notin Y_{\mathcal{T}^{(V)},v} \tag{7.8}$$

nach. Nach Definition von A_v existiert ein $u \in V$ mit $v \sqsubset u$, $v \in D_u$ und $X_i \notin Y_u$. Daraus ergibt sich $u \mid v$ und $\deg_i(u) = \deg_i(v)$. Da v nur endlich viele Teiler besitzt, muß es ein bezüglich $\sqsubset$ größtes u geben, welches die obigen Bedingungen erfüllt. Für dieses größte u gilt $X_i \notin A_u$ und folglich ist $Y_u \cup \{X_i\}$ eine unabhängige Menge des Potenzproduktideals (A_u). Andererseits ist $Y_u \cup \{X_i\}$ wegen der vorausgesetzten Submaximalität von $\mathcal{D}$ eine abhängige Menge von $(A_u) + (C_u) : (u)$. Also muß $Y_u \cup \{X_i\}$ für $(C_u) : (u)$ abhängig sein. Somit enthält V ein Potenzprodukt, welches einen höheren Grad als u und v in X_i aufweist und die Gültigkeit von (7.8) ist bewiesen.

Zusammenfassend haben wir gezeigt, daß für jede maximale unabhängige Menge Z von $(A_v) + (C_v) : (v)$ die Inklusion $Y_{\mathcal{T}^{(V)},v} \subseteq Z$ vorliegt. □

Lemma 7.14 *Sei $\mathcal{D}$ die von $Y = (Y_t)_{t \in T}$ erzeugte partielle Division und $V \subset T$ eine endliche, nicht leere Menge von Potenzprodukten. Weiterhin verfeinere $\mathcal{D}$ die Thomasdivision über der Trägermenge V, das heißt $\mathcal{T}^{(V)} \leq \mathcal{D}$. Dann gilt für alle $v \in V$ und $X_i \in X \setminus Y_v$ die Beziehung*

$$X_i v \mid kgV(V) \, , \tag{7.9}$$

wobei $kgV(V)$ das kleinste gemeinsame Vielfache aller Elemente von V bezeichnet.

Beweis: Wegen $X_i \in X \setminus Y_v \subseteq X \setminus Y_{\mathcal{T}^{(V)},v}$ gibt es ein Potenzprodukt $u \in V$ mit $\deg_i(v) < \deg_i(u)$ und es folgt unmittelbar die Behauptung. □

7.5 Termination der involutiven Methode

Wir kommen nun auf die Untersuchung des Terminationsverhaltens von Algorithmus InvBas2 zurück. Dazu präzisieren wir die Berechnungsvorschrift wie folgt:

$H := \text{Gauss}(F)$
Wähle ein $\mathcal{D} \in \mathbb{D}_{\text{lpp}(H)}$ mit $\mathcal{T}^{(\text{lpp}H)} \leq \mathcal{D}$
$\hat{a} := \text{IBTest}(H, \mathcal{D})$
while $\hat{a} \neq 0$ **do**
    $H := H \cup \{\hat{a}\}$
    Wähle ein $\mathcal{D} \in \mathbb{D}_{\text{lpp}(H)}$ mit $\mathcal{T}^{(\text{lpp}H)} \leq \mathcal{D}$

$\hat{a} := \text{IBTEST}(H, \mathcal{D})$

return$(H, \mathcal{D})$

Die Funktion GAUSS bewirkt eine *Gaussreduktion* der Elemente von F (siehe auch unter *Autoreduktion* in Abschnitt 7.6.2). Darunter ist zu verstehen, daß die Elemente von F als Erzeugendensystem eines Untervektorraums U des $\mathbb{K}$-Vektorraums R aufgefaßt werden. Die Elemente von R werden in der $\mathbb{K}$-Basis T von R dargestellt. Unter einer Gaussreduktion von F verstehen wir die Überführung von F in eine Basis H von U, welche sich relativ zu $(T, \prec)$ in Trapezgestalt befindet. Diese Umformung kann mittels des Gaussschen Algorithmus vorgenommen werden. Das so ermittelte H erzeugt natürlich dasselbe Linksideal I wie F. Außerdem sind die führenden Potenzprodukte der Elemente von H paarweise verschieden.

Es ist offensichtlich, daß der vorbereitende Gaussreduktionsschritt nicht die Korrektheit des Algorithmus INVBAS2 beeinflußt. Der Vorbereitungsschritt ist optional, sein Einbau vereinfacht jedoch die Ausführung der aufgerufenen Unterprogramme IBTEST.

Die entscheidende Änderung an der Berechnungsvorschrift besteht in der Einschränkung der Auswahl von $\mathcal{D}$ durch die zusätzliche Forderung $\mathcal{T}^{(\text{lpp}H)} \leq \mathcal{D}$. Diese sichert die Termination der Abarbeitung des Algorithmus für beliebige endliche Linksidealerzeugendensysteme F.

Terminationsbeweis des modifizierten Algorithmus INVBAS2 Wir stellen ein Lemma voran, welches uns helfen wird, eine wichtige Eigenschaft der Ausgabe von IBTEST nachzuweisen.

Lemma 7.15 *Seien H eine endliche Teilmenge von Null verschiedener Elemente der graduierten Struktur $\mathfrak{R} = (R, T, \prec, \text{lpp})$, $t_0 \in T$, $\mathcal{D}$ die von $Y = (Y_t)_{t \in T}$ erzeugte partielle Division und $\sqsubset$ eine lineare irreflexive Ordnung der Menge $\text{lpp}(H)$ der führenden Potenzprodukte der Elemente von H. Zu jedem $h \in H$ und jedem $y \in X \setminus Y_{\text{lpp}(h)}$ mit $y \circ \text{lpp}(h) \preceq t_0$ existiere ein Element $h' \in H$ mit $\text{lpp}(h') \mid y \circ \text{lpp}(h)$ und $\text{lpp}(h') \sqsubset \text{lpp}(h)$. Dann gilt für alle $t \preceq t_0$ die Äquivalenz*

$$t \in \text{Id}_T(\text{lpp}(H)) \Longleftrightarrow t \in \bigcup_{h \in H} D_{\text{lpp}(h)} \, .$$

Beweis: Die Implikation $\Longleftarrow$ ist trivial. Sei $t \in \text{Id}_T(\text{lpp}(H))$ beliebig und $h \in H$ ein Element mit bezüglich $\sqsubset$ minimalem führenden Potenzprodukt, für welches $\text{lpp}(h) \mid t$ erfüllt ist. Angenommen, t wäre kein $\mathcal{D}$-involutives Vielfaches von $\text{lpp}(h)$. Dann müßte es eine Variable $y \in X$ geben, welche $\frac{t}{\text{lpp}(h)}$ teilt und nicht zu $Y_{\text{lpp}(h)}$ gehört. Nach Voraussetzung existiert somit ein $h' \in H$ mit $\text{lpp}(h') \mid y \circ \text{lpp}(h) \mid t$ und $\text{lpp}(h') \sqsubset \text{lpp}(h)$. Das stellt einen Widerspruch zur Konstruktion von h dar und folglich $t \in D_{\text{lpp}(h)}$. Damit ist auch $\Longrightarrow$ nachgewiesen. □

Folgerung 7.16 *Sei $\hat{a}$ das von Algorithmus* IBTEST *bei Eingabe von F und $\mathcal{D}$ berechnete Element. Falls $\hat{a}$ von Null verschieden ist, so gilt entweder*

i) $\mathrm{lpp}(\hat{a}) \notin \mathrm{Id}_T(\mathrm{lpp}(F))$ *oder*

ii) es existieren $h \in F$ *und* $y \in X \setminus Y_{\mathrm{lpp}(h)}$ *mit* $\mathrm{lpp}(\hat{a}) = y \circ \mathrm{lpp}(h)$.

Beweis: Sei $\hat{a} \neq 0$ und (u, h) das von IBTest zuletzt bearbeitete Paar, also $\hat{a} = \mathrm{Nf}_{\mathcal{D},H}(uh)$, wobei H eine bezüglich Inklusion minimale Teilmenge von F mit der Eigenschaft $\bigcup_{g\in H} D_{\mathrm{lpp}(g)} = \bigcup_{f\in F} D_{\mathrm{lpp}(f)}$ ist. $\mathrm{Nf}_{\mathcal{D},H}(uh)$ gibt den Rest von uh bei $\mathcal{D}$-Division modulo H mittels pDivide$_R$ an. Insbesondere gilt $\mathrm{lpp}(\hat{a}) \notin \bigcup_{g\in H} D_{\mathrm{lpp}(g)}$. Zunächst halten wir fest, daß sich *i)* und *ii)* einander trivialerweise ausschließen.

Der Fall $\mathrm{lpp}(\hat{a}) = u \circ \mathrm{lpp}(h) \notin \bigcup_{g\in H} D_{\mathrm{lpp}(g)}$ zieht nach Konstruktion der Teilmenge H die Ungleichung $u \neq 1$ nach sich. Folglich $u \in X \setminus Y_{\mathrm{lpp}(h)}$ und es liegt Eigenschaft *ii)* vor.

Sei nun $\mathrm{lpp}(\hat{a}) \prec u \circ \mathrm{lpp}(h)$. Die Auswahlstrategie der Paare aus L in Algorithmus IBTest sichert, daß H, $t_0 = \mathrm{lpp}(uh)$ und $\mathcal{D}$ die Voraussetzungen von Lemma 7.15 erfüllen. Daher gilt wegen $\mathrm{lpp}(\hat{a}) \notin \bigcup_{g\in H} D_{\mathrm{lpp}(g)}$ auch die Beziehung $\mathrm{lpp}(\hat{a}) \notin \mathrm{Id}_T(\mathrm{lpp}(H)) = \mathrm{Id}_T(\mathrm{lpp}(F))$, also Eigenschaft *i)*. □

Nunmehr sind alle für den Terminationsbeweis erforderlichen Aussagen bereitgestellt. H_ν bezeichne den Wert der Variablen H vor Ausführung des ν-ten Durchlaufs der **while**-Schleife. Dann ist $\mathrm{Id}_T(\mathrm{lpp}(H_1)) \subseteq \mathrm{Id}_T(\mathrm{lpp}(H_2)) \subseteq \cdots \subseteq \mathrm{Id}_T(\mathrm{lpp}(H_\nu)) \subseteq \cdots$ eine aufsteigende Kette von Monoididealen von T. Da T noethersch ist, muß diese Kette stationär werden, sagen wir bei ν_0, also $\mathrm{Id}_T(\mathrm{lpp}(H_\nu)) = \mathrm{Id}_T(\mathrm{lpp}(H_{\nu_0}))$ für alle $\nu \geq \nu_0$. Ab dem ν-ten Schleifendurchlauf werden somit nur noch Elemente $\hat{a}_\nu$ zum Erzeugendensystem hinzugenommen, die in Bezug auf die aktuellen Werte von H und $\mathcal{D}$ die Eigenschaft *ii)* aus Folgerung 7.16 aufweisen. Wegen $\mathcal{T}^{(\mathrm{lpp}H)} \leq \mathcal{D}$ folgt daraus mit Hilfe von Lemma 7.14 für alle $\nu \geq \nu_0$ die Gleichheit

$$kgV\,(\mathrm{lpp}(H_\nu)) = kgV\,(\mathrm{lpp}(H_{\nu_0}))\ .$$

Daraus können wir schließen, daß die Folge $H_1, H_2, \ldots$ nach endlicher Zeit abbrechen muß und InvBas2 terminiert. □

7.6 Verbesserungen der involutiven Methode

Es ist wohlbekannt, daß Zeit- und Speicherverhalten des Buchbergeralgorithmus in hohem Maße von Auswahl- und Reduktionsstrategien sowie der Anwendung von Kriterien zum Erkennen unnötiger Reduktionen abhängen (siehe zum Beispiel [Bu79],[Bu85],[GM88] und [G&91]).

Völlig analog verhält es sich mit dem Algorithmus zur Berechnung involutiver Basen. Dem heutigen Standard der Implementationen des Buchbergeralgorithmus sind Jahrzehnte experimenteller Untersuchungen vorausgegangen, um geeignete Heuristiken für die Festlegungen der Strategien zu finden. Diese Phase der Entwicklung steht dem Algorithmus zur Berechnung involutiver Basen erst noch bevor. Heute wird sich eine Implementierung zunächst einmal a priori an den Heuristiken des Buchbergeralgorithmus orientieren. Eine wesentliche Neuheit besteht jedoch in der Notwendigkeit der Auswahl einer geeigneten partiellen

Division nach jeder Erweiterung des Erzeugendensystems. Wir konzentrieren uns auf die Untersuchung dieser Problematik und reißen danach noch einige vom Buchbergeralgorithmus übernommene Strategien an.

7.6.1 Auswahl der partiellen Division

Wir lassen uns bei der Auswahl einer geeigneten partiellen Division von folgenden Zielen leiten. *i)* Die Wahrscheinlichkeit, daß die Zwischenbasis H bereits eine $\mathcal{D}$-involutive Linksidealbasis ist, sollte möglichst groß sein. *ii)* Der Test IBTest$(H,\mathcal{D})$ zur Feststellung dieses Sachverhalts sollte möglichst geringen Aufwand verursachen. *iii)* Nach dem Komplettieren der Zwischenbasis durch Hinzunahme von $\hat{a}$ sollten möglichst viele der getesteten Nullreduktionen für den anschließenden Test mit der erweiterten Linksidealbasis Bestand haben.

Seien $\mathcal{D}$ und $\mathcal{C}$ zwei auf $\mathrm{lpp}(H)$ zulässige partielle Divisionen mit $\mathcal{T}^{(\mathrm{lpp}H)} \leq \mathcal{C} \leq \mathcal{D}$. Gemäß Bemerkung 7.5 (*ii*) ist H erst recht eine $\mathcal{D}$-involutive Basis, wenn es eine $\mathcal{C}$-involutive Basis ist. Vergleichen wir nun den für die Ausführung von IBTest erforderlichen Aufwand beim Test von H auf die Eigenschaft, $\mathcal{D}$-involutive beziehungsweise $\mathcal{C}$-involutive Basis zu sein. $H_\mathcal{D}$ bezeichne die minimale Teilmenge von H mit der Eigenschaft, daß $\bigcup_{h\in H_\mathcal{D}} D_{\,\mathrm{lpp}(h)} = \bigcup_{h\in H} D_{\,\mathrm{lpp}(h)}$ gilt. Da die Elemente von H aufgrund der vorangestellten Gaussreduktion paarweise verschiedene führende Potenzprodukte haben, ist die Menge $H_\mathcal{D}$ eindeutig bestimmt. Analog definieren wir $H_\mathcal{C} \subseteq H$ für die partielle Division $\mathcal{C}$.

Falls die Gleichheit $H_\mathcal{D} = H_\mathcal{C}$ zutrifft, so ist die zu $\mathcal{D}$ gehörige Paarmenge $L_\mathcal{D}$ in der zu $\mathcal{C}$ gehörigen Paarmenge $L_\mathcal{C}$ enthalten. An dieser Stelle interessieren wir uns nur für den Fall, daß H bereits eine $\mathcal{C}$-involutive Basis ist. Daher gilt für alle $(u,h) \in L_\mathcal{C}$ die Beziehung $\mathrm{Nf}_{\mathcal{C},H_\mathcal{C}}(uh) = \mathrm{Nf}_{\mathcal{D},H_\mathcal{D}}(uh) = 0$ und die Abarbeitung beider Normalformalberechnungen verläuft völlig identisch. Der Aufwand des Nachweises der Eigenschaft involutive Basis zu sein, erfordert also für $\mathcal{D}$ insgesamt höchstens soviel Aufwand wie für $\mathcal{C}$.

Nehmen wir nun an, daß sich $H_\mathcal{D}$ und $H_\mathcal{C}$ unterscheiden. In diesem Fall muß $H_\mathcal{D} \subsetneqq H_\mathcal{C}$ gelten. Man überzeugt sich leicht davon, daß dann die Anzahl der in $L_\mathcal{D}$ enthaltenen Paare echt kleiner als die Anzahl der zu $L_\mathcal{C}$ gehörigen Paare ist. Zunächst stellen wir fest, daß der Verlauf der Nullreduktionen $\mathrm{Nf}_{\mathcal{C},H_\mathcal{C}}(uh) = \mathrm{Nf}_{\mathcal{D},H_\mathcal{D}}(uh) = 0$ für Paare $(u,h) \in L_\mathcal{C} \cap L_\mathcal{D}$ im allgemeinen verschiedene Zwischenschritte aufweisen wird. Außerdem ist in der gegenwärtigen Situation zu beachten, daß nicht jedes Element von $L_\mathcal{D}$ zu $L_\mathcal{C}$ gehört. So enthält $L_\mathcal{D}$ für jedes $h \in H_\mathcal{C} \setminus H_\mathcal{D}$ das Paar $(1,h)$. Dafür befinden sich in der Menge $L_\mathcal{C}$ alle Paare der Form (X_i,h), wobei $X_i \in X$ und $X_i \circ \mathrm{lpp}(h) \notin C_{\mathrm{lpp}(h)}$. Uns interessiert wieder nur der Fall, daß H eine $\mathcal{C}$-involutive Basis ist. In diesem folgt außerdem die Existenz eines Paares $(X_j,h') \in L_\mathcal{C} \setminus L_\mathcal{D}$ mit $X_j \circ \mathrm{lpp}(h') = \mathrm{lpp}(h)$.

Zum Beweis dieser Aussage betrachten wir ein $h' \in H_\mathcal{C}$ mit bezüglich $\sqsubset$ minimalem $\mathrm{lpp}(h')$, für welches ein $X_j \in X$ mit $\mathrm{lpp}(h') \mid_\mathcal{C} \frac{\mathrm{lpp}(h)}{X_j}$ existiert. Ein derartiges Paar (X_j,h') existiert stets, denn wegen $h \notin H_\mathcal{D}$ gehört bereits ein echter Teiler von $\mathrm{lpp}(h)$ dem Monoidideal $\mathrm{Id}_T(\mathrm{lpp}(H))$ an und unter der Annahme, daß H eine $\mathcal{C}$-involutive Basis ist, besitzt jedes Element von $\mathrm{Id}_T(\mathrm{lpp}(H))$ einen $\mathcal{C}$-involutiven Teiler in $\mathrm{lpp}(H_\mathcal{C})$. Angenommen, es gäbe ein $X_i \in X$ mit $X_i \circ X_j \circ \mathrm{lpp}(h') \mid \mathrm{lpp}(h)$. Zunächst einmal gilt $\mathrm{lpp}(h') \nmid_\mathcal{C} X_j \circ \mathrm{lpp}(h')$, andern-

falls wäre $\mathrm{lpp}(h')$ im Widerspruch zur Voraussetzung $h \in H_{\mathcal{C}}$ ein $\mathcal{C}$-involutiver Teiler von $\mathrm{lpp}(h)$. Daraus ergibt sich $\deg_j(\mathrm{lpp}(h')) = \deg_j(\mathrm{lpp}(h)) - 1$, also $i \neq j$. Weiterhin existiert ein $\tilde{h} \in H_{\mathcal{C}}$ mit $\mathrm{lpp}(\tilde{h}) \mid_{\mathcal{C}} \frac{\mathrm{lpp}(h)}{X_i}$. Nach Konstruktion gelten $\mathrm{lpp}(h') \sqsubset \mathrm{lpp}(\tilde{h})$ und $\frac{\mathrm{lpp}(h)}{X_i} \in \mathbb{C}_{\mathrm{lpp}(\tilde{h})} \cap \mathrm{Id}_T(\mathrm{lpp}(h'))$. Aus der Zulässigkeit von $\mathcal{C}$ folgt $C_{\mathrm{lpp}(h')} \subset C_{\mathrm{lpp}(\tilde{h})}$. Insbesondere müßte im Widerspruch zu $\mathrm{lpp}(h') \nmid_{\mathcal{C}} X_j \circ \mathrm{lpp}(h')$ und $\deg_j(\mathrm{lpp}(h')) = \deg_j(\mathrm{lpp}(h)) - 1$ die Beziehung $\mathrm{lpp}(h') \mid_{\mathcal{C}} \frac{\mathrm{lpp}(h)}{X_i}$ gelten. Folglich war die Annahme der Existenz eines X_i mit $X_i \circ X_j \circ \mathrm{lpp}(h') \mid \mathrm{lpp}(h)$ falsch, weshalb die Gleichheit $X_j \circ \mathrm{lpp}(h') = \mathrm{lpp}(h)$ vorliegen muß.

In Abhängigkeit von der Struktur der Elemente von H könnte es somit passieren, daß einer Vielzahl billiger Reduktionen beim Test auf $\mathcal{C}$-Involutivität eine geringe Anzahl aufwendiger Reduktion beim Test auf $\mathcal{D}$-Involutivität gegenübersteht. Ein Vergleich des Gesamtaufwands ist daher schwierig. Allerdings kann man jeden Weg der Berechnung einer $\mathcal{C}$-Normalform des Elementes uh, wobei $(u, h) \in L_{\mathcal{C}} \cap L_{\mathcal{D}}$, modulo H auch als speziellen Berechnungsweg einer $\mathcal{D}$-Normalform des Elementes uh modulo H ansehen. Ebenso kann die Normalformberechnung $\mathrm{Nf}_{\mathcal{D},H_{\mathcal{D}}}(h)$ für $h \in H_{\mathcal{C}} \setminus H_{\mathcal{D}}$ entsprechend der Reduktion $\mathrm{Nf}_{\mathcal{C},H_{\mathcal{C}}}(X_j h')$ simuliert werden, die ausgeführten Reduktionsschritte und damit auch der Aufwand sind für beide Reduktionen gleich. Bei Zulassung aller Elemente von H zur Reduktion und geeigneter Wahl der Strategie zur $\mathcal{D}$-Normalformberechnung kann daher immer erreicht werden, daß der Aufwand zum Test von H auf eine $\mathcal{D}$-involutive Basis nicht höher ausfällt, als der Test auf eine $\mathcal{C}$-involutive Basis.

Die vorangegangene Diskussion zeigt, daß aus Sicht der Anforderungen *i)* und *ii)* eine Beschränkung auf maximale partielle Divisionen, die auf $\mathrm{lpp}(H)$ zulässig sind, angezeigt ist. Dabei handelt es sich nicht einmal nur um eine Heuristik, sondern um eine exakte Abschätzung. Diese trifft allerdings nur unter der Voraussetzung zu, daß beide partiellen Divisionen $\mathcal{D}$ und $\mathcal{C}$ a priori gegeben sind. Kennt man dagegen nur $\mathcal{C}$, so ist auch der Aufwand zur Verfeinerung von $\mathcal{C}$ zu berücksichtigen. Mit SubMaxVerf kennen wir einen schnellen Algorithmus zur submaximalen Verfeinerung, für maximale Verfeinerungen ist uns dergleichen nicht bekannt. Daher werden wir im weiteren nur submaximale Verfeinerungen fordern. Ob tatsächlich sogar eine Verschärfung zur Forderung der Maximalität ratsam ist, wird erst auf der Grundlage experimenteller Untersuchungen zu klären sein.

Nach Satz 7.13 verfeinert jede submaximale partielle Division $\mathcal{D}$ die entsprechende Thomasdivision. Die im Algorithmus gestellte Bedingung $\mathcal{T}^{(\mathrm{lpp}H)} \leq \mathcal{D}$ schränkt also die Menge der geeigneten submaximalen $\mathcal{D}$ nicht ein, insbesondere kann bei der Auswahlbeschränkung auf submaximale partielle Divisionen auf ihre Überprüfung verzichtet werden. Welche der verschiedenen submaximalen zulässigen partiellen Divisionen auszuwählen ist, bedarf ebenfalls heuristischer Untersuchungen. Das Verhältnis von Zeit- und Speicherbedarf zwischen den verschiedenen Möglichkeiten wird nicht mehr nur von der Menge der führenden Potenzprodukte der Elemente von H, sondern auch von der Feinstruktur der Elemente des Erzeugendensystems H beeinflußt. Mögliche Richtlinien wären zum Beispiel, die Anzahl der in L befindlichen Paare zu minimieren oder das

Volumen von $\bigcup_{h\in H} D_{\mathrm{lpp}(h)}$ zu maximieren. Auch bietet es sich an, bei der Entscheidung neben den bisherigen rein statischen auch dynamische Gesichtspunkte zu berücksichtigen. Im allgemeinen ist eine Abschätzungen des voraussichtlichen weiteren Verlaufes des Vervollständigungsprozesses nur in sehr beschränktem Maße möglich. Eine entsprechende Heuristik ist wiederum die Maximierung des Volumens von $\bigcup_{h\in H} D_{\mathrm{lpp}(h)}$. Besser als der zukünftige läßt sich der bisherige Verlauf der Vervollständigung berücksichtigen. Wir kommen damit zur Untersuchungen von Anforderung *iii)*, nämlich der Frage der Übernahme alter Nullreduktionen in den neuen Test.

Wir betrachten die folgende Situation. $\mathcal{D}$ sei eine auf $\mathrm{lpp}(H)$ zulässige partielle Division und $a \neq 0$ sei ein Element des von H erzeugten Linksideals $I \subseteq R$ mit der Eigenschaft $\mathrm{lpp}(a) \notin \bigcup_{h\in H} D_{\mathrm{lpp}(h)}$. Weiterhin sei $\mathcal{C}$ eine auf $\mathrm{lpp}(H \cup \{a\})$ zulässige partielle Division. Seien $h \in H$ und $X_i \in X$ so beschaffen, daß sowohl $\mathrm{lpp}(X_i h) \notin D_{\mathrm{lpp}(h)}$ als auch $\mathrm{lpp}(X_i h) \notin C_{\mathrm{lpp}(h)}$ gelten. In dieser Allgemeinheit wird sicher niemand erwarten, daß im Falle $\mathrm{Nf}_{\mathcal{D},H}(X_i h) = 0$ notwendigerweise auch $\mathrm{Nf}_{\mathcal{C},H\cup\{a\}}(X_i h) = 0$ gelten muß. Es gibt Gegenbeispiele die belegen, daß eine derartige Implikation selbst dann nicht zutrifft, wenn die Auswahl der partiellen Division einer strengen Regel, wie zum Beispiel $\mathcal{D} = \mathcal{J}^{(\mathrm{lpp}(H))}$ und $\mathcal{C} = \mathcal{J}^{(\mathrm{lpp}(H\cup\{a\}))}$, folgt.

Angenommen, das Paar (X_i, h) wurde bereits während der Abarbeitung von $\mathrm{IBTest}(H, \mathcal{D})$ getestet, darf man es dann beim Test $\mathrm{IBTest}(H\cup\{a\}, \mathcal{C})$ a priori aus der Paarmenge L streichen? Im allgemeinen ist die Antwort negativ, legt man jedoch auf T eine lineare Ordnung $\sqsubset$ fest und verschärft die Bedingungen an $\mathcal{D}$ und $\mathcal{C}$ durch $\mathcal{D} \in \mathbb{D}_{(\mathrm{lpp}(H),\sqsubset)}$ sowie $\mathcal{C} \in \mathbb{D}_{(\mathrm{lpp}(H\cup\{a\}),\sqsubset)}$, dann kann mit Hilfe von Bedingung *iii)* aus Satz 7.6 gezeigt werden, daß ein beliebiges Paar (u, h) im Laufe des Vervollständigungsprozesses höchstens einmal betrachtet werden muß.

Aufruf: $(H, \mathcal{D}) := \mathrm{InvBas3}(F, \sqsubset)$
Eingaben: F endliches Erzeugendensystem des Linksideals I, $0 \notin F$
$\sqsubset$ lineare Ordnung von T mit $u \mid v \Rightarrow v \sqsubset u$

Ausgaben: $\mathcal{D}$ auf $(\mathrm{lpp}(H), \sqsubset)$ zulässige partielle Division
H endliche $\mathcal{D}$-involutive Basis von I.

function CHECK(In: $F, \mathcal{D}$; Out: $\hat{a}$)
$H := \{g \in F \mid \forall f \in F \setminus \{g\} : \mathrm{lpp}(f) \nmid_{\mathcal{D}} \mathrm{lpp}(g)\}$
$L := \{(1, h) \mid h \in F \setminus H\} \cup$
$\{(y, h) \mid h \in H \wedge y \in X \wedge \mathrm{lpp}(h) \nmid_{\mathcal{D}} y \circ \mathrm{lpp}(h)\}$
$L := L \setminus L_{all}$
while $L \neq \emptyset$ **do**
Wähle $(u, h) \in L$ mit $u \circ \mathrm{lpp}(h)$ minimal bezüglich $\prec$
$L := L \setminus \{(u, h)\}$
$L_{all} := L_{all} \cup \{(u, h)\}$
$\hat{a} := \mathrm{Nf}_{\mathcal{D},H}(uh)$
if $\hat{a} \neq 0$ **then return**$(\hat{a})$
return(0)

end CHECK

begin INVBAS3

$H := \text{GAUSS}(F)$

$L_{all} := \emptyset$

Wähle submaximales $\mathcal{D} \in \mathbb{D}_{(\text{lpp}(H),\sqsubset)}$

$\hat{a} := \text{CHECK}(H, \mathcal{D})$

while $\hat{a} \neq 0$ **do**

$H := H \cup \{\hat{a}\}$

Wähle submaximales $\mathcal{D} \in \mathbb{D}_{(\text{lpp}(H),\sqsubset)}$

$\hat{a} := \text{CHECK}(H, \mathcal{D})$

return$(H, \mathcal{D})$

end INVBAS3

Die Paarmenge L_{all} ist global sichtbar und sammelt alle irgendwann einmal betrachteten Paare auf.

Beginnen wir mit dem Terminationsbeweis. Es werden nur solche Paare (X_i, h) aus L entfernt, die bereits früher reduziert wurden. Daher existiert spätestens ab Beendigung dieses früheren Testaufrufs ein Element $h' \in H$ mit $\text{lpp}(h') \sqsubset \text{lpp}(h)$ und $\text{lpp}(h') \mid \text{lpp}(X_i h)$. Da die Ordnung $\sqsubset$ festgehalten wird und keine Elemente aus H entfernt werden, bleibt diese Existenzaussage für immer bestehen. Aus diesem Grund kann der in Abschnitt 7.5 dargestellte Terminationsbeweis unverändert übernommen werden.

Kommen wir nun zum Korrektheitsbeweis. Seien H und $\mathcal{D}$ die von INVBAS3 berechneten Resultate bei Eingabe von F und $\sqsubset$. $\mathcal{D}$ werde von $Y = (Y_t)_{t \in T}$ erzeugt. Trivialerweise erzeugt H in R das gleiche Linksideal wie F. Wir haben also nur nachzuweisen, daß H tatsächlich eine $\mathcal{D}$-involutive Basis ist. Sei $H_{\mathcal{D}}$ die minimale Teilmenge von H mit der Eigenschaft $\bigcup_{h \in H_{\mathcal{D}}} D_{\,\text{lpp}(h)} = \bigcup_{h \in H} D_{\,\text{lpp}(h)}$. Wir zeigen zunächst, daß jedes Element $f \in H \setminus H_{\mathcal{D}}$ eine Darstellung

$$f = \sum_{i=1}^{l} g_i h_i \ , \ \text{wobei } g_i \in R \setminus \{0\}, h_i \in H_{\mathcal{D}} \text{ und } \text{lpp}(g_i h_i) \preceq \text{lpp}(f) \ , \quad (7.10)$$

besitzt. Zu einem gewissen Zeitpunkt während der Abarbeitung von INVBAS3 wurde das Paar $(1, f)$ in der CHECK-Funktion behandelt. Die Normalformberechnung lieferte eine Darstellung $f = \sum_{i=1}^{l} g_i' h_i'$ mit $g_i' \in R \setminus \{0\}$, $h_i' \in H$ und $\text{lpp}(g_i' h_i') \preceq \text{lpp}(f)$. Angenommen, in der Darstellung würde ein h_i' mit $\text{lpp}(h_i') = \text{lpp}(f)$ auftreten. Dann müßte aufgrund von $h_i', f \in H$ und der Gaussreduziertheit von H die Gleichheit $f = h_i'$ vorliegen. Im Widerspruch zur Annahme $(1, f) \in L$ wäre f damit zum Zeitpunkt seiner Normalformberechnung irreduzibel gewesen. Also gilt für alle $i = 1, \ldots, l$ die Relation $\text{lpp}(g_i') \prec \text{lpp}(f)$. Bisher dürfen in die Darstellung noch Elemente der gesamten Menge H anstelle der geforderten Menge $H_{\mathcal{D}}$ eingehen. Mittels noetherscher Induktion über $\text{lpp}(f)$ bezüglich $\prec$ zeigt man schließlich leicht, daß sich alle Darstellungen durch

Ersetzen der auf der rechten Seiten auftauchenden Elemente $h_i' \in H \setminus H_{\mathcal{D}}$ durch deren Darstellungen (7.10) in die Gestalt (7.10) umformen lassen.

Schließlich wollen wir zeigen, daß $H_{\mathcal{D}}$ und $\mathcal{D}$ die Voraussetzungen von Bedingung *iii)* aus Satz 7.6 erfüllen. Seien $f \in H_{\mathcal{D}}$ und $X_i \in X \setminus Y_{\mathrm{lpp}(f)}$ beliebig. Der obige Algorithmus sichert die Existenz einer Teilmenge $H' \subseteq H$ und einer auf $(\mathrm{lpp}(H'), \sqsubset)$ zulässigen partiellen Division $\mathcal{C}$, für welche während der Ausführung von $\textsc{check}(H', \mathcal{C})$ eine Normalform $\mathrm{Nf}_{\mathcal{C},H'_{\mathcal{C}}}(X_i f)$ berechnet wurde, wobei $H'_{\mathcal{C}}$ die eindeutig bestimmte minimale Teilmenge von H' mit der Eigenschaft $\bigcup_{h \in H'_{\mathcal{C}}} C_{\mathrm{lpp}(h)} = \bigcup_{h \in H'} C_{\mathrm{lpp}(h)}$ ist.
i) Sei $\mathrm{lpp}(X_i f) \notin \bigcup_{h \in H'_{\mathcal{C}}} C_{\mathrm{lpp}(h)}$. In diesem Fall war $\hat{a} = \mathrm{Nf}_{\mathcal{C},H'_{\mathcal{C}}}(X_i f)$ das Resultat der Abarbeitung von $\textsc{check}(H', \mathcal{C})$, es existiert eine Darstellung

$$X_i f - \hat{a} = \sum_{i=1}^{l} g_i h_i \ , \tag{7.11}$$

wobei $g_i \in R \setminus \{0\}, h_i \in H'_{\mathcal{C}} \subseteq H$ sowie $\mathrm{lpp}(g_i h_i) \prec \mathrm{lpp}(X_i f) = \mathrm{lpp}(\hat{a})$, und es gelten die Beziehungen $\hat{a} \in H$ sowie $\mathrm{lpp}(\hat{a}) \sqsubset \mathrm{lpp}(f)$.
ii) Es steht noch die Untersuchung des Falls der Existenz eines Elementes $h \in H'_{\mathcal{C}}$ mit $\mathrm{lpp}(h) \mid_{\mathcal{C}} \mathrm{lpp}(X_i f)$ aus. Wegen $f \in H'_{\mathcal{C}}$ müssen $\mathrm{lpp}(f) \notin C_{\mathrm{lpp}(h)}$ und folglich $\mathrm{lpp}(h) \sqsubset \mathrm{lpp}(f)$ gelten. Die Normalformberechnung liefert eine Darstellung

$$X_i f - cth = \sum_{i=1}^{l} g_i h_i \ , \tag{7.12}$$

wobei $g_i \in R \setminus \{0\}, h_i \in H, 0 \neq c \in \mathbb{K}$ und $\mathrm{lpp}(g_i h_i) \prec \mathrm{lpp}(X_i f) = \mathrm{lpp}(th)$.

Substituiert man die in den Darstellungen (7.11) und (7.12) auftretenden Elemente aus der Menge $H \setminus H_{\mathcal{D}}$ durch ihre Darstellungen (7.10), so erhält man die in Satz 7.6*(iii)* geforderten Relationen. Folglich ist $H_{\mathcal{D}}$ eine $\mathcal{D}$-involutive Basis. Nach (7.10) stimmen die von H und $H_{\mathcal{D}}$ erzeugten Linksideale von R überein, ferner ist $\mathcal{D}$ nach Konstruktion auf $(\mathrm{lpp}(H), \sqsubset)$ zulässig. Also ist auch H eine $\mathcal{D}$-involutive Basis. □

Am Rande sei bemerkt, daß Eigenschaft *ii)* aus Satz 7.6 für den obigen Korrektheitsbeweis nicht anwendbar ist, da die Bedingung $\mathrm{Nf}_{\mathcal{D},H}(uh) = 0$ selbst bei festgehaltenem $\sqsubset$ keine Invariante der **while**-Schleife darstellt.

Der obige Algorithmus InvBas3 zeigt, daß die Fixierung der Zulässigkeitsordnung $\sqsubset$ zur Einsparung einer großen Anzahl von Nullreduktionen führen kann. Auch beschleunigt das Festhalten der Ordnung den Schritt zur Berechnung von $\mathcal{D}$ aufgrund drastischer Suchraumbeschränkungen oftmals erheblich. Die Fixierung birgt aber auch einen offensichtlichen Nachteil in sich. Es kann nicht ausgeschlossen werden, daß die schnellsten Wege zur Vervollständigung von H zu einer involutiven Basis gerade über den abgeschnitten Teil des Suchraums führen würden. So könnte sogar bereits eine $\mathcal{C}$-involutive Basis bezüglich einer partiellen Division $\mathcal{C} \in \mathbb{D}_{(\mathrm{lpp}(H), \sqsubset')}$ vorliegen. Außer in diesem Extremfall ist es aber bisher praktisch unmöglich, die Güte der einzelnen Vervollständigungswege a priori zu vergleichen. Wenigstens solange dafür keine brauchbaren Heuristiken gefunden werden, erscheint die Anwendung von Algorithmus InvBas3 vorteilhaft.

Den gleichen Argumenten folgend wie bisher, ist es angezeigt, die Auswahl von $\mathcal{D}$ in einer solchen Weise zu treffen, daß möglichst viele der bereits untersuchten Paare der Menge L_{all} auch tatsächlich wieder bearbeitet werden müßten. Sei $\hat{H} = H \setminus \{\hat{a}\}$ das Erzeugendensystem vor der letzten Erweiterung und $\mathcal{C}$ die dazu ausgewählte auf $\left(\mathrm{lpp}(\hat{H}), \sqsubset\right)$ zulässige partielle Division. $[\mathcal{D}]_{\equiv_{\mathrm{lpp}(H)}}$ und $[\mathcal{C}]_{\equiv_{\mathrm{lpp}(\hat{H})}}$ werden von $Y^{(\mathcal{D})} = \left(Y_u^{(\mathcal{D})}\right)_{u \in \mathrm{lpp}(H)}$ beziehungsweise $Y^{(\mathcal{C})} = \left(Y_u^{(\mathcal{C})}\right)_{u \in \mathrm{lpp}(\hat{H})}$ erzeugt. Dann bedeutet die obige Forderung, daß im Idealfall die Beziehung $\forall u \in \mathrm{lpp}(\hat{H}) \; : \; Y_u^{(\mathcal{D})} \subseteq Y_u^{(\mathcal{C})}$ angestrebt werden sollte. Mit anderen Worten versuchen wir, $\mathcal{C}$ durch ein geeignetes $\mathcal{D}$ zu vergröbern, das soll heißen

$$[\mathcal{D}]_{\equiv_{\mathrm{lpp}(\hat{H})}} \leq_{\equiv_{\mathrm{lpp}(\hat{H})}} [\mathcal{C}]_{\equiv_{\mathrm{lpp}(\hat{H})}} \; . \tag{7.13}$$

Die Forderung (7.13) erweist sich insofern als zu streng, daß sie mit der Forderung nach Submaximalität von $\mathcal{D}$ unvereinbar ist, wie Lemma 7.17 noch zeigen wird. Wir ändern die Hauptschleife von Algorithmus InvBas3 folgendermaßen ab:

while $\hat{a} \neq 0$ **do**

$H := H \cup \{\hat{a}\}$

$\mathcal{C} := \mathcal{D}$

Wähle submaximales $\mathcal{D} \in \mathbb{D}_{(\mathrm{lpp}(H), \sqsubset)}$ mit maximalem $\inf(\mathcal{D}, \mathcal{C})$

$\hat{a} := \textsc{check}(H, \mathcal{D})$

Das Infimum $\inf(\mathcal{D}, \mathcal{C})$ bezieht sich auf die Verbandshalbordnung $\leq$. Die partielle Division $\inf(\mathcal{D}, \mathcal{C})$ ist auf $(\mathrm{lpp}(H), \sqsubset)$ zulässig und wird bis auf $\mathrm{lpp}(\hat{H})$-Äquivalenz von der Familie $\left(Y_u^{(\mathcal{D})} \cap Y_u^{(\mathcal{C})}\right)_{u \in \mathrm{lpp}(\hat{H})}$ erzeugt. Falls ein $\mathcal{D}$ existiert, welches unter allen auf $(\mathrm{lpp}(H), \sqsubset)$ zulässigen partiellen Divisionen submaximal ist und durch $\mathcal{C}$ verfeinert wird, so erfolgt die oben beschriebene Auswahl nur unter diesen. Allgemein wird eine möglichst feine der auf $(\mathrm{lpp}(H), \sqsubset)$ zulässigen Vergröberungen von $\mathcal{C}$ submaximal verfeinert.

Jede nur von den führenden Potenzprodukten der Elemente von H abhängige Auswahlstrategie der partiellen Divisionen in Algorithmus InvBas2 kann durch eine Familie $(\mathcal{D}_V)_{V \subseteq T}$ mit $\mathcal{D}_V \in \mathbb{D}_V$ und die Auswahlvorschrift $\mathcal{D} := \mathcal{D}_{\mathrm{lpp}(H)}$ beschrieben werden. Nach diesem Prinzip arbeiten die Algorithmen zur Berechnung von Janet- und Thomasbasen unter Verwendung der Familien ι beziehungsweise τ. Die von uns untersuchten Modifikationen von Algorithmus InvBas2 bis hin zu InvBas3 stellen zusätzliche Bedingungen an die einzusetzende Familie partieller Divisionen $(\mathcal{D}_V)_{V \subseteq T}$. Zunächst bewirken unsere Modifikationen, daß es sich bei jeder partiellen Division $\mathcal{D}_V$ der Familie um ein submaximales Element der Menge $\mathbb{D}_{(V, \sqsubset)}$ handeln muß. Schließlich stellt die Forderung nach der Maximalität des Infimums $\inf\left(\mathcal{D}_V, \mathcal{D}_{V \cup \{v\}}\right)$ für alle $\mathcal{D}_V$ und $v \in T \setminus V$ eine die Familie in ihrer Gesamtheit betreffende Bedingung dar.

Eine Familie $(\mathcal{D}_V)_{V \subseteq T}$ partieller Divisionen $\mathcal{D}_V \in \mathbb{D}_V$ wird ein *Filter partieller Divisionen* genannt, wenn für alle Potenzproduktmengen $W \subseteq V$ die

Beziehung $\mathcal{D}_V \leq \mathcal{D}_W$ zutrifft. Sowohl Janet- als auch Thomasdivision sind Filter partieller Divisionen.

Lemma 7.17 *Die Menge X bestehe aus wenigstens drei Variablen und $\lhd$ bezeichne die reverse lexikographische Ordnung von $T = T(X)$. Dann existiert kein Filter $(\mathcal{D}_V)_{V \subseteq T}$ partieller Divisionen, so daß $\mathcal{D}_V$ für alle $V \subseteq T$ ein submaximales Element der Menge $\mathbb{D}_{(V,\lhd)}$ ist.*

Beweis: Seien $x, y, z \in X$ drei beliebige paarweise verschiedene Variablen. Wir betrachten die Potenzprodukte $u = x^2y^2z$, $v = xyz^2$, $s = xy^3z$ und $t = x^3z$. Da keines der Potenzprodukte ein anderes davon teilt, fallen Maximalität und Submaximalität auf $(U, \lhd)$, wobei $U \subseteq \{u, v, s, t\}$, zulässiger partieller Divisionen zusammen. Wir haben $t \lhd u \lhd s \lhd v$. Durch einfaches Nachrechnen zeigt man, daß jeweils genau eine maximale auf $(\{u, v, s\}, \lhd)$ beziehungsweise $(\{u, v, t\}, \lhd)$ zulässige partielle Division existiert. Ebenso sieht man leicht, daß es genau zwei maximale auf $(\{u, v\}, \lhd)$ zulässige partielle Divisionen gibt. Jede davon verfeinert nur genau eines der beiden maximalen Elemente von entweder $\mathbb{D}_{(\{u,v,s\},\lhd)}$ oder $\mathbb{D}_{(\{u,v,t\},\lhd)}$. □

Wir hatten bereits früher angedeutet, daß die Forderungen nach submaximaler Wahl von $\mathcal{D}$ und Beziehung (7.13) unvereinbar sind. Das soll am im Beweis dargestellten Beispiel verdeutlicht werden. Angenommen, es liegt $\mathrm{lpp}(H) = \{u, v\}$ vor und es wurde diejenige maximale auf $\mathrm{lpp}(H)$ zulässige partielle Division $\mathcal{D}$ ausgewählt, welche die maximale auf $\{u, v, s\}$ zulässige partielle Division verfeinert. Besitzt dann das im Ergebnis der CHECK-Funktion zur Basis hinzuzufügende Element $\hat{a}$ das führende Potenzprodukt t, so können bei der Auswahl der nachfolgenden partiellen Division nicht gleichzeitig beide obigen Anforderungen erfüllt werden.

An den in diesem Abschnitt dargestellten Resultaten werden entscheidende Einschränkungen des axiomatischen Ansatzes von Gerdt und Blinkov gegenüber der hier beschriebenen Methode deutlich. Zum ersten ließen sie nur ganze Familien partieller Divisionen in die Untersuchungen einfließen und zum zweiten fordern sie in einem ihrer Axiome sinngemäß sogar die Filtereigenschaft der Familie. Dadurch werden Effizienz und Flexibilität des Algorithmus zur Berechnung involutiver Basen erheblich eingeschränkt. Hinzu kommt, daß ihre Axiomatik weder die Werkzeuge zur Klassifikation aller involutiven Divisionen[2] noch die Möglichkeit von Qualitätsvergleichen oder Verbesserungen gegebener involutiver Divisionen bietet.

7.6.2 Verschiedenes

Kopf- gegen Totalreduktion Im Zusammenhang mit der Untersuchung kanonischer Simplifikatoren haben wir uns in Abschnitt 5.3 mit dem Unterschied zwischen Kopf- und Totalreduktion im Sinne der Gröbnerbasistheorie auseinandergesetzt. Aus dieser theoretischen Sicht erwies sich die Totalreduktion als vorteilhaft, da sie für Gröbnerbasen einen kanonischen Simplifikator liefert.

[2] Bei Gerdt und Blinkov wird ein ihren Axiomen genügender Filter partieller Divisionen als involutive Division bezeichnet (siehe [GB96]).

Buchberger stellte in [Bu85] die Vor- und Nachteile beider Ansätze mit Blick auf die Effizienz der Berechnungen gegenüber. Auf der Grundlage experimenteller Untersuchungen gelangten Giovini, Mora, Niesi, Robbiano und Traverso zu dem Schluß, daß die Totalreduktion wenigstens im Mittel auch effizienter arbeitet als die Kopfreduktion (siehe [G&91]).

Für die involutive Methode gilt folgende Relativaussage. Setzt man nur Kopfreduktionen ein, so ist der Aufwand der involutiven Methode mindestens ebenso groß, wie der Aufwand einer geeigneten Version des Buchbergeralgorithmus bei gleichen Eingaben. Diese Tatsache erkennt man sofort daran, daß sich beide Algorithmen bei Verwendung von Kopfreduktion nur noch dadurch unterscheiden, daß die Zwischenbasis im involutiven Fall durch (unreduzierte) Vielfache anderer Basiselemente mit Potenzprodukten angereichert wird. Jedes im Gröbnerfall betrachtete S-Polynom muß auch im involutiven Fall reduziert werden und gemäß Lemma 7.15 stimmen die Normalformalgorithmen im Gröbner- und im involutiven Fall überein. Zusammenfassend kann man sagen: falls der involutive Algorithmus mit Kopfreduktion besser arbeitet als mit Totalreduktion, dann ist es in jedem Fall günstiger, zuerst eine Gröbnerbasis mittels eines effizienten Buchbergeralgorithmus zu berechnen und diese anschließend, sofern man tatsächlich an der feineren Struktur der involutiven Basis interessiert ist, zu vervollständigen.

Die Beispielrechnungen von Zharkov und Blinkov sowie Nischke geben Grund zu der Annahme, daß der involutive Algorithmus mit Totalreduktion in vielen Situationen den besten gegenwärtig vorhandenen Implementationen des Buchbergeralgorithmus überlegen ist. Aus diesem Grund sind weiterführende Untersuchungen zur involutiven Methode sinnvoll und dabei gibt es keine Alternative zur Verwendung der Totalreduktion.

Autoreduktion der Zwischenbasen Seien $\mathcal{D}$ eine beliebige partielle Division und $F \subset R$ eine Menge von Null verschiedener Elemente, ohne daß $\mathcal{D}$ notwendigerweise auf $\mathrm{lpp}(F)$ zulässig zu sein braucht.

Wir nennen F eine *$\mathcal{D}$-autoreduzierte* Menge, wenn für alle Elemente $f \in F$ gilt, daß keines der in f auftretenden Potenzprodukte $\mathcal{D}$-Vielfaches des führenden Potenzproduktes eines Elementes von $F \setminus \{f\}$ ist. Ist F nicht $\mathcal{D}$-autoreduziert, so führt die Anweisungsfolge

Aufruf: $H :=$ AUTOREDUCE$(F, \mathcal{D})$
Eingaben: F endliches Erzeugendensystem des Linksideals I, $0 \notin F$
$\mathcal{D} \in \mathbb{D}_\emptyset$ partielle Division.
Ausgaben: H endliches $\mathcal{D}$-autoreduziertes Erzeugendensystem von I

H := F
while es existiert $f \in H$ mit $\mathrm{Nf}_{\mathcal{D},H\setminus\{f\}}(f) \neq f$ **do**
wähle ein beliebiges derartiges $f \in H$
$H := H \setminus \{f\}$
if $\mathrm{Nf}_{\mathcal{D},H\setminus\{f\}}(f) \neq 0$ **then** $H := H \cup \{\mathrm{Nf}_{\mathcal{D},H\setminus\{f\}}(f)\}$

nach endlicher Zeit auf eine das gleiche Linksideal wie F erzeugende $\mathcal{D}$-autoreduzierte Menge. Korrektheits- und Terminationsbeweis des Algorithmus sind

trivial.

Eine spezielle Form der *Autoreduktion* ist die in Algorithmus InvBas3 gerufene Funktion Gauss. Dieser liegt das minimale Element des Verbandes $\mathbb{D}_\emptyset$ aller partiellen Divisionen zugrunde. Dabei hat jedes Potenzprodukt nur sich selbst als involutives Vielfaches. Über den Nutzen dieser vorbereitenden Gaussreduktion hatten wir bereits in Abschnitt 7.5 gesprochen. Wurde anfangs eine vorbereitende Gaussreduktion ausgeführt, so werden später alle in InvBas3 auftretenden Zwischenbasen Gaussreduziert sein, so daß eine nochmalige Anwendung überflüssig ist.

Der andere Extremfall besteht in der *Gröbnerreduktion*, welche auf der gewöhnlichen Division, dem maximalen Element von $\mathbb{D}_\emptyset$, basiert. Ähnlich wie beim Verhältnis von Kopf- und Totalreduktion gibt es auch hier gegeneinander abzuwägende Für und Wider (siehe [Bu85], [G&91]). Aktueller Standard beim Buchbergeralgorithmus ist der Verzicht auf die Gröbnerreduktion von Zwischenbasen. In unserer Situation der involutiven Basen ist die Sachlage noch eindeutiger, denn Einfügen von Gröbnerreduktionen zerstört das Terminationsverhalten. Ähnliches trifft auch für $\mathcal{D}$-Autoreduktionen bezüglich der jeweils aktuellen partiellen Division zu. Zusätzlich ist unbedingt zu beachten, daß aus der Zulässigkeit von $\mathcal{D}$ für $\mathrm{lpp}(F)$ keineswegs die Zulässigkeit von $\mathcal{D}$ für $\mathrm{lpp}\left(\textsc{Autoreduce}(F,\mathcal{D})\right)$ folgen muß. Grundsätzlich ist der im Buchbergeralgorithmus aus Effizienzgründen übliche Verzicht auf Zwischenautoreduktionen hier schon deshalb unbedingt zu übernehmen, da sonst die Termination des Algorithmus verlorengehen würde.

Die einzige weitere sinnvolle Autoreduktion besteht in der Nachbearbeitung der Ergebnisse H und $\mathcal{D}$ von InvBas3. Jede Teilmenge $H' \subseteq H$ mit $\bigcup_{h\in H'} D_{\mathrm{lpp}(h)} = \bigcup_{h\in H} D_{\mathrm{lpp}(h)} = \mathrm{Id}_T(\mathrm{lpp}(I))$ ist ebenfalls $\mathcal{D}$-involutive Basis des Linksideals I. Der Übergang von H zu einer minimalen Teilmenge $H' \subseteq H$ mit dieser Eigenschaft stellt eine teilweise $\mathcal{D}$-Autoreduktion dar, denn es werden gerade die Elemente h weggelassen, die modulo $H\backslash\{h\}$ die $\mathcal{D}$-Normalform 0 haben. Für alle $h \in H'$ gilt $\mathrm{lpp}\left(\mathrm{Nf}_{\mathcal{D},H'\backslash\{h\}}(h)\right) = \mathrm{lpp}(h)$ und $\textsc{Autoreduce}(H',\mathcal{D})$ führt wieder auf eine $\mathcal{D}$-involutive Basis von I. Diese ist ähnlich der reduzierten Gröbnerbasis von I durch das Linksideal I, die graduierte Struktur $\mathfrak{R}$ und $\mathcal{D}$ eindeutig bestimmt.

Die Ausführung von $\textsc{Autoreduce}(H,\mathcal{D})$ im Anschluß an die Abarbeitung von $\textsc{InvBas3}(F,\sqsubset)$ ist daher mit Blick auf die Normalisierung des Ergebnisses durchaus ratsam. Man beachte aber, daß sich die Eindeutigkeitsaussage auf ein festes $\mathcal{D}$ bezieht. Es besteht im allgemeinen keine Eindeutigkeit des Ergebnisses in Bezug auf die Eingaben F und $\sqsubset$ (sowie mittelbar $\mathfrak{R}$ und I) von InvBas3.

Auswahl des Basispolynoms zur Ausführung des nächsten Reduktionsschritts Bei der Ausführung eines Reduktionsschrittes während der Berechnung einer Normalform $\mathrm{Nf}_{\mathcal{D},F}(uh)$ bestehen im allgemeinen Freiheiten in der Auswahl des Potenzprodukts an dem und im Basiselement mit welchem reduziert wird. Die erste Entscheidung fällt klar zugunsten des maximal möglichen Potenzprodukts aus, da dieser Reduktionsschritt in jedem Fall später nachgeholt werden müßte. Die Auswahl des Basiselements spielt in der involutiven

Methode nur eine untergeordnete Rolle. Ist die Zwischenbasis $\mathcal{D}$-autoreduziert, so gibt es niemals mehr als ein zur Reduktion geeignetes Basiselement. Bei der Janet- oder der Thomasmethode liegt beispielsweise zu jedem Zeitpunkt diese Situation vor.

Im allgemeinen Fall besteht höchstens die Wahl zwischen Basiselementen deren führende Potenzprodukte in einer $\mathcal{D}$-Teilerbeziehung zueinander stehen. Übertragung der in [G&91] für den Gröbnerfall vorgeschlagenen Methode der Auswahl des Basiselementes mit der am weitesten zurückliegenden Berechnung bedeutet, daß unter allen möglichen Basiselementen immer das zu verwenden ist, welches das gradhöchste führende Potenzprodukt besitzt. Die auf Seite 164 dargestellte Form von Algorithmus InvBas3 beruht gerade auf der entgegengesetzten Strategie, das heißt, es wird immer das Element mit gradkleinstem führenden Potenzprodukt zur Reduktion ausgewählt. Diese Reduktionsstrategie hat den rein technischen Vorteil, daß sich der Korrektheitsbeweis etwas vereinfacht. Durch einige Zusatzüberlegungen überzeugt man sich jedoch schnell davon, daß der Algorithmus auch bei Ersetzen von $\mathrm{Nf}_{\mathcal{D},H}$ durch $\mathrm{Nf}_{\mathcal{D},F}$ korrekt bleibt und stets terminiert. Die Erfahrungen aus dem Gröbnerfall können und sollten also wieder genutzt werden.

Auswahl des nächsten kritischen Paares (u,h) aus L Auch in Bezug auf die Auswahl des nächsten zu bearbeitenden kritischen Paares (u,h) aus der Menge L bestehen wesentlich weniger Freiheiten als im Gröbnerfall. Von der Standardstrategie, welche immer ein Paar mit bezüglich $\prec$ minimalem $\mathrm{lpp}(uh)$ auswählt, darf nicht abgewichen werden. Andernfalls ist die Termination des Algorithmus nicht mehr gesichert. Insbesondere kann die Zuckerstrategie, welche gegenwärtig im Gröbnerfall allgemein als am geeignetsten anerkannt ist (siehe [G&91]), nicht verwendet werden. Damit ist die praktische Bedeutung der involutiven Methode zunächst auf $\prec$ vom Ordnungstyp ω beschränkt und eine wesentliche Aufgabe für die Zukunft besteht im Auffinden weiterer terminationserhaltender Auswahlstrategien.

Entfernen unnötiger Paare aus der Menge L Diese Frage wurde bereits in Abschnitt 7.6.1 angesprochen. Gerdt und Blinkov schlagen eine Übertragung des auf der Abhängigkeit von Leittermsyzygien beruhenden Buchbergerschen Kettenkriteriums (siehe [Bu79]) vor. Allerdings ist der Korrektheitsbeweis ihres gesamten Algorithmus bisher noch unbrauchbar. Inwieweit eine derartige Verallgemeinerung in unserem Kontext möglich ist, wurde bisher nicht untersucht.

7.6.3 Vergleich von Buchberger- und involutivem Algorithmus

Im vorangegangenen Abschnitt sind wir bereits im Zusammenhang mit der Entscheidung zwischen Kopf- und Totalreduktion auf die Beziehung von Buchbergeralgorithmus und involutiver Methode eingegangen. Die oberflächliche Unterschiedlichkeit beider Algorithmen darf nicht darüber hinwegtäuschen, daß die ausgeführten Operationen in sehr großem Maße übereinstimmen. Sei P

die Menge aller kritischen Paare die bei Abarbeitung des Buchbergeralgorithmus mit Standardstrategie und Kriteriumsanwendung behandelt werden muß. Es existiert eine injektive Abbildung $P \ni (g_i, g_j) \mapsto (u, f) \in L_{all}$ von P in die Menge L_{all} der von Algorithmus InvBas3 bei gleicher Eingabebasis behandelten kritischen Paare, wobei für alle Zuordnungspaare die Beziehung $kgV(\mathrm{lpp}(g_i), \mathrm{lpp}(g_j)) = \mathrm{lpp}(uf)$ gilt. Darüberhinaus wies Mall in [Mal95] nach, daß Buchbergeralgorithmus und Pommaretalgorithmus für homogene Ideale in allgemeiner Lage bei Zugrundelegen einer gradverträglichen Termordnung und Standardauswahlstrategie kritischer Paare während der gesamten Abarbeitung identische Zwischenbasen erzeugen. Die beschriebenen Sachverhalte deuten zunächst darauf hin, daß der involutive Algorithmus weitgehend mittels Strategieanpassung durch den Buchbergeralgorithmus simuliert werden kann. Letztendlich besteht nur ein nicht simulierbarer Unterschied, welcher daher für die experimentell festgestellten Effizienzvorteile der involutiven Methode verantwortlich sein muß. In der Tat werden wir feststellen, daß er sich harmonisch in die Effizienzuntersuchungen aus [G&91] einpaßt und tatsächlich auch aus dieser Sicht eine Begründung für den Vorteil der involutiven Methode liefert.

Die folgenden Ausführungen machen zum einen die Vorschrift der oben behaupteten injektiven Abbildung von der Menge P der kritischen Paare des Buchbergeralgorithmus in die Menge L der kritischen Paare der involutiven Methode deutlich. Zum anderen wird auch der Vorzug der Bearbeitung des Elementes aus L gegenüber seinem Urbild aus P herausgearbeitet.

Sei H eine Zwischenbasis im Buchbergeralgorithmus und (g_1, g_2) das nächste zu bearbeitende kritische Paar. Das kleinste gemeinsame Vielfache der führenden Potenzprodukte von g_1 und g_2 bezeichnen wir mit t. Wir setzen voraus, daß die Standardpaarauswahlstrategie verwendet und eine abgeschwächte Form des Buchbergerschen Kettenkriteriums eingesetzt wird. Das Kriterium soll nur solche Paare aussondern, die bei der involutiven Methode automatisch unberücksichtigt bleiben. Wir setzen also voraus, daß (g_1, g_2) auch von der involutiven Methode behandelt werden würde. Es sei daran erinnert, daß die Frage, welche Paare aufgrund des Kettenkriteriums ausgesondert werden können, keine eindeutige Antwort besitzt. Die in modernen Implementationen des Buchbergeralgorithmus verwendeten Strategien zur Anwendung der Kriterien gehen auf [GM88] und [BF91] zurück. Die durch die involutive Methode aufgeprägte Strategie führt im allgemeinen zum Aussondern einer geringeren Anzahl kritischer Paare.

Bei Anwendung der involutiven Methode auf H werden im allgemeinen zunächst noch einige Paare der Gestalt (X_i, g_j) zu bearbeiten sein. Dabei wird sich das von den führenden Potenzprodukten der Zwischenbasis erzeugte Monoidideal gegenüber $\mathrm{Id}_T(\mathrm{lpp}(H))$ nicht weiter vergrössern, da vorausgesetzt war, daß alle kritischen Paare $(g_i, g_j) \in H^2$ mit $kgV(\mathrm{lpp}(g_i), \mathrm{lpp}(g_j)) \prec t$ bereits früher abgearbeitet wurden. Insbesondere entstehen zwei Folgen

$$g_1^{(0)} = g_1, g_1^{(1)} = \mathrm{Nf}\left(X_{i_1} g_1^{(0)}\right), \ldots, g_1^{(l)} = \mathrm{Nf}\left(X_{i_l} g_1^{(l-1)}\right)$$

und

$$g_2^{(0)} = g_2, g_2^{(1)} = \mathrm{Nf}\left(X_{j_1} g_2^{(0)}\right), \ldots, g_2^{(m)} = \mathrm{Nf}\left(X_{j_m} g_2^{(m-1)}\right)$$

von Elementen, die den Bedingungen $\mathrm{lpp}\left(g_1^{(k)}\right) = X_{i_k} \circ \mathrm{lpp}\left(g_1^{(k-1)}\right) \mid t$ $(1 \leq k \leq l)$ sowie $\mathrm{lpp}\left(g_2^{(k)}\right) = X_{j_k} \circ \mathrm{lpp}\left(g_2^{(k-1)}\right) \mid t \quad (1 \leq k \leq m)$ genügen und noch vor Bearbeitung des (g_1, g_2) entsprechenden Paares aus L in die Zwischenbasis aufgenommen werden. Die Normalformfunktion Nf bezieht sich auf die jeweils gültige partielle Division und Zwischenbasis. Nach endlicher Zeit wird die Situation eintreten, daß jedes Potenzprodukt, welches Vielfaches des führenden Potenzproduktes von g_1 oder g_2 ist und t teilt, ein $\mathcal{C}$-involutives Vielfaches eines Elementes der dann aktuellen Zwischenbasis H' ist. $\mathcal{C}$ bezeichnet dabei die zu diesem Zeitpunkt gültige partielle Division. Wir können davon ausgehen, daß alle $\mathcal{C}$-involutiven Vielfachen unter den führenden Potenzprodukten der Elemente der obigen beiden Folgen zu finden sind. Andernfalls, wäre (g_1, g_2) ein Paar, welches durch die verwendete Version des Kettenkriteriums ausgesondert worden wäre. Weiterhin können wir annehmen, daß die beiden obigen Folgen so beschaffen sind, daß diese Eigenschaft bei Verkürzung einer der beiden Folgen nicht mehr zutrifft. Für die weiteren Überlegungen benötigen wir nur noch die Endglieder $g_1' = g_1^{(l)}$ und $g_2' = g_2^{(m)}$. Offensichtlich gilt $kgV(\mathrm{lpp}(g_1'), \mathrm{lpp}(g_2')) = kgV(\mathrm{lpp}(g_1), \mathrm{lpp}(g_2)) = t$.

Falls $\mathrm{lpp}(g_1')$ kein $\mathcal{C}$-involutiver Teiler von t ist, so muß $\deg(\mathrm{lpp}(g_1')) = \deg(t) - 1$ gelten[3]. Analoges trifft für den Grad von $\mathrm{lpp}(g_2')$ zu. Aufgrund der Zulässigkeit von $\mathcal{C}$ ist daher der Fall $\max(\deg(\mathrm{lpp}(g_1')), \deg(\mathrm{lpp}(g_2'))) < \deg(t) - 1$ unmöglich, denn dann hätte t zwei $\mathcal{C}$-involutive Teiler, welche untereinander nicht in einer Teilerbeziehung stehen. Sei ohne Beschränkung der Allgemeinheit $\mathrm{lpp}(g_1')$ ein $\mathcal{C}$-involutiver Teiler von t. Falls dann $\mathrm{lpp}(g_2')$ ebenfalls ein $\mathcal{C}$-involutiver Teiler von t ist, so muß eines der beiden führenden Potenzprodukte $\mathrm{lpp}(g_1')$ oder $\mathrm{lpp}(g_2')$ gleich t sein und eines der kritischen Paare $(1, g_1')$ oder $(1, g_2')$ gehört zur Menge L. Ist $\mathrm{lpp}(g_2')$ dagegen kein $\mathcal{C}$-involutiver Teiler von t, so existiert eine Variable $X_i \in X$ mit $X_i \circ \mathrm{lpp}(g_2') = t$ und das Paar $(X_i, \mathrm{lpp}(g_2'))$ gehört der Menge L an. In Abhängigkeit vom vorliegenden Fall bezeichne (u, g) das tatsächlich zu L gehörige der obigen Paare.

Nun kann es passieren, daß es im nächsten Durchlauf der Testfunktion CHECK noch nicht zur Bearbeitung des Paares (u, g) kommt. Irgendwann in endlicher Zeit wird es aber dazu kommen, daß H' und $\mathcal{C}$ so beschaffen sind, daß alle oben diskutierten Bedingungen erfüllt sind und das entsprechende Paar (u, g) aus L auch tatsächlich zur Abarbeitung kommt.

Im Ergebnis des ersten Reduktionsschrittes des kritischen Paares $(u, g) \in L$ entsteht (bis auf einen skalaren Faktor) gerade das S-Polynom $Spol(g_1', g_2')$ im Sinne der Gröbnerbasistheorie. Die oben behauptete injektive Abbildung weist $(g_1, g_2) \in P$ das Paar $(u, g) \in L$ zu.

In Bezug auf die Gröbnerfiltrierung $\mathfrak{F}^{(H)} = \left(\mathcal{F}_t^{(H)}\right)_{t \in T}$ bezüglich der zum Bearbeitungszeitpunkt von (g_1, g_2) gültigen Zwischenbasis H des Buchbergeralgorithmus gilt die Beziehung

$$Spol(g_1, g_2) - Spol\left(g_1', g_2'\right) \in \mathcal{F}_t^{(H)} .$$

[3]Der Beweisgedanke dieser Aussage ist ähnlich dem, den wir auf Seite 162 verwendet haben, um für jedes $h \in H_{\mathcal{C}} \setminus H_{\mathcal{D}}$ die Existenz eines Paares $(X_j, h') \in (X \times H_{\mathcal{D}}) \cap L_{\mathcal{C}}$ mit $\mathrm{lpp}(X_j h') = \mathrm{lpp}(h)$ zu zeigen.

Aus diesem Grund sind beide S-Polynome aus Sicht des Buchbergeralgorithmus in dem Sinne äquivalent, daß der Nullreduktionstest des einen durch den des anderen ersetzt werden könnte. Die eigentliche Reduktion des entsprechenden S-Polynoms verläuft in Buchberger- und involutivem Algorithmus bei geeigneter Strategiefestlegung völlig gleich ab. Nach Lemma 7.15 ist die Ausgabe des involutiven Normalformalgorithmus auch im Gröbnersinne irreduzibel.

Fassen wir also zusammen, der nicht simulierbare Unterschied des involutiven Algorithmus besteht in der Konstruktion der Elemente $g_1' = \rho\mathrm{Nf}_H(g_1)$ und $g_2' = \rho\mathrm{Nf}_H(g_2)$ vor Bildung des S-Polynoms. Dabei bezeichnet $\rho\mathrm{Nf}_H$ eine rekursive Variante des Normalformalgorithmus Nf_H der Gröbnertheorie. Er genügt den definierenden Gleichungen

$$\begin{aligned} \rho\mathrm{Nf}_H(1,g) &= \mathrm{head}(g) + \mathrm{Nf}_H(\mathrm{tail}(g)) \text{ und} \\ \rho\mathrm{Nf}_H(wX_i,g) &= \rho\mathrm{Nf}_H(w, \mathrm{head}(X_i g) + \mathrm{Nf}_H(\mathrm{tail}(X_i g))) \,. \end{aligned}$$

Zwar ist die Implementierung der Funktion ρNf innerhalb des Buchbergeralgorithmus problemlos möglich. Dennoch bliebe für die involutive Methode der Vorteil, daß dort einmal berechnete Normalformen zur späteren wiederholten Nutzung aufgehoben werden.

Beleuchten wir nun etwas den Zusammenhang zwischen der abweichenden S-Polynombildung und den Schlußfolgerungen aus den in [G&91] ausgewerteten Experimenten. Dazu betrachten wir ein Polynom $f \in H$ mit bezüglich $H \setminus \{f\}$ irreduziblem Kopf $\mathrm{head}(f)$, dessen Rest $\mathrm{tail}(f)$ jedoch bezüglich $H \setminus \{f\}$ reduzibel ist. Nachreduktion von f bezüglich $H \setminus \{f\}$ liefert ein Polynom $f' = \mathrm{Nf}_{H\setminus\{f\}}(f) \neq f$ mit $\mathrm{head}(f) = \mathrm{head}(f')$. Ein einzelner Reduktionsschritt bewirkt die Ersetzung eines Monoms durch eine Vielzahl kleinerer Monome. Sofern das zur Reduktion verwendete Basiselement aus mindestens drei Monomen besteht und keine Auslöschungen auftreten, wird f' also länger sein als f. Stellen wir uns nun die Frage, ob es günstiger ist, ein Monom t mittels f oder mittels f' zu reduzieren. Aus jedem in f vorkommenden reduziblen Monom entsteht nach Reduktion von t mittels f wieder ein reduzibles Monom. Würde man t dagegen mittels f' reduzieren, so bestünde die Chance, sofort zu einem irreduziblen Ergebnis zu gelangen. Wir haben es also mit zwei gegenläufigen Phänomenen zu tun: *i)* Ersetzen von f durch f' kann zu längeren Elementen mit komplizierteren Koeffizienten führen und *ii)* Beibehalten von f kann die vielfach wiederholte Ausführung der an f nicht durchgeführten Reduktionsschritte bewirken. Beide Sachverhalte besitzen aber keinen allgemeingültigen Charakter, so kann f' auch kürzer und einfacher als f sein und ebenso kann nach Multiplikation mit einem Potenzprodukt u der Fall eintreten, daß in uf' wesentlich mehr reduzible Potenzprodukte auftreten als in uf.

In [G&91] gelangten die Autoren auf experimentellem Wege zu der Erkenntnis, daß das Längen- und Koeffizientenwachstum der Elemente der Zwischenbasis am besten beschränkt werden kann, indem man den Kompromiß der Totalreduktion neuer Elemente bei Verzicht auf Autoreduktion der Zwischenbasen eingeht. Die gleiche Strategie auf den involutiven Algorithmus angewandt führt auf einen moderateren Kompromiß. Zwar läßt man alte Elemente unberührt in der Zwischenbasis stehen. Sobald aber in den Graden aufgestiegen wird,

entstehen durch Multiplikation mit Elementen aus X zusätzliche Basiselemente, welche jünger sind und somit zu einem späteren Zeitpunkt totalreduziert werden. Nischkes Experimente (vgl. [Ni96]) geben Anlaß zu der Hoffnung, daß damit eine noch bessere Abschwächung des Koeffizienten- und Längenwachstums der Zwischenbasiselemente einhergeht.

Bei Algebren von auflösbarem Typ kommt ein zweiter Vorteil der involutiven S-Polynombildung hinzu. Seien $f, g \in R$ von Null verschiedene Elemente und $t \in T$ ein Potenzprodukt. Ist R ein kommutativer Polynomring, so erfordern die Operationen $f + tg$ und $f + g'$, wobei $g' = tg$ bereits vorliegt, nahezu den gleichen Aufwand. Anders verhält es sich, wenn in den definierenden Relationen der Algebra R von Null verschiedene $p_{i,j}$ auftreten. In diesem Fall überwiegt im allgemeinen der Aufwand zur Berechnung des Produkts $g' = tg$ deutlich gegenüber dem der Addition $f + g'$. Aus diesem Grund bewirkt die Redundanz der Zwischenbasis beim involutiven Algorithmus eine große Zeitersparnis durch Vermeidung mehrfacher Produktberechnungen.

Eines wird an den Ausführungen dieses Kapitels jedoch auch deutlich. Die Simulation des involutiven Algorithmus durch eine Variante des Buchbergeralgorithmus, die bis auf die S-Polynombildung mit dem involutiven Algorithmus gleichverläuft, führt nicht auf eine Umsetzung des Buchbergeralgorithmus, die dem heutigen Standard entspricht. Dabei ist es nicht so, daß man auf eine neue, vielversprechende, bisher nicht untersuchte Strategie des Buchbergeralgorithmus geführt wird, sondern man erhält eine bekanntermaßen schwache Variante. Umso erstaunlicher ist die Tatsache, daß die Vorteile gemäß der experimentellen Erfahrungen viel schwerer zu wiegen scheinen, als die bisher in Kauf zu nehmenden Strategienachteile. Eine vielversprechende Aufgabe für die Zukunft besteht also darin, die involutive Methode so weiter zu entwickeln, daß man auch noch die aus dem Gröbnerfall bekannten Strategieverbesserungen einbauen kann.

Kapitel 8

Implementationsfragen

8.1 Allgemeines

Eine ernsthafte Beschäftigung mit Problemen der konstruktiven Mathematik sollte ab einem bestimmten Punkt auch die Frage nach der rechentechnischen Umsetzung der entwickelten Algorithmen einbeziehen. Gerade in Bereichen, wo man aus theoretischen Erwägungen heraus keine Polynomialzeitalgorithmen mehr erwarten kann, ist es von großer Bedeutung, an Hand experimenteller Berechnungen abzuschätzen, wie breit das Fenster praktisch lösbarer Aufgaben ist. Jedes der modernen Allzweckcomputeralgebrasysteme, wie zum Beispiel AXIOM, Derive, Macsyma, Maple, Mathematica oder REDUCE, beinhaltet heute mehr oder weniger ausgefeilte Implementierungen des Buchbergeralgorithmus für Polynomringe über Körpern. Der Vorteil eines Allzwecksystems besteht vor allem in der Möglichkeit des Zugriffs auf andere komplizierte mathematische Verfahren, wie zum Beispiel die Faktorisierung multivariater Polynome. Damit wird die Umsetzung interessanter Anwendungen des Buchbergeralgorithmus möglich. So können Primärzerlegungen berechnet und Gleichungssysteme gelöst werden. In schwachem, aber ansteigendem Maße findet man heute in einigen Systemen auch nichtkommutative Versionen des Buchbergeralgorithmus. Zum Beispiel enthält die REDUCE-Bibliothek einen Modul NCPOLY zum Rechnen in Shiftoperatorenalgebren, einer sehr speziellen Teilklasse der Algebren von auflösbarem Typ. Dieser dient in erster Linie der Unterstützung des Moduls ZEILBERG zur infiniten Summation auf Grundlage des Zeilenbergeralgorithmus. Die Tatsache, daß die nichtkommutativen Varianten des Buchbergeralgorithmus in wesentlich geringerem Maße implementiert wurden, hat verschiedene Gründe. Das Fenster des praktisch Machbaren ist noch viel enger als im Polynomring. So gelangt man beispielsweise beim Rechnen in Algebren von auflösbarem Typ bereits nach kurzen Rechnungen zu dicht besetzten Basiselementen. In nahezu allen Allzwecksystemen ist der Multiplikationsoperator $*$ a priori als assoziativ und kommutativ vordefiniert und eine nachträgliche Implementation einer nichtkommutativen Multiplikation ist aufwendig und meist nicht besonders effizient möglich. Eine Übersicht über die Allzwecksysteme findet man in [CAGI] auf den Seiten 145 bis 178.

Neben den kommerziellen Allzwecksystemen gibt es eine ganze Reihe von

Spezialsystemen. Eine Vielzahl davon wird ebenfalls in Kapitel 4 des Übersichtsbandes [CAGI] beschrieben. Die in den Spezialsystemen enthaltenen Algorithmen stellen sich allgemeiner und flexibler dar. Auch sind sie durch zahlreiche spezielle Anwendungen angereichert. Sobald jedoch zusätzliche komplizierte Algorithmen benötigt werden, sind ihre Grenzen im allgemeinen erreicht. Macaulay (siehe [BS86], [CAGI, S. 229–234])) ist eines der leistungsfähigsten und weitverbreitesten Systeme für Anwendungen der kommutativen Algebra und der algebraischen Geometrie. Nichtkommutative Gröbnerbasen können beispielsweise mit den Systemen MAS (siehe [Kr90], [CAGI, S. 222–228]), Bergman (siehe [BF91]) oder Felix (siehe [AK91], [CAGI, S. 198–205]) berechnet werden.

8.2 Felix

Ende der 80iger Jahre, zur gleichen Zeit als der Autor dieser Arbeit theoretische Untersuchungen zu Gröbnerbasen in universellen Einhüllenden von Liealgebren durchführte, beschäftigte sich Klaus an der gleichen Universität mit grundlegenden Problemen des Aufbaus, der Arbeitsweise und des Designs von Computeralgebrasystemen (siehe [Kl89]). Die gemeinsamen Interessen führten schließlich zur Entwicklung des Computeralgebrasystems Felix . Das System besteht aus drei Ebenen. Die maschinennahe Schicht ist möglichst klein gehalten und in der Programmiersprache C geschrieben. Neben dem Systeminterface beinhaltet sie den Aufbau des Interpreters einer LISP-ähnlichen Programmiersprache. Auf dieser Sprache baut die zweite Schicht auf, in der eine komfortable imperative Programmiersprache zur Verfügung gestellt wird. Wie in Computeralgebrasystemen üblich, wird sie standardmäßig im Interpretermodus eingesetzt. Die zweite Felix-Ebene umfaßt jedoch auch Compiler und Linker (siehe [AK93]). Beide können on-line innerhalb der Interpreterschleife eingesetzt werden. Das Compilerkonzept ist modular, innerhalb eines Moduls können lokale Funktionen deklariert werden. Diese sind nach Einbinden des Moduls nach außen hin unsichtbar, wodurch Namenskonflikte von Hilfsfunktionen vermieden werden. In der dritten Schicht werden die algebraischen Algorithmen implementiert, sie besteht aus einer Bibliothek von Moduln kompilierter Felix-Programme.

Felix hat das Rechnen in und mit algebraischen Strukturen zum Anliegen. Unter dem Arbeiten mit algebraischen Strukturen ist beispielsweise der Übergang zu Faktorstrukturen oder Lokalisierungen zu verstehen. Für derartige Anwendungen ist die in den meisten kommerziellen Computeralgebrasystemen mit Ausnahme von AXIOM übliche Verfahrensweise, durch Festlegung globaler Auswertungsregeln eine algebraische Arbeitsstruktur zu erklären, ungeeignet. Jede verwendete algebraische Struktur wird selbst durch ein Felix-Objekt dargestellt. Im wesentlichen stehen in Felix die folgenden algebraischen Strukturen zur Verfügung:
i) der Ring der ganzen Zahlen, der Körper der rationalen Zahlen, endliche Körper, Körper rationaler Funktionen,
ii) Polynomringe, Algebren von auflösbarem Typ sowie G-Algebren über den unter *i)* genannten Ringen und Körpern und
iii) Linksmoduln über den Ringen aus *ii)*.

Das Kernstück der Implementation der unter *ii)* und *iii)* aufgeführten Ringe und Moduln wird jeweils von der Umsetzung des Buchbergeralgorithmus zur Berechnung von Gröbnerbasen gebildet. Dabei handelt es sich um die in Kapitel 5 der vorliegenden Arbeit dargestellten Algorithmen. Kürzlich wurde Felix um ein Parallelkonzept für lose gekoppelte Rechner erweitert. Darauf aufbauend wurde eine parallele Variante des Buchbergeralgorithmus bereitgestellt. Implementierungen der in Kapitel 6 für Potenzreihenringe entwickelten Algorithmen und der in Kapitel 7 erarbeiteten involutiven Methode stehen noch aus.

Die umfangreichsten bisher mit dem System Felix durchgeführten Berechnungen standen im Zusammenhang mit mathematischen Untersuchungen zur Klassifikation von Differentialkalkülen und stellten ein wichtiges Hilfsmittel zur Herleitung der in [AS94] erzielten Resultate dar. Einige Bemerkungen zu den für [AS94] zu lösenden Aufgabenstellungen belegen die Leistungsfähigkeit des Systems.

Zunächst liegt eine G-Algebra $\mathcal{X}_{q,\lambda,\rho}$ in drei Unbestimmten e_{-1}, e_0, e_1 zugrunde. Koeffizientenbereich ist der Quotientenkörper $\mathbb{C}(q,\lambda,\rho)$ des Polynomrings in den Variablen q, λ und ρ über den komplexen Zahlen. Eine Vektorraumbasis der Algebra $\mathcal{X}_{q,\lambda,\rho}$ besteht aus allen Termen $e_{-1}^i e_0^\epsilon e_1^k$ mit $i,k \in \mathbb{N}$ und $\epsilon \in \{0,1\}$. Das ist keine Poincaré-Birkhoff-Witt-Basis, also liegt keine Algebra von auflösbarem Typ vor und der graduierten Struktur kann keine echte Bewertungsfunktion zugrundegelegt werden. Die gesuchten Differentialkalküle Γ sind endlich erzeugte Unterbimoduln des von $\{\mathrm{d}e_{-1}, \mathrm{d}e_0, \mathrm{d}e_1\}$ frei erzeugten $\mathcal{X}_{q,\lambda,\rho}$-Bimoduls. Von Γ kann ein neunelementiges Erzeugendensystem H angegeben werden, in welchem allerdings noch sieben Parameter $y_1, \ldots, y_7$ für Elemente aus $\mathbb{C}(q,\lambda,\rho)$ auftreten. Außerdem muß Γ eine Reihe weiterer algebraischer Eigenschaften aufweisen. Beispielsweise muß er als $\mathcal{X}_{q,\lambda,\rho}$-Rechtsmodul durch $\{\mathrm{d}e_{-1}, \mathrm{d}e_0, \mathrm{d}e_1\}$ frei erzeugt werden. Die Klassifikation der Differentialkalküle erfordert nun, festzustellen, für welche Werte der $y_1, \ldots, y_7 \in \mathbb{C}(q,\lambda,\rho)$ alle an Γ gestellten Bedingungen erfüllt werden. In den bisherigen Betrachtungen wurden die Variablen q, λ, ρ unterschwellig als transzendent über dem Körper der komplexen Zahlen angesehen. Tatsächlich handelt es sich aber um komplexwertige Parameter. Wenigstens für eine gewisse Zariski-offene Teilmenge von $\mathbb{C}^3$ übertragen sich die Lösungen aus dem transzendenten Fall. Auf einer algebraischen Menge von Spezialisierungen für q, λ, ρ müssen die Rechnungen mit den entsprechenden algebraischen Körpererweiterungen von $\mathbb{C}$ als Koeffizientenbereich wiederholt werden. Man beachte, daß die Auswirkung der Spezialisierungen der komplexwertigen Parameter q, λ, ρ von Beginn der Rechnungen an berücksichtigt werden muß. Durch eine dem Konzept der *allumfassenden Gröbnerbasen* (siehe [We92]) ähnliche Verfahrensweise kann man für parametrige Unterbimoduln allumfassende Gröbnerbasen konstruieren, welche bei jeder beliebigen Spezialisierung der Parameter in eine Gröbnerbasis des spezialisierten Moduls übergehen. Nach einer derartigen Gröbnerbasisberechnung für den von H erzeugten Unterbimodul erhält man zehn Gleichungen in den zehn Variablen $q, \lambda, \rho, y_1, \ldots, y_7$ als System notwendiger und hinreichender Bedingungen für das Vorliegen eines gesuchten Differentialkalküls. In den Variablen $y_1, \ldots, y_7$ sind die Gleichungen höchstens quadratisch. Der Gesamtgrad in allen Variablen reicht bis 18. Mittels Gröbnerbasisberechnungen in Polynomringen,

Berechnungen von Eliminationsidealen und Faktorisierungen multivariater Polynome konnte dieses Gleichungssystem schließlich gelöst werden. Das System Felix wäre allerdings nicht zu einer vollständig automatischen Lösung in der Lage gewesen. Gerade in Bezug auf notwendige Eingriffe in die Berechnungen erweist sich die Verwendung eines eigenen Spezialsystems als sehr vorteilhaft.

Sitzungsprotokoll Abschließend geben wir das Protokoll einer Felix -Sitzung an. Die Eingabezeilen beginnen mit dem Zeichen > und die erste Zeile einer Ausgabe wird jeweils durch @ eingeleitet. In Abweichung von der tatsächlichen Arbeitsweise des Systems haben wir die Eingabezeilen aus Gründen der leichteren Bezugnahme numeriert. Abschluß einer Eingabe mit dem Dollarzeichen bewirkt die anschließende Ausgabe des ausgewerteten Ausdrucks. Der Unterstrich als Trennzeichen unterdrückt die Ausgabe des Ergebnisses.

Eingabe 1 legt die aktuelle Arbeitsstruktur fest. Dabei handelt es sich um eine Algebra von auflösbarem Typ über dem Körper der rationalen Zahlen. a ist zentrales Element der Algebra und x und y vertauschen gemäß der Regel $yx = xy + a$. Es wird keine zulässige Termordnung angegeben. Damit wird standardmäßig die totale Gradordnung mit $y \prec x \prec a$ angenommen. Die Eingaben 2 und 3 weisen den (Felix-)Variablen k und h die Elemente y^3+x^2y+xy beziehungsweise $x^2 + x$ der Arbeitsstruktur zu. Schließlich wird in Eingabe 4 die Berechnung der reduzierten Gröbnerbasis des von h und k erzeugten Linksideals des aktuellen Ringes verlangt. Das anschließende Ergebnis stellt die Gröbnerbasis $\{x^2 + x, a^2, y^3 - 2ax - a, ay^2\}$ dar. Analog wird dann in den Eingaben 5 und 6 mit dem rechts- und zweiseitigen Idealfall verfahren.

```
1> select rat[a,x,y]/{y*x==x*y+a}_
2> k := y^3+x^2*y+x*y$
@ := X^2*Y+Y^3+X*Y
3> h := x^2+x$
@ := X^2+X
4> standard(leftideal(k,h))$
*****************************************************************
LEFTIDEAL of 4 elements
  X^2+X
  A^2
  Y^3-2*A*X-A
  A*Y^2
*****************************************************************
5> standard(rightideal(k,h))$
*****************************************************************
RIGHTIDEAL of 5 elements
  X^2+X
  Y^3
  A*Y^2
  A^2*Y
  A^3
*****************************************************************
```

```
6>standard(ideal(k,h))$
************************************************************************
IDEAL of 3 elements
  A
  X^2+X
  Y^3
************************************************************************
```

Literaturverzeichnis

[AdL94] Adams, W.W., Loustaunau, P., An Introduction to Gröbner Bases. Graduate Studies in Mathematics, Vol. 3, AMS Press, 1994.

[AMR92] Alonso, M.E., Mora, T., Raimondo, M.: A computational method for algebraic power series. *J. Pure Appl. Algebra* **77** S. 1–38, 1992.

[Ap88] Apel, J., Gröbnerbasen in nichtkommutativen Algebren und ihre Anwendung, Dissertation, Univ. Leipzig, 1988.

[Ap92] Apel, J., A relationship between Gröbner bases of ideals and vector modules of G-algebras. Contemporary Mathematics, Band **131**, Teil 2, S. 195–204, 1992.

[Ap95a] Apel, J., Division of Entire Functions by Polynomial Ideals. *Lect. Notes Comp. Sci.* **948**, S. 82–95, 1995.

[Ap95b] Apel, J., A Gröbner Approach to Involutive Bases. *J.Symb.Comp.* **19**/5, S. 441–457, 1995.

[Ap96] Apel, J., The Theory of Involutive Divisions and an Application to Hilbert Function Computations. Erscheint im *J.Symb.Comp.*, 1996.

[Ap98] Apel, J., The Computation of Gröbner Bases Using an Alternative Algorithm. Progress in Computer Science and Applied Logic, Vol. **15**, Birkhäuser, Basel, S. 35–45, 1998.

[AK91] Apel, J., Klaus, U., Felix – an assistant for algebraists. Konferenzband ISSAC'91, Watt, S.M. (Editor), ACM Press, New York, S. 382–389, 1991.

[AK93] Apel, J., Klaus, U., Data Representation and In-built Compilation in the Computer Algebra Program FELIX. *L.N.C.S.* **721**, S. 173–192, 1993.

[ApL85] Apel, J., Lassner, W., An Algorithm for Calculations in Enveloping Algebras. Proc. Int. Conf. on. Comp. Algebra and its Appl. in Theoretical Physics, JINR, D11-85-791, S. 231–241, Dubna, 1985.

[ApL88] Apel, J., Lassner, W., An Extension of Buchberger's Algorithm and Calculations in Enveloping Fields of Lie Algebras. *J.Symb.Comp.* **6**, S. 361–370, 1988.

[AS94] Apel, J., Schmüdgen, K., Classification of Three Dimensional Covariant Differential Calculi on Podles' Quantum Spheres and on Related Spaces. *Letters in Mathematical Physics* **32**, S. 25–36, 1994.

[ASTW] Apel, J., Stückrad, J., Tworzewski, P., Winiarski, T.: Reduction of everywhere convergent power series with respect to Gröbner bases. *J. Pure Appl. Algebra* **110**, S. 113–129, 1995.

[BF91] Backelin, J., Fröberg, R., How we proved that there are exactly 924 cyclic 7-roots. Konferenzband ISSAC'91, Watt, S.M. (Editor), ACM Press, New York, S. 103–111, 1991.

[Ba82] Bayer, D., The Division Algorithm and the Hilbert Scheme. Dissertation, Harvard Univ., 1982.

[BS86] Bayer, D., Stillman, M., The design of Macaulay: A system for computing in algebraic geometry and commutative algebra. Konferenzband ACM Symposium on Symbolic and Algebraic Computation, Char, B.W. (Editor), University of Waterloo, Ontario, S. 157–162, 1986.

[Bec90] Becker, T., Standard bases and some computations in rings of power series. *J.Symb.Comp.* **10**, S. 165–178, 1990.

[BW93] Becker, T., Weispfenning, V., in cooperation with Kredel, H., Gröbner Bases, A Computational Approach to Commutative Algebra. Springer, New York, Berlin, Heidelberg, 1993.

[BS90] Beckmann, P., Stückrad, J., The Concept of Gröbner Algebras. *J.Symb.Comp.* **10**, S. 465–479, 1990.

[Ber78] Bergman, G., The Diamond Lemma for Ring *Theory. Adv. Math.* **29**, S. 178–218, 1978.

[Bet59] Beth, E.W., The Foundations of Mathematics. North-Holland Publishing Company, Amsterdam, 1959.

[Bo85] Bose, N.K. (Editor), Recent Trends in Multidimensional System Theory, D. Reidel Publ. Comp., 1985.

[Bu65] Buchberger, B., Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Dissertation, Univ. Innsbruck, 1965.

[Bu79] Buchberger, B., A criterion for detecting unnecessary reductions in the construction of Gröbner bases. *L.N.C.S.* **72**, S. 3–21, 1979.

[Bu83] Buchberger, B., A critical pair/completion algorithm in reduction rings. *L.N.C.S.* **171**, S. 137–161, 1983.

[Bu85] Buchberger, B., An Algorithmic Method in Polynomial Ideal Theory. Kapitel 6 in [Bo85].

[BCL83] Buchberger, B., Collins, G.E., Loos, R., Computer Algebra - Symbolic and Algebraic Computation. Springer-Verlag, Wien, New York, 1983.

[BL83] Buchberger, B., Loos, R., Algebraic Simplification. S. 11–40 in [BCL83].

[Ca70] Caviness B.F., On Canonical Forms and Simplification. *J. ACM* **17**/2, S. 385–396, 1970.

[CMP95] Cerlienco, L., Mureddu, M., Piras, F., Combinatorical-Algebraic Techniques in Gröbner Bases Theory. Sém. Lothar. Combin. **34**, 1995.

[Co81] Cohn, P.M., Universal Algebra. rev.ed., D. Reidel Pub. Comp., Dordrecht, 1981.

[CAGI] Computeralgebra in Deutschland. Fachgruppe Computeralgebra der GI, DMV und GAMMM. Grabmeier, J., Weispfenning, V. (Editoren), Passau, Heidelberg, 1993.

[CLO92] Cox, D., Little, J., O'Shea, D., Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer Verlag, New York, 1992.

[Di13] Dickson, L.E., Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. *Am.J.of Math.* **35**, S. 413–426, 1913.

[Ei68] Eisenreich, G., Zur Syzygientheorie und Theorie des inversen Systems perfekter Ideale und Vektormoduln in Polynomringen und Stellenringen. Habilitationsschrift, Universität Leipzig 1968. (auch erschienen in: Sitzungsbericht der sächsischen Akademie der Wissenschaften zu Leipzig, Band 109, Heft 3, Akademie-Verlag, Berlin 1970)

[Ei89] Eisenreich, G., Lexikon der Algebra. Akademie-Verlag, Berlin, 1989.

[Er56] Erdös, J., On the structure of ordered real vector spaces. Publ. Math. Debrecen **4**, S. 334–343, 1956.

[Er80] Ershov, Yu.L., Entscheidbarkeitsprobleme und konstruktive Modelle (in Russisch). Verlag Nauka, Moskau, 1980.

[GM88] Gebauer, R., Möller, H.M., An installation of Buchberger's algorithm. *J.Symb.Comp.* **6**, S. 275–286, 1988.

[GB96] Gerdt, V.P., Blinkov, Yu.A., Involutive bases of polynomial ideals. Preprint 01/96, Naturwissenschaftlich-Theoretisches Zentrum, Univ. Leipzig, 1996.

[GB97] Gerdt, V.P., Blinkov, Yu.A., Minimal involutive bases. Poster session zur ISSAC'97, Maui, Hawaii. Erscheint in *Mathematics and computers in simulation*, Vorabdruck als Preprint E5-97-4 des VIK Dubna, 1997.

[GTZ88] Gianni, P., Trager, B., Zacharias, G., Gröbner bases and primary decomposition of polynomial ideals. *J.Symb.Comp.* **6**/2,3, S. 149–167, 1988.

[G&91] Giovini, A., Mora, T., Niesi, G., Robbiano, L., Traverso, C., Öne sugar cube, please," or Selection Strategies in the Buchberger Algorithm. In: Watt, S.M. (ed.), Proc. ISSAC'91, ACM Press, New York, S. 49–54, 1991.

[GH90] Goltz, H.-J., Herre, H., Grundlagen der logischen Programmierung. Akademie-Verlag, Berlin, 1990.

[Gr95] Gräbe, H.-G., Algorithms in Local Algebra, *J.Symb.Comp.* **19**, S. 545–557, 1995.

[GR71] Grauert, H., Remmert, R., Analytische Stellenalgebren. Springer-Verlag, Berlin, Heidelberg, New York, 1971.

[He49] Henkin, L., The Completeness of the First-Order Functional Calculus. *J. Symbolic Logic* **14**, S. 159–166, 1949.

[He53] Henkin, L., Some Interconnections Between Modern Algebra and Mathematical Logic. *Trans. Amer. Math. Soc.* vol **74**, S. 410–427, 1953.

[Hi64] Hironaka, H., Resolution of singularities of an algebraic variety over a field of characteristic zero. *Annals of Math.* **79**, S. 109–326, 1964.

[Ja29] Janet, M., Lecons sur les systèmes d'equations aux dérivées partielles. Gauthier-Villars, Paris, 1929.

[KK84] Kandri-Rody, A., Kapur, D., Algorithms for computing Gröbner bases of polynomial ideals over various Euclidean rings. *L.N.C.S.* **174**, S. 193–206, 1984.

[KK88] Kandri-Rody, A., Kapur, D., Computing a Gröbner basis of a polynomial ideal over a Euclidean domain. *J.Symb.Comp.* **6**/1, S. 37–57, 1988.

[KW90] Kandri-Rody, A., Weispfenning, V., Non-Commutative Gröbner Bases in Algebras of Solvable Type. *J.Symb.Comp.* **9**/1, S. 1–26, 1990.

[Kl89] Klaus, U., Eine virtuelle Maschine für ein Computeralgebra-System. Dissertation, Univ. Leipzig, 1989.

[KB67] Knuth, D.E., Bendix, P.B., Simple word problems in universal algebra. Proc. Conf. on Computational Problems in Abstract Algebra, Oxford 1967, Pergamon Press, S. 263–297, 1970.

[Kr90] Kredel, H., MAS: Modula-2 algebra system. *L.N.C.S.* **429**, S. 270–271, 1990.

[Kr92] Kredel, H., Solvable polynomial rings. Dissertation, Univ. Passau, Shaker-Verlag, 1992.

[Ku70] Kurosch, A.G., Gruppentheorie I und II. Akademie-Verlag, Berlin, 1970, 1972.

[La71] Lang, S., Transcendental Numbers and Diophantine Approximations. *Bull. AMS* **77**/5, S. 635–677, 1971.

[Lu76] Lugowski, H., Grundzüge der Universellen Algebra. Teubner-Verlag, Leipzig, 1976.

[MR93] Madlener, K., Reinert, B., Computing Gröbner Bases in Monoid and Group Rings. Proc. ISSAC'93, ACM-Press, S. 254–263, 1993.

[MR96] Madlener, K., Reinert, B., A Generalization of Gröbner Basis Algorithms to Polycyclic Group Rings. Erscheint in *J.Symb.Comp.*, 1996.

[Mal95] Mall, D., A Note on Pommaret Bases. Eingereicht bei *J.Symb.Comp.*, 1995.

[MaMe82] Mayr, E.W., Meyer, A.R., The complexity of the word problem for commutative semigroups and polynomial ideals. *Adv.Math.* **46**, S. 305–329, 1982.

[Mat70] Matiyasevic, Yu.V., Diophantine Representation of Recursively Enumerable Predicates. Konferenzband Second Scandinavian Logic Symp. Amsterdam, North Holland, 1970.

[Mö88] Möller, H.M., On the construction of Gröbner bases using syzygies. *J.Symb.Comp.* **6** S. 345–359, 1988.

[MöMo84] Möller, H.M., Mora, F., Upper and lower bounds for the degree of Groebner bases. *L.N.C.S.* **174**, S. 172–183, 1984.

[MöMo86] Möller, H.M., Mora, T., New Constructive Methods in Classical Ideal Theory. *J.Algebra* **100**, S. 138–178, 1986.

[Mo82] Mora, T., An algorithm to compute the equations of tangent cones. *L.N.C.S.* **144**, S. 158–165, 1982.

[Mo86] Mora, T., Gröbner Bases for Non-Commutative Polynomial Rings. *L.N.C.S.* **229**, S. 353–362, 1986.

[Mo88a] Mora, T., Seven Variations on Standard Bases. Preprint, Univ. di Genova, Dip. di Mathematica, N. 45, 1988.

[Mo88b] Mora, T., Gröbner Bases in Non-Commutative Algebras. *L.N.C.S.* **358**, S. 150–161, 1988.

[Na62] Nagata, M., Local rings. Interscience, New York, 1962.

[Ni96] Nischke, K., Private Information über eine Implementierung zum ESPRIT-BRA Projekt PoSSo.

[Pa85] Pan, L., Application of Rewriting Techniques. Dissertation, Univ. Santa Barbara, 1985.

[Po78] Pommaret, J.F., Systems of Partial Differential Equations and Lie Pseudogroups. Gordan and Breach, New York, 1978.

[Rei95] Reinert, B., On Gröbner Bases in Monoid and Group Rings. Dissertation, Univ. Kaiserslautern, 1995.

[Ren76] Renschuch, B., Elementare und praktische Idealtheorie. Deutscher Verlag der Wissenschaften, Berlin, 1976.

[Ri68] Richardson, D., Some Unsolvable Problems Involving Elementary Functions of a Real Variable. *J.Symb.Logic* **33**, S. 511–520, 1968.

[Rob85] Robbiano, L., Term orderings on the polynomial ring. *L.N.C.S.* **204** S. 513–517, 1985.

[Rob86] Robbiano, L., On the Theory of Graded Structures. *J.Symb.Comp.* **2**, S. 139–170, 1986.

[RS88] Robbiano, L., Sweedler, M., Subalgebra Bases. *L.N.M.* **1430**, S. 61–87, 1988.

[Ros93] Rosenman, A., An Algorithm for Constructing Gröbner and Free Schreier Bases in Free Group Algebras. *J.Symb.Comp.* **16**, S. 523–549, 1993.

[Sch79] Schaller, S.C., Algorithmic aspects of polynomial residue class rings. Dissertation, Univ. Wisconsin at Madison, 1979.

[Swa92] Schwarz, F., Reduction and Completion Algorithms for Partial Differential Equations. Proc. ISSAC'92, ACM Press, New York, S. 49–56, 1992.

[SS88] Shannon, D., Sweedler, M., Using Gröbner Bases to Determine Algebra Membership, Split Surjective Algebra Homomorphisms Determine Birational Equivalence. *J.Symb.Comp.* **6**, S. 267–273, 1988.

[Sh67] Shoenfield, J.R., Mathematical Logic. Addison-Wesley Verlag, 1967.

[Sti87] Stifter, S., A generalization of reduction rings. *J.Symb.Comp.* **4**/3, S. 351–364, 1987.

[Stu96] Sturmfels, B., Gröbner Bases and Convex Polytopes. Vol. **8** of Univ. Lect. Series. AMS, 1996.

[Swe88] Sweedler, M., Ideal Bases and Valuation Rings. Preprint, 1988.

[Th37] Thomas, J., Differential Systems. American Mathematical Society, New York, 1937.

[Tra77] Trachtenbrot, B.A., Algorithmen und Rechenautomaten. Deutscher Verlag der Wissenschaften, 1977.

[Tri78] Trinks, W., Über Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Number Theory* **10** S. 475–488, 1978.

[vW67] Van der Waerden, B.L., Algebra I und II. Springer Verlag, Berlin, Heidelberg, New York, 1971, 1967.

[Wa94] Wagner, K.W., Einführung in die Theoretische Informatik, Grundlagen und Modelle. Springer-Verlag, 1994.

[We92] Weispfenning, V., Comprehensive Gröbner bases. *J.Symb.Comp.* **14**/1, S. 1–29, 1992.

[Wi84] Winkler, F., The Church-Rosser property in computer algebra and special theorem proving: an investigation of critical-pair/completion algorithms. Dissertation, Univ. Linz, 1984.

[Za78] Zacharias, G., Generalized Gröbner Bases in Commutative Polynomial Rings. Diplomarbeit. MIT, Boston, 1978.

[Zh94] Zharkov, A.Yu., Involutive Polynomial Bases: General Case. Preprint, 1994.

[ZB93] Zharkov, A.Yu., Blinkov, Yu.A., Involution Approach to Solving Systems of Algebraic Equations. Proc. IMACS'93, S. 11–16, 1993.

Index

Zusammenfassung der wissenschaftlichen Ergebnisse zur Habilitationsschrift

Zu Berechenbarkeitsfragen der Idealtheorie

der Fakultät für Mathematik und Informatik
der Universität Leipzig

eingereicht von
Dr. rer. nat. Joachim Apel

angefertigt an der
Universität Leipzig, Institut für Informatik

September 1997

Zentrales Problem der vorliegenden Arbeit ist die Untersuchung verschiedener Klassen von Ringen auf die Entscheidbarkeit ihrer Enthaltenseinsprobleme für ein- beziehungsweise zweiseitige Ideale. Das Idealenthaltenseinsproblem eines Ringes R wird entscheidbar genannt, falls es einen Algorithmus gibt, der zu vorgegebenem Ringelement $a \in R$ und Ideal $I \subseteq R$ in endlicher Zeit feststellt, ob a zu I gehört. Falls R ein effektiver Ring ist, so ist die Effektivität des Restklassenringes R/I äquivalent zur Entscheidbarkeit von I. Damit sind auch Hauptmotivation und -anwendung der vorliegenden Arbeit charakterisiert.

Um nicht auf dem Niveau naiver Berechenbarkeits- und Entscheidbarkeitsbetrachtungen stehenzubleiben, wird die Entwicklung eines exakten Berechenbarkeitskalküls für abstrakte algebraische Strukturen an den Anfang gestellt. Daran schließen sich Untersuchungen zu drei Themenkreisen an. Zunächst wird auf die Gröbnertheorie graduierter Strukturen mit wohlgeordnetem Wertemonoid eingegangen. Dabei stehen Fragen nach Bedingungen für die Konstruktivität der Buchbergerschen Methode und nach der Existenz und Konstruierbarkeit kanonischer Objekte sowie die Verallgemeinerbarkeit der Theorie auf den Modulfall im Mittelpunkt des Interesses. Weiter beschäftigen wir uns mit Gröbner- und Standardbasen in topologischen Ringen, wobei die Fragen nach der Stetigkeit der Divisionsformeln und der algorithmischen Konstruierbarkeit von Näherungslösungen einen zentralen Platz einnehmen. Schließlich wird eine allgemeine Theorie involutiver Basen als alternative Entscheidungsmethode des Idealenthaltenseinsproblems in effektiven Algebren von auflösbarem Typ entwickelt und der Buchbergerschen Methode gegenübergestellt.

1. Eine abstrakte algebraische Struktur $\mathcal{A} = (A; f_1, \ldots, f_n; P_1, \ldots, P_m)$ wird in Bezug auf eine *Beschreibungsvorschrift* $b : \Omega^* \to A$ *effektiv* genannt, falls eine surjektive, berechenbare Funktion $\nu : \Omega^* \to \mathbb{N}$ und eine bijektive Numerierung $\mu : \mathbb{N} \to A$ von A existieren, so daß das Diagramm

$$\begin{array}{ccc} A & \xleftarrow{\ b\ } & \Omega^* \\ & {\scriptstyle\mu}\searrow & \downarrow{\scriptstyle\nu} \\ & & \mathbb{N} \end{array}$$

kommutativ ist und alle Operationen $f_i^{(\mu)}$ $(i = 1, \ldots, n)$ rekursive Funktionen und alle Relationen $P_i^{(\mu)}$ $(i = 1, \ldots, m)$ rekursive Mengen sind. Dabei bezeichnen $f_i^{(\mu)}$ und $P_i^{(\mu)}$ die von f_i beziehungsweise P_i durch μ induzierten Funktionen und Relationen über den natürlichen Zahlen.

2. Sei $\mathcal{A}$ eine bezüglich einer beliebigen Beschreibungsvorschrift b effektive algebraische Struktur der Signatur Σ und $\mathfrak{F} \subset \mathfrak{Fm}(\Sigma)$ eine konsistente, axiomatisierbare, kanonische Theorie des Prädikatenkalküls erster Stufe mit Identität. Falls alle kanonischen Modelle von $\mathfrak{F}$ isomorph zu $\mathcal{A}$ sind, so heißt $\mathfrak{F}$ eine *effektive Theorie von* $\mathcal{A}$. **[Satz 2.6]** Zu jeder effektiven algebraischen Struktur $\mathcal{A}$ existiert eine Konstantenexpansion $\mathcal{A}_C$ mit effektiver Theorie.

3. [Satz 2.7] Sei $\mathcal{A}$ eine die identische Gleichheit beinhaltende algebraische Struktur der Signatur Σ und $\mathcal{A}_E$ eine Konstantenexpansion von $\mathcal{A}$ zu einer um eine Menge E von Konstantensymbolen erweiterten Signatur Σ_E. Die Interpretationsabbildung $\hat{b} : T(\Sigma_E, \emptyset) \to A$ von $\mathcal{A}_E$ sei surjektiv. Dann ist $\mathcal{A}$ genau dann eine effektive algebraische Struktur bezüglich einer Beschreibungsvorschrift $b : \Sigma_E^* \to A$ mit $b \mid_{T(\Sigma_E,\emptyset)} = \hat{b}$, wenn die Menge der in $\mathcal{A}_E$ gültigen variablenfreien Atomformeln entscheidbar ist.

4. [Satz 2.8] Sei $\mathcal{A}$ eine effektive algebraische Struktur bezüglich der Beschreibungsvorschrift $b : \Omega^* \to A$ und $\equiv \subseteq A \times A$ eine Kongruenzrelation von $\mathcal{A}$. Falls der natürliche Homomorphismus $\iota : \mathcal{A} \to \mathcal{A}/\equiv$ stark ist, so ist die aus den Restklassen $[a]_\equiv$ $(a \in A)$ bestehende Faktoralgebra $\mathcal{A}/\equiv$ genau dann bezüglich der durch $\bar{b}(w) = [b(w)]_\equiv$ definierten Beschreibungsvorschrift $\bar{b} : \Omega^* \to A/\equiv$ effektiv, wenn die Expansion $(\mathcal{A}; \equiv)$ der Algebra $\mathcal{A}$ bezüglich b effektiv ist.

5. [Satz 3.1] R sei ein effektiver Ring[1] bezüglich b, F eine rekursiv aufzählbare Menge und $I \subseteq R$ das von F erzeugte Ideal. Dann ist der Restklassenring R/I genau dann effektiv bezüglich der durch b induzierten Beschreibungsvorschrift, wenn es einen *Divisionsalgorithmus* gibt, welcher zu beliebig vorgegebenem $a \in R$ Elemente $q_1, \ldots, q_k, p_1, \ldots, p_k \in R$, $f_1, \ldots, f_k \in F$ sowie $b \in R$ berechnet, so daß $a \mapsto b$ kanonischer Simplifikator für R/I ist und die Gleichheit $a = \sum_{i=1}^{k} q_i f_i p_i + b$ gilt.

6. Die Ausführungen zur Theorie der Gröbnerbasen in graduierten Strukturen mit wohlgeordnetem Wertemonoid basieren auf dem Robbiano/Moraschen

[1] Ring steht in der vorliegenden Arbeit immer für Ring mit Einselement ebenso wird ein R-Modul stets als unitär vorausgesetzt.

Kalkül zur Verallgemeinerung der Buchbergerschen Methode auf graduierte Strukturen. Dabei schenken wir der Behandlung von Syzygienbimoduln zweiseitiger Ideale besondere Beachtung. Insbesondere wird Moras Idee der trivialen Syzygien so verallgemeinert, daß die Behandlung ein- und zweiseitiger Ideale kommutativer Ringe wieder in der gewohnten Weise zusammenfallen. Im Rahmen einer echt zweiseitigen Betrachtung von Idealen nichtkommutativer Ringe mit kommutativem assoziierten graduierten Ring ordnet sich nun auch die Kandri-Rody/Weispfenningsche Vervollständigungstechnik harmonisch in die Theorie der graduierten Strukturen ein.

7. [**Satz 5.5**] Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur mit Wohlordnung $\prec$ und noetherschem assoziierten graduierten Ring G. Dann ist das Idealenthaltenseinsproblem des noetherschen Rings R relativ zur Effektivität des gefilterten Rings R und des graduierten Rings G, zur Berechenbarkeit der Initialabbildung $\mathrm{in} : R \to G$ und eines Schnittes $\mathrm{in}^* : G \to R$ von in bezüglich der homogenen Elemente von G, zur Entscheidbarkeit des Idealenthaltenseinsproblems endlich erzeugter homogener Ideale des graduierten Rings G und der algorithmischen Lösbarkeit des TRIV-Syzygienproblems endlich erzeugter homogener Ideale von G berechenbar.

Falls $\mathfrak{R}$ den Voraussetzungen des Satzes genügt, so wird sie eine *effektive (graduierte) Gröbnerstruktur* genannt. Analoge Sätze und Definitionen gelten für einseitige Ideale.

8. [**Satz 5.8**] Seien $(R, \Gamma, \prec_\Gamma, \varphi_\Gamma)$ und $(R, \Omega, \prec_\Omega, \varphi_\Omega)$ zwei graduierte Strukturen des Ringes R, so daß es einen schwach ordnungsverträglichen Monoidepimorphismus $\tau : \Omega \to \Gamma$ mit $\varphi_\Gamma = \varphi_\Omega \circ \tau$ gibt. Weiterhin sei I ein ein- oder zweiseitiges Ideal von R. Jede Gröbnerbasis von I bezüglich $(R, \Omega, \prec_\Omega, \varphi_\Omega)$ ist auch Gröbnerbasis von I bezüglich $(R, \Gamma, \prec_\Gamma, \varphi_\Gamma)$.

9. $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ sei eine effektive graduierte Gröbnerstruktur und F eine Gröbnerbasis des Ideals $I \subseteq R$ bezüglich $\mathfrak{R}$. Weiterhin halten wir einen beliebigen (homogenen) kanonischen Simplifikator $S_{\mathrm{In}(I)}$ des Initialideals von I fest. Mit Hilfe von $S_{\mathrm{In}(I)}$ und der Division modulo der Gröbnerbasis F kann zu jedem $a \in R$ ein modulo I kongruentes $\hat{a} \in R$ berechnet werden, dessen Initialterm Fixpunkt von $S_{\mathrm{In}(I)}$ ist. [**Satz 5.10**] Die durch

$$S_I(a) = \begin{cases} 0 & : \text{ falls } \hat{a} = 0 \\ \mathrm{in}^*(\mathrm{in}(\hat{a})) + S_I\left(\hat{a} - \mathrm{in}^*(\mathrm{in}(\hat{a}))\right) & : \text{ sonst} \end{cases}$$

rekursiv definierte Funktion S_I ist ein kanonischer Simplifikator für R/I. Im klassischen Buchbergerschen Kalkül entspricht $S_I(a)$ dem Ergebnis der Totalreduktion modulo F.

10. Sei μ eine Funktion, die jedem homogenen Ideal J des assoziierten graduierten Rings G ein (ausgezeichnetes) minimales homogenes Erzeugendensystem $\mu(J)$ zuweist. Falls $F \subseteq I$ den Bedingungen

i) $\mathrm{in}(F) = \mu(\mathrm{In}(I))$,

ii) $\mathrm{in}(f) \neq \mathrm{in}(f')$ für alle $f, f' \in F$ mit $f \neq f'$ und

iii) $S_{(F\setminus\{f\})}(f) = f$ für alle $f \in F$

genügt, so wird F eine *μ-reduzierte Gröbnerbasis* des Ideals I genannt. [**Satz 5.12**] Seien $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Ringstruktur und μ eine Funktion, die für jedes homogene Ideal des assoziierten graduierten Rings ein minimales homogenes Erzeugendensystem auszeichnet. Dann besitzt jedes Ideal $I \subseteq R$ eine μ-reduzierte Gröbnerbasis. Bei festgehaltenem Schnitt in^* der Initialabbildung ist sie sogar eindeutig bestimmt. Ist $\mathfrak{R}$ eine effektive Gröbnerstruktur und μ berechenbar, dann ist aus einem beliebigen endlichen Erzeugendensystem von I die μ-reduzierte Gröbnerbasis von I berechenbar.

11. [**Satz 5.16**] Q sei ein effektiver kommutativer Hauptidealring und $\nu : Fin(Q) \to Q$ sei eine berechenbare Funktion, die jeder endlichen Teilmenge $H \subseteq Q$ ein erzeugendes Element $\nu(H)$ des Ideals $(H) \subseteq Q$ zuordnet. $G = \bigoplus_{\gamma\in\Gamma} R_\gamma$ sei ein effektiver Γ-graduierter Ring mit entscheidbarem Enthaltenseinsproblem für endlich erzeugte homogene Ideale und zu jedem $\gamma \in \Gamma$ existiere ein berechenbarer Isomorphismus $\iota_\gamma : R_\gamma \to Q$. Für beliebige Elemente $\gamma, \omega \in \Gamma$ des Monoids Γ sei die Menge $quot(\gamma, \omega) = \{(\gamma', \gamma'') \in \Gamma \times \Gamma \mid \gamma' \circ \gamma \circ \gamma'' = \omega\}$ endlich und algorithmisch konstruierbar. Dann ist die Funktion μ, die jedem homogenen Ideal J das Erzeugendensystem $U(J) := \left\{\iota_\gamma^{-1}\left(\nu\left(\iota_\gamma(J \cap R_\gamma)\right)\right) \mid \gamma \in \Gamma(J)\right\}$ zuweist, in dem Sinne berechenbar, daß $U(J)$ aus einem beliebigen endlichen Erzeugendensystem F von J auf algorithmischem Wege gewonnen werden kann. Dabei bezeichnet $\Gamma(J)$ die eindeutig bestimmte Menge von Graden, die in einem minimalen homogenen Erzeugendensystem von J auftreten.

Sei $\mathfrak{R}$ eine effektive Gröbnerstruktur, deren assoziierter graduierter Ring den an G gestellten Bedingungen genügt. Dann kann zu jeder endlichen Teilmenge $F \subset R$ die μ-reduzierte Gröbnerbasis des von F erzeugten Ideals berechnet werden.

12. [**Satz 5.20**] Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur und $\mathfrak{F} = (\mathcal{F}_\gamma)_{\gamma\in\Gamma}$ die davon induzierte Filtrierung von R. Γ sei ein effektives noethersches Monoid mit lösbarem Faktorisierungsproblem und zu jeder endlichen Teilmenge $\Omega \subseteq \Gamma$ sei die Menge $mgRV(\Omega)$ der minimalen gemeinsamen Rechtsvielfachen von Ω algorithmisch konstruierbar. Weiterhin seien R ein effektiver Γ-gefilterter Ring und $Q = \mathcal{F}_\epsilon = R_\epsilon$ ein noetherscher Ring mit entscheidbarem Linksidealenthaltenseins- und lösbarem Linkssyzygienproblem. Jeder Faktormodul $R_\gamma = \mathcal{F}_\gamma/\hat{\mathcal{F}}_\gamma$ sei bizyklisch und für alle $\gamma, \omega \in \Gamma$ gelte die Beziehung $R_\gamma R_\omega = R_{\gamma\circ\omega}$. Zu beliebig vorgegebenem γ seien ein bi-erzeugendes Element $\mathbb{1}_\gamma$ von R_γ und ein endliches Erzeugendensystem des annullierenden Linksideals I_γ des Q-Linksmoduls R_γ berechenbar. Schließlich sei für jedes $\gamma \in \Gamma$ entscheidbar, ob die Menge $\Gamma_\gamma = \{\omega \in \Gamma \mid Q/I_\gamma \ncong Q/I_{\omega\circ\gamma}\}$ leer ist und falls nicht, so sei ein endliches Monoidlinksidealerzeugendensystem B_γ von Γ_γ auf algorithmischem Wege konstruierbar. Dann ist $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine effektive graduierte Linksgröbnerstruktur.

13. [**Satz 5.22**] Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ graduierte Struktur eines effektiven Γ-gefilterten Ringes R. Das Monoid Γ sei kommutativ, noethersch und effektiv und habe das minimale Erzeugendensystem X. Das Faktorisierungsproblem

von Γ sei lösbar und zu jeder endlichen Menge $\Omega \subseteq \Gamma$ sei die Menge $mgRV(\Omega)$ der minimalen gemeinsamen Rechtsvielfachen aller Elemente von Ω berechenbar. Weiterhin sei Q als Modul über dem Ring aller zu Q gehörigen zentralen Elemente von R endlich erzeugt und ein endliches Erzeugendensystem Z sei algorithmisch konstruierbar. Außerdem wird die Existenz berechenbarer Funktionen $\delta : Q \times Q \to Q$ und $\delta_X : X \times Q \to Q$ mit $c \cdot d = \delta(c,d) \cdot c$ und $c \cdot \mathbb{1}_x = \delta_X(x,c) \cdot \mathbb{1}_x \cdot c$ für alle $c, d \in Q$ und $x \in X$ vorausgesetzt. Der Ring Q sei noethersch und habe ein entscheidbares Linksidealenthaltenseinsproblem sowie ein lösbares Linkssyzygienproblem. Jeder homogene direkte Summand R_γ des assoziierten graduierten Rings G sei bizyklischer Q-Modul und zu jedem $\gamma \in \Gamma$ seien ein bi-erzeugendes Element $\mathbb{1}_\gamma$ von R_γ und ein endliches Erzeugendensystem des annullierenden Linksideals $I_\gamma = ann_L(R_\gamma)$ berechenbar. Schließlich gelte für alle $\gamma, \omega \in \Gamma$ die Beziehung $R_\gamma R_\omega = R_{\gamma \circ \omega}$ und für jedes $\gamma \in \Gamma$ sei entscheidbar, ob die Menge $\Gamma_\gamma = \{\omega \in \Gamma \mid Q/I_\gamma \ncong Q/I_{\omega \circ \gamma}\}$ leer ist und falls nicht, so sei ein endliches Monoidlinksidealerzeugendensystem B_γ von Γ_γ auf algorithmischem Wege konstruierbar. Dann ist $\mathfrak{R}$ sowohl effektive graduierte Linksgröbnerstruktur als auch effektive graduierte Gröbnerstruktur. Sei I ein zweiseitiges Ideal von R. Dann ist jede Gröbnerbasis des zweiseitigen Ideals I bezüglich der graduierten Struktur $\mathfrak{R}$ auch eine Gröbnerbasis des Linksideals I bezüglich $\mathfrak{R}$.

14. [Satz 5.23] Sei $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ graduierte Struktur eines effektiven Γ-gefilterten Ringes R. Γ sei ein noethersches, kommutatives, effektives Monoid mit lösbarem Faktorisierungsproblem und zu jeder endlichen Teilmenge $\Omega \subseteq \Gamma$ sei die Menge $mgV(\Omega)$ der minimalen gemeinsamen Vielfachen der Elemente von Ω algorithmisch konstruierbar. $Q = F_\epsilon \cong R_\epsilon$ sei ein noetherscher Unterring des Zentrums von R, das Idealenthaltenseinsproblem von Q sei entscheidbar und das Syzygienproblem von Q sei lösbar. Jeder homogene direkte Summand R_γ des assoziierten graduierten Rings G sei ein zyklischer Q-Modul, für welchen ein erzeugendes Element $\mathbb{1}_\gamma$ und ein endliches Erzeugendensystem des annullierenden Ideals $I_\gamma = ann_L(R_\gamma) = ann_R(R_\gamma)$ berechenbar sind. Weiterhin wird zu beliebigen $\gamma, \omega \in \Gamma$ mit $\gamma \mid \omega$ die Existenz zweier Elemente γ' und γ'' mit $\gamma' \circ \gamma \circ \gamma'' = \omega$ vorausgesetzt, so daß für alle Tripel $(\delta', \delta, \delta'')$ von Teilern $\delta' \mid \gamma'$, $\delta \mid \gamma$ und $\delta'' \mid \gamma''$ die Beziehung $R_{\delta'} R_\delta R_{\delta''} = R_{\delta' \circ \delta \circ \delta''}$ erfüllt ist. Schließlich sei die Frage, ob die Menge $\Gamma_\gamma = \{\omega \in \Gamma \mid \gamma \mid \omega \wedge Q/I_\gamma \ncong Q/I_\omega\}$ leer ist, für jedes $\gamma \in \Gamma$ entscheidbar und im Falle einer nichtleeren Menge sei ein endliches Monoididealerzeugendensystem B_γ von Γ_γ berechenbar. Dann besitzt jedes zweiseitige Ideal I von R eine endliche Gröbnerbasis bezüglich $\mathfrak{R}$ und aus einem beliebigen endlichen Erzeugendensystem von I kann eine solche endliche Gröbnerbasis von I berechnet werden.

15. [Satz 5.25, Folgerung 5.26] Für eine effektive graduierte Linksgröbnerstruktur $\mathfrak{R}$ ist das Enthaltenseinsproblem endlich erzeugter R-Linksmoduln entscheidbar. Darüberhinaus kann zu jeder endlichen Teilmenge $F \subset R^m$ ein endliches Erzeugendensystem des Linkssyzygienmoduls $LSyz(F)$ berechnet werden.

16. Seien $\mathfrak{R}_l = (R, \Gamma, \prec, \varphi_l)$ und $\mathfrak{R}_r = (R, \Gamma, \prec, \varphi_r)$ zwei graduierte Strukturen des Ringes R mit den davon induzierten Filtrierungen $\mathfrak{F}_l$ und $\mathfrak{F}_r$. Weiterhin sei

$S \subseteq R$ ein das Einselement enthaltender Unterring von R und $M = (R \otimes_S R)^m$. Schließlich sei $\mathfrak{M} = (M, \Gamma, \mathfrak{F}^M)$ eine gefilterte $(R, \Gamma, \mathfrak{F}_l, \mathfrak{F}_r)$-Bimodulstruktur von M. Die assoziierten graduierten Ringe von $\mathfrak{R}_l$ und $\mathfrak{R}_r$ werden mit G_l beziehungsweise G_r und der assoziierte graduierte Modul von $\mathfrak{M}$ wird mit G_M bezeichnet. Dann wird $F \subseteq M$ eine *Gröbnerbasis* des von F erzeugten R-Biuntermoduls $N \subseteq M$ bezüglich $\mathfrak{M}$ genannt, wenn die Gleichheit $G_l \cdot \text{ in}(F) \cdot G_r = G_l \cdot \text{ in}(N) \cdot G_r$ erfüllt ist.

Sei $\mathfrak{R} = (R, \Omega, \prec, \varphi)$ eine graduierte Struktur und T das von $\{e_1, \ldots, e_m\}$ frei erzeugte kommutative Monoid. Dann lassen sich graduierte Strukturen $\mathfrak{R}_l$ und $\mathfrak{R}_r$ mit dem direkten Produkt $\Gamma := \Omega \times T \times \Omega$ als Wertemonoid konstruieren, so daß die graduierten Strukturen $\mathfrak{R}_l$, $\mathfrak{R}_r$ und $\mathfrak{R}$ in Bezug auf die Berechnung von Gröbnerbasen gleichwertig sind und die durch die graduierte Struktur $\mathfrak{R}_l$ für den linken sowie $\mathfrak{R}_r$ für den rechten Operatorenbereich induzierte Γ-Filtrierung $\mathfrak{F}^M$ des R-Bimoduls M so beschaffen ist, daß die Berechnung von Gröbnerbasen in M auf die Berechnung von Gröbnerbasen in $R \otimes_S R$ reduziert werden kann.

17. [Satz 5.31] $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ sei sowohl effektive Links- als auch effektive Rechtsgröbnerstruktur. $R_{G,\epsilon} = Q$ sei ein effektiver Körper und Unterring des Zentrums von R. Jeder direkte Summand $R_{G,\gamma}$ des assoziierten graduierten Ringes G habe als Q-Vektorraum höchstens die Dimension 1.

Dann ist das Enthaltenseinsproblem endlich erzeugter R-Biuntermoduln des Moduls $M = (R \otimes_Q R)^m$ semientscheidbar.

Falls R ein Σ-graduierter Ring ist, wobei seine Γ-Filtrierung die Σ-Filtrierung verfeinert, dann ist das Enthaltenseinsproblem endlich erzeugter Σ-homogener R-Biuntermoduln von M für jede durch eine Funktion $\deg_\Sigma : \{e_1, \ldots, e_m\} \to \Sigma$ induzierte Σ-Modulgraduierung von M entscheidbar.

18. Eine Ordnung $\prec$ von M wird als *beschränkte Wohlordnung* bezeichnet, falls jede nach unten beschränkte Teilmenge von M bezüglich der Einschränkung von $\prec$ wohlgeordnet ist. Eine graduierte Struktur $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ des Ringes R mit beschränkt wohlgeordnetem Monoid Γ ohne kleinstem Element induziert auf R eine Hausdorff-Topologie indem man die abelschen Gruppen $\mathcal{F}_\gamma$ der durch $\mathfrak{R}$ bestimmten Filtrierung $\mathfrak{F}$ als Umgebungsbasis des Nullelementes von R ansieht. Besitzt R ein größtes Element bezüglich $\prec$, dann ist jedes $\mathcal{F}_\gamma$ ein Ideal von R und $\mathfrak{R}$ induziert eine graduierte Struktur $\mathfrak{R}/\mathcal{F}_\gamma$ auf dem Restklassenring $R/\mathcal{F}_\gamma$.

19. [Sätze 6.7, 6.8] Der assoziierte graduierte Ring G der graduierten Ringstruktur $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ sei linksnoethersch. Das Monoid $(\Gamma, \prec)$ sei beschränkt wohlgeordnet und besitze ein größtes Element. Weiterhin sei G ein effektiver graduierter Ring mit entscheidbarem Enthaltenseins- und lösbarem Syzygienproblem für endlich erzeugte homogene Linksideale. Es existiere ein Unterring R' von R, welcher mit der induzierten Filtrierung effektiv ist. Die Einschränkung $\text{in}|_{R'}$ der Initialabbildung auf R' sei berechenbar und es existiere ein berechenbarer Schnitt in^* der Initialabbildung, so daß $im(\text{ in}^*) \subseteq R'$. Dann ist für beliebiges $\gamma \in \Gamma$ das Enthaltenseinsproblem endlich erzeugter Linksideale des Restklassenrings $R/\mathcal{F}_\gamma$ entscheidbar.

Sei außerdem $H \subset R'$ ein endliches Erzeugendensystem des Linksideals I und $S_{\mathrm{LIn}(I)}$ ein beliebiger (homogener) kanonischer Simplifikator des Restklassenmoduls $G/\mathrm{LIn}(I)$. Falls R in der durch $\mathfrak{R}$ induzierten Topologie komplett ist, so ist die Funktion $S_I^{(\gamma)} : R' \to R'$, die jedem $a \in R'$ das γ-Anfangsstück $\mathrm{trunc}(\hat{a}, \gamma)$ des Elementes $\hat{a} \in R$ mit $a - \hat{a} \in I$ und $\forall u \in \mathrm{Mon}(\hat{a}) : S_{\mathrm{LIn}(I)}(u) = u$ zuordnet, für alle $\gamma \in \Gamma$ berechenbar.

Für jede streng monoton fallende Folge $\gamma_0 \succ \gamma_1 \succ \cdots$ von Elementen aus Γ und alle $a \in R$ gilt: $\lim_{i\to\infty} S_{I_{\gamma_i}}(a) = S_I(a)$. Dabei werden die Elemente von $R/\mathcal{F}_{\gamma_i}$ in natürlicher Weise in R eingebettet und $S_{I_{\gamma_i}}$ bezeichnet den unter Punkt 9 beschriebenen kanonischen Simplifikator des Bildes I_{γ_i} von I unter dem natürlichen Homomorphismus von R nach $R/\mathcal{F}_{\gamma_i}$.

Darüberhinaus existiert eine in a und den Elementen von H stetige Divisionsformel $a = \sum_{h\in H} g_h h + S_I(a)$. Der oben für S_I formulierte Grenzübergang gilt in entsprechender Weise auch für jeden der Faktoren g_h. Für alle Bestandteile der Formel können Näherungswerte in der gleichen Genauigkeit berechnet werden, in der die Eingabegrößen a und H bestimmt werden können. Dabei ist für die Werte $\varphi(g_h)$ eine Verschiebung um $\varphi(h)$ zu berücksichtigen.

20. Sei $E = \mathbb{C}\{\{X\}\}$ der Ring der ganzen Funktionen in den Variablen $X = \{X_1, \ldots, X_n\}$ und $R = \mathbb{C}[X] \subset E$ der Polynomring über $\mathbb{C}$ in X. $\mathbb{R}_+$ bezeichne die Menge der positiven reellen Zahlen. Für ein beliebiges n-Tupel $r = (r_1, \ldots, r_n) \in \mathbb{R}_+^n$ definiert

$$\left\| \sum_{\nu_1,\ldots,\nu_n} \beta_{\nu_1,\ldots,\nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \right\|_r := \sum_{\nu_1,\ldots,\nu_n} |\beta_{\nu_1,\ldots,\nu_n}| r_1^{\nu_1} \cdots r_n^{\nu_n} ,$$

eine Halbnorm $\|\cdot\|_r : E \to \mathbb{R}$ und die durch dieses System von Halbnormen auf E festgelegte Topologie stimmt mit der Topologie der lokalen gleichförmigen Konvergenz überein. $\mathfrak{R} = (R, T(X), \prec, \mathrm{lpp})$ sei eine graduierte Struktur des Polynomrings mit wohlgeordnetem Wertemonoid $(T(X), \prec)$ bestehend aus den Potenzprodukten in X. Seien $I \subseteq R$ ein vom Nullideal verschiedenes Polynomideal und $H = \{h_1, \ldots, h_k\} \not\ni 0$ eine Gröbnerbasis von I sowie $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ eine Zerlegung des Monoidideals $\mathrm{lpp}(I)$ in paarweise disjunkte Teilmengen mit der Eigenschaft $t \in \Delta_i \to \mathrm{lpp}(h_i) \mid t$ für alle $1 \le i \le k$ und alle $t \in T$. Zu jedem $a \in R$ existieren eindeutig bestimmte Polynome $b, b_1, \ldots, b_k$, so daß $a = \sum_{i=1}^k b_i h_i + b$, wobei $\mathrm{lpp}(h_i) \nmid X^\mu$ und $X^\nu \, \mathrm{lpp}(h_i) \in \Delta_i$ für alle $1 \le i \le k$, $X^\mu \in \mathrm{supp}(b)$ und $X^\nu \in \mathrm{supp}(b_i)$. Durch die Vorschriften $a \mapsto b$ und $a \mapsto b_i$ werden lineare Operatoren $\mathrm{rem}_I : R \to R$ und $\mathrm{q}_{H,\Delta_H}^{(i)} : R \to R$ festgelegt.

21. **[Satz 6.15]** Sei $\{0\} \subsetneqq I \subseteq R$ ein Polynomideal, $H = \{h_1, \ldots, h_k\}$ eine nicht das Nullpolynom enthaltende Gröbnerbasis von I und $\Delta_H = \{\Delta_1, \ldots, \Delta_k\}$ eine zugehörige Zerlegung von $\mathrm{lpp}(I)$. $\mathcal{D}$ bezeichne die Menge $T(X) \setminus \mathrm{lpp}(I) = \{t \in T(X) \mid \mathrm{lpp}(h_1) \nmid t, \ldots, \mathrm{lpp}(h_k) \nmid t\}$ aller Potenzprodukte, die in keinem Element von I führend sind. Weiterhin bezeichne $E(\mathcal{D})$ den linearen Unterraum aller ganzen Funktionen, deren Träger in $\mathcal{D}$ enthalten ist. Die Operatoren rem_I und $\mathrm{q}_{H,\Delta_H}^{(j)}$ lassen sich linear auf ganz E zu Operatoren rem_{IE} und $\mathrm{q}_{HE,\Delta_H}^{(j)}$ $(j = 1, \ldots, k)$ mit den folgenden Eigenschaften fortsetzen.

i) rem_{IE} und $\mathrm{q}^{(j)}_{HE,\Delta_H}$ $(j = 1, \ldots, k)$ sind stetig,

ii) $im(\mathrm{rem}_{IE}) \subseteq E(\mathcal{D})$,

iii) $\forall a \in E \,:\, a = \sum_{j=1}^{k} \mathrm{q}^{(j)}_{HE,\Delta_H}(a) h_j + \mathrm{rem}_{IE}(a)$,

iv) $\mathrm{rem}_{IE}(a) = 0 \Longleftrightarrow a \in IE$,

v) $(a + IE) \cap E(\mathcal{D}) = \{\mathrm{rem}_{IE}(a)\}$.

Man beachte aber, daß keiner der Operatoren als Funktion seines Index stetig ist. Das heißt, es liegt keine Stetigkeit in den Elementen der Gröbnerbasis vor.

22. [Satz 6.16] Seien $\{0\} \subsetneqq I \subseteq R$ ein Polynomideal, $H = \{h_1, \ldots, h_k\}$ eine nicht das Nullpolynom enthaltende Gröbnerbasis von I und Δ_H eine zugehörige Zerlegung des Monoidideals $\mathrm{lpp}(I)$. Weiterhin seien $g_1, \ldots, g_n$ positive ganze Zahlen, welche eine gewichtete partielle Gradordnung $\sqsubset$ definieren, deren Einschränkung auf $\bigcup_{i=1}^{k} \mathrm{supp}(h_i) \subset T(X)$ mit der von $\prec$ übereinstimmt. $\kappa \geq 1$ sei eine reelle Zahl mit der Eigenschaft, daß für alle $j = 1, \ldots, k$ die Ungleichung $\|\mathrm{head}(h_j)\|_{r_\kappa} \geq \|\mathrm{tail}(h_j)\|_{r_\kappa} + 1$, wobei r_κ das n-Tupel $(\kappa^{g_1}, \ldots, \kappa^{g_n})$ bezeichnet, erfüllt ist. Weiterhin seien $r = (\rho_1, \ldots, \rho_n)$ ein beliebiges n-Tupel positiver reeller Zahlen und $\psi \geq \kappa$ eine reelle Zahl mit $\rho_j \leq \psi^{g_j}$ für alle $j = 1, \ldots, n$. r_ψ bezeichne das n-Tupel $(\psi^{g_1}, \ldots, \psi^{g_n})$. Schließlich sei op einer der Operatoren $\mathrm{q}^{(1)}_{HE,\Delta_H}, \ldots, \mathrm{q}^{(k)}_{HE,\Delta_H}$ oder rem_{IE}. Dann gelten für alle ganzen Funktionen a und b die Abschätzungen $\mathrm{d}_{koeff}(\mathrm{op}(a), \mathrm{op}(b)) \leq \|a - b\|_{r_\kappa}$ und $\mathrm{d}_r(\mathrm{op}(a), \mathrm{op}(b)) \leq \|a - b\|_{r_\psi}$, wobei $\mathrm{d}_r(\hat{c}, c) = \|\hat{c} - c\|_r$ und $\mathrm{d}_{koeff}(\hat{c}, c) = \max_{t \in T(X)} |\beta_t|$ für $\hat{c} - c = \sum_{t \in T(X)} \beta_t t$. Sei $R' \subset E$ ein effektiver Unterpolynomring und $H \subset R'$. Dann kann die näherungsweise Berechnung der Bestandteile der Divisionsformel von a modulo H auf die Näherung von a durch ein $b \in R'$ reduziert werden. Die verbleibende Lücke besteht in der Approximation komplexer Reihen und ist von numerischer Natur.

23. [Satz 6.19, Folgerung 6.20] $Y = \{Y_1, \ldots, Y_n\}$ sei ein zweiter Satz von Variablen, die graduierte Struktur $\mathfrak{R}_Y$ des Polynomrings $R_Y = \mathbb{C}[Y]$ sei bis auf die Variablenumbenennung $X_i \mapsto Y_i$ gleich $\mathfrak{R}$ und $\mathfrak{R}_{X,Y}$ sei eine graduierte Struktur von $R_{X,Y} = \mathbb{C}[X, Y] \cong R[Y]$, wobei die Einschränkungen der Monoidordnung $\prec_{X,Y}$ auf R beziehungsweise R_Y mit den Ordnungen der graduierten Strukturen $\mathfrak{R}$ und $\mathfrak{R}_Y$ übereinstimmen und für alle $t \in T(Y)$ und $s \notin T(Y)$ die Beziehung $t \prec_{X,Y} s$ gilt. Die Ringe ganzer Funktionen E_Y und $E_{X,Y}$ werden analog eingeführt. Seien $a \in E$ eine ganze Funktion, I ein Ideal von $R = \mathbb{C}[X]$ und $\alpha = (\alpha_1, \ldots, \alpha_n)$ ein Punkt des Raumes $\mathbb{C}^n$. Weiterhin seien $J \subset R_{X,Y}$ das von $F = \{X_1 - Y_1 + \alpha_1, \ldots, X_n - Y_n + \alpha_n\}$ erzeugte Polynomideal und τ_α der durch $X_i \mapsto Y_i - \alpha_i$ $(i = 1, \ldots, n)$ erklärte Isomorphismus von E nach E_Y. Dann gilt die Gleichheit $\tau_\alpha(\mathrm{rem}_{IE}(a)) = \mathrm{rem}_{JE_{X,Y}}(\mathrm{rem}_{IE}(a)) = \mathrm{rem}_{(J + IR_{X,Y})E_{X,Y}}(a)$. Folglich gilt $\mathrm{rem}_{IE}(a)(\alpha) = \mathrm{rem}_{(J+IR_{X,Y})E_{X,Y}}(a)(0, \ldots, 0)$ und die näherungsweise Berechnung der rechten Seite ist auf Punkt 22 reduzierbar.

24. Sei Γ ein kommutatives Monoid mit minimalem Erzeugendensystem X und $Y = (Y_\gamma)_{\gamma \in \Gamma}$ eine Familie von Teilmengen $Y_\gamma \subseteq X$, die direkte Faktoren $\Omega_\gamma = \langle Y_\gamma \rangle$ von Γ erzeugen. Dann wird die Familie $\mathcal{D} = (\gamma \circ \Omega_\gamma)_{\gamma \in \Gamma}$ die von Y erzeugte

partielle Division von Γ genannt. Für $\omega \in \gamma \circ \Omega_\gamma$ wird γ als $\mathcal{D}$-*Teiler* von ω bezeichnet und $\gamma \mid_{\mathcal{D}} \omega$ geschrieben. Sei $\Delta \subseteq \Gamma$ eine Menge von Monoidelementen und $\sqsubset$ eine lineare Ordnung von Δ. Die partielle Division $\mathcal{D} = (D_\gamma)_{\gamma\in\Gamma}$ heißt auf $(\Delta, \sqsubset)$ *zulässig*, falls für alle $\delta, \delta' \in \Delta$ mit $\delta' \sqsubset \delta$ eine der Bedingungen *i)* $D_{\delta'} \subseteq D_\delta$ oder *ii)* $D_\delta \cap \mathrm{Id}_\Gamma(\delta') = \emptyset$ zutrifft. $\mathbb{D}_{(\Delta,\sqsubset)}$ bezeichnet die Menge aller auf $(\Delta, \sqsubset)$ zulässigen partiellen Divisionen. Darüberhinaus nennen wir $\mathcal{D}$ auf Δ *zulässig*, falls eine lineare Ordnung $\sqsubset$ von Δ existiert, für welche $\mathcal{D}$ auf $(\Delta, \sqsubset)$ zulässig ist. Entsprechend bezeichnet $\mathbb{D}_\Delta$ die Menge aller auf Δ zulässigen partiellen Divisionen.

Seien $\mathcal{D} = (D_\gamma)_{\gamma\in\Gamma}$ und $\mathcal{C} = (C_\gamma)_{\gamma\in\Gamma}$ zwei partielle Divisionen und $\Delta \subseteq \Gamma$ eine Menge von Monoidelementen. Falls für alle $\delta \in \Delta$ die Gleichheit $D_\delta = C_\delta$ zutrifft, so nennen wir $\mathcal{D}$ und $\mathcal{C}$ Δ-*äquivalent* und schreiben dafür $\mathcal{D} \equiv_\Delta \mathcal{C}$. Im Falle der Gültigkeit der Enthaltenseinsrelationen $D_\gamma \subseteq C_\gamma$ für alle $\gamma \in \Gamma$ wird $\mathcal{C}$ als *Verfeinerung* von $\mathcal{D}$ bezeichnet und $\mathcal{D} \leq \mathcal{C}$ geschrieben. Die Menge $\mathbb{D}_\emptyset$ aller partiellen Divisionen bildet mit der Verfeinerung $\leq$ einen Verband. Für jede Teilmenge $\Delta \subseteq \Gamma$ ist $\mathbb{D}_\Delta / \equiv_\Delta$ mit der durch $[\mathcal{D}]_{\equiv_\Delta} \leq_{\equiv_\Delta} [\mathcal{C}]_{\equiv_\Delta} :\Longleftrightarrow \exists \mathcal{D}', \mathcal{C}' \ : \ \mathcal{D} \equiv_\Delta \mathcal{D}' \wedge \mathcal{C} \equiv_\Delta \mathcal{C}' \wedge \mathcal{D}' \leq \mathcal{C}'$ definierten Halbordnung $\leq_{\equiv_\Delta}$ ein unterer Unterhalbverband der Restklassenstruktur $\mathbb{D}_\emptyset / \equiv_\Delta$.

25. Seien $\mathfrak{R} = (R, \Gamma, \prec, \varphi)$ eine graduierte Struktur mit noetherschem wohlgeordnetem kommutativem Wertemonoid $(\Gamma, \prec)$ und $\mathcal{D}$ eine partielle Division von Γ. Eine Teilmenge F des Ideals $I \subseteq R$ heißt eine $\mathcal{D}$-*involutive Basis* von I bezüglich $\mathfrak{R}$, falls $\mathcal{D}$ auf $\varphi(F)$ zulässig ist und jedes homogene Element $a \in \mathrm{In}(I)$ bereits dem von $\{\mathrm{in}(f) \mid f \in F \wedge \deg_\Gamma(\mathrm{in}(f)) \mid_{\mathcal{D}} \deg_\Gamma(a)\}$ erzeugten Unterideal von $\mathrm{In}(I)$ angehört.

26. **[Satz 7.6]** R sei eine Algebra von auflösbarem Typ mit graduierter Struktur $\mathfrak{R} = (R, T, \prec, \mathrm{lpp})$. Weiterhin sei I das von $F \subset R \setminus \{0\}$ erzeugte Linksideal von R. Die von $(Y_u)_{u\in T}$ erzeugte partielle Division $\mathcal{D} = (D_u)_{u\in T}$ sei auf der linear geordneten Menge $(\mathrm{lpp}(F), \sqsubset)$ der führenden Potenzprodukte der Elemente von F zulässig und die Elemente von $\mathrm{lpp}(F)$ seien paarweise nicht $\mathcal{D}$-Teiler voneinander. Dann sind die folgenden Eigenschaften zueinander äquivalent:

i) F ist eine $\mathcal{D}$-involutive Basis bezüglich $\mathfrak{R}$.

ii) Für alle $f \in F$ und $x \in X \setminus Y_{\mathrm{lpp}(f)}$ besitzt das Produkt xf eine Darstellung $xf = \sum_{i=1}^k c_i t_i f_i$ mit den Eigenschaften $0 \neq c_i \in \mathbb{K}$, $t_i \in T$, $f_i \in F$, $\mathrm{lpp}(f_i) \mid_D t_i \circ \mathrm{lpp}(f_i)$ für alle $i = 1, \ldots, k$ und $t_{i+1} \circ \mathrm{lpp}(f_{i+1}) \prec t_i \circ \mathrm{lpp}(f_i)$ für alle $i = 1, \ldots, k-1$.

iii) Für alle $f \in F$ und $x \in X \setminus Y_{\mathrm{lpp}(f)}$ existiert ein $f' \in F \setminus \{f\}$ mit $\mathrm{lpp}(f') \sqsubset \mathrm{lpp}(f)$, so daß zwischen den Elementen von F eine Relation der Gestalt $xf - ctf' = \sum_{i=1}^k h_i f_i$, wobei $0 \neq c \in \mathbb{K}$, $t \in T$, $0 \neq h_i \in R$, $f_i \in F$ sowie $\mathrm{lpp}(h_i) \circ \mathrm{lpp}(f_i) \prec x \circ \mathrm{lpp}(f) = t \circ \mathrm{lpp}(f')$ für alle $i = 1, \ldots, k$, besteht.

iv) F ist eine Gröbnerbasis von I bezüglich $\mathfrak{R}$ und es gilt $X \circ \mathrm{lpp}(F) \subseteq \bigcup_{f\in F} D_{\mathrm{lpp}(f)}$.

27. **[Satz 7.7]** Seien $\mathcal{D} = (D_t)_{t\in T}$ die von $(Y_t)_{t\in T}$ erzeugte partielle Division und $(U, \sqsubset)$ eine endliche linear geordnete Menge von Potenzprodukten. Für

jedes $t \in U$ erklären wir folgende drei Potenzproduktmengen: $A_t = \{X_i \in X \mid \exists v \in U : (t \sqsubset v \wedge t \in D_v \wedge X_i \notin Y_v)\}$, $B_t = \{v \in U \mid v \sqsubset t \wedge v \notin \mathrm{Id}_T(t)\}$ und $C_t = \{v \in U \mid v \sqsubset t \wedge D_v \not\subseteq t \circ \langle Y_t \cup \{X_i \in X \mid \deg_i(t) < \deg_i(v)\}\rangle\}$. Dann sind die folgenden Bedingungen zueinander äquivalent:

i) $\mathcal{D}$ ist zulässig für $(U, \sqsubset)$,

ii) für alle $t \in U$ ist Y_t eine unabhängige Menge des Potenzproduktideals $(A_t) + ((B_t) : (t)) \subseteq k[X]$,

iii) für alle $t \in U$ ist Y_t eine unabhängige Menge des Potenzproduktideals $(A_t) + ((C_t) : (t)) \subseteq k[X]$.

Sind alle Mengen Y_t mit $t \in U$ maximal unabhängig für das entsprechende Potenzproduktideal $(A_t) + ((B_t) : (t))$, so ist die die Äquivalenzklasse $[\mathcal{D}]_{\equiv_U}$ ein maximales Element von $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$ bezüglich $\leq_{\equiv_U}$. Ist umgekehrt $[\mathcal{D}]_{\equiv_U}$ ein bezüglich $\leq_{\equiv_U}$ maximales Element von $\mathbb{D}_{(U,\sqsubset)}/\equiv_U$, so sind alle Mengen Y_t mit $t \in U$ maximal unabhängig für $(A_t) + ((C_t) : (t))$.

28. Die unter 26. und 27. aufgeführten Ergebnisse bilden die Grundlage einer Reihe von Algorithmen. Algorithmus IBTest beruht auf Aussage 26*(ii)* und testet, ob eine endliche Menge F eine $\mathcal{D}$-involutive Basis bezüglich einer vorgegebenen partiellen Division $\mathcal{D}$ ist. Außerdem werden drei verschiedene Vervollständigkeitsmethoden InvBas1, 2, 3 angegeben. Die erste hält $\mathcal{D}$ über die gesamte Laufzeit fest, weshalb $\mathcal{D}$ auf der Menge der führenden Potenzprodukte jeder Zwischenbasis, also a priori auf ganz T, zulässig sein muß, und terminiert im allgemeinen nicht. Die zweite Methode paßt die partielle Division nach jedem erfolglosen Testdurchlauf an das neue Zwischenerzeugendensystem an. Wählt man für $\mathcal{D}$ immer eine bezüglich der Verfeinerungshalbordnung (sub-) maximale zulässige partielle Division aus, so ist die Termination des Algorithmus gesichert. Bedingung 27*(ii)* liefert einen Algorithmus PartDivOrd zur Berechnung aller auf einer vorgegebenen Potenzproduktmenge zulässigen partiellen Divisionen. SubMaxVerf beruht auf 27*(iii)* und erlaubt die zulässige Verfeinerung einer gegebenen partiellen Division. Dabei wird eine Submaximalität erreicht, welche bereits die Termination von Algorithmus InvBas2 sichert. Um nicht bereits früher ausgeführte Nullreduktionstests wiederholen zu müssen, bedarf es weiterer Einschränkungen und eines auf Bedingung 26*(iii)* fußenden Korrektheitsbeweises. Die Änderungen und Verbesserungen führen schließlich auf Algorithmus InvBas3.

29. Schließlich werden Fragen der Strategieauswahl bei der involutiven Methode diskutiert und ein Vergleich mit dem Buchbergeralgorithmus vorgenommen. Insbesondere wird herausgearbeitet, daß die involutive Methode nur einen Unterschied aufweist, der für ihren empirisch ermittelten Geschwindigkeitsvorteil verantwortlich sein könnte und es zeigt sich, daß dieser die heute üblichen Kompromisse des Buchbergeralgorithmus noch konsequenter umsetzt und damit erneut experimentell bestätigt.

30. Eine Vielzahl der in der Arbeit vorgestellten Algorithmen wurde im Spezialcomputeralgebrasystem Felix implementiert.