Solvable Polynomial Rings

Von der Fakultät für Mathematik und Informatik
der Universität Passau
genehmigte Dissertation
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften

vorgelegt von

Diplom Mathematiker Heinz Kredel
Passau 1992

Preface

This work treats solvable polynomial rings, which can be characterized as commutative polynomial rings with a new non-commutative multiplication $*$, such that the $*$-product of two polynomials is the sum of a commutative polynomial, smaller with respect to a fixed quasi order on the polynomials and a head monomial which is is equal to a scalar multiple of the head term of the commutative product.

We show under which conditions, the 'classical' topics of computational commutative polynomial ring theory – such as Noetherianity, Gröbner bases, Buchberger algorithm, standard representations, elimination ideals, residue class rings, syzygies, module and subalgebra bases – can be carried over to the theory of suitable solvable polynomial rings. Furthermore we identify methods not applicable in the theory of solvable polynomial rings. We present programs for the solution of several problems and discuss computing examples.

We develop the method of comprehensive Gröbner bases for solvable polynomial rings and use it in the model theory of (suitable) algebraically complete structures to show that these structures are axiomizable and allow elimination of existential quantifiers.

A detailed introduction and overview is given in the first chapter.

Acknowledgements

At first I thank Prof. Dr. V. Weispfenning for the encouragement to the development of this work and many suggestions and hints to various mistakes. He introduced me to the theory of solvable polynomial rings and to model theory. Furthermore he gave me the opportunity to work at the university of Passau on computer algebra. I also thank T. Becker, M. Pesch and the students of the seminars, where I could present parts of this work, for their patience and helpful discussions. In particular T. Becker provided me with much insight into standard representations. I also learnt much from the cooperation with V. Weispfenning and T. Becker in writing a book on commutative computational algebra.

Furthermore I thank J. Apel and U. Klaus for valuable discussions on the implementation of non-commutative polynomial rings. In commutative Gröbner base theory I learnt most from B. Buchberger and in non-commutative Gröbner base theory I learnt many facts form T. Mora. In the development of MAS, which could not be presented here, I profited from valuable discussions with M. Wirsing.

Finally I thank my wife Lioba and my son Samuel for their patience and support. Also I owe much to my parents.

Technical Notes

All examples, definitions, lemmas, propositions and theorems are numbered first after the chapter, then after the section and then consecutively within the section. So cross-reference 'lemma 4.5.2' refers to item '2' of section '5' of chapter '4'. The end of a proof is indicated by '□'.

Citations are in the form '[Buchberger 1965]', which indicates first the family name of the author(s) 'Buchberger' and then the year of publication '1965'. Publications within the same year are distinguished by small letters 'a', 'b', etc.

At the end there is a list of special notations, an author index and a subject index refering to the page numbers where an item appears.

Printing Notes

This is the corrected Dissertation as approved by the Promotionsausschuß of the Fakultät für Mathematik und Informatik of the Universität Passau. The Dissertation was submitted on May 24, 1992 and has been refereed by Prof. Dr. V. Weispfenning and Prof. Dr. N. Schwartz. The Rigorosum was held on November 12, 1992 under supervision of Prof. Dr. B. Schmidt. The examiners were Prof. Dr. V. Weispfenning, Prof. Dr. N. Schwartz, Prof. Dr. H. Volger and Prof. Dr. M. Kaufmann.

Passau, December 15, 1992 H. Kredel

Contents

List of Tables

Chapter 1

Introduction

If we compare commutative rings with non-commutative rings and in particular commutative polynomial rings over fields with non-commutative polynomial rings over skew fields, we observe, that several properties no longer hold in the latter cases. Most remarkably non-commutative rings are in general no more Noetherian. Even if we restrict our interest to non-commutative Noetherian rings many properties of commutative Noetherian rings do no longer hold. Notably the residue class rings modulo a prime ideal need not be integral domains. In commutative field theory the algebraic closure of a field is a 'well' behaving object, in non-commutative field theory the analogue, the existentially closed fields, are in general not even an axiomatic class, i.e. they cannot be characterized by a set of (first order) axioms (not even an infinite set of axioms).

On the other hand there do exist non-commutative Noetherian rings, which have 'good' properties. Namely the enveloping algebras of Lie algebras, skew polynomial rings (iterated Ore extensions) and skew Laurent series rings. There are several attempts to characterize non-commutative rings as rings with relations. In our characterization of such rings we emphasize algorithmical computability. That means, that for most definitions and propositions, we insist that there exist algorithms (potentially implementable on a computer under some restrictions) which can carry out the abstract constructions involved.

Guided by the development of notions compatible with computational methods – Gröbner bases, Buchberger algorithm, comprehensive Gröbner bases – we are nevertheless able to obtain some far reaching results and characterizations. Most notable, the algebraically closed skew fields arising from a subclass of the class of polynomial rings under consideration are indeed an axiomatic class.

In the next section we give a closer overview of the work, then we attempt to trace some of the sources and related work in the literature. Finally we mention some open problems and possible future directions of research.

1.1 Overview

Starting point of the current work was the theory of solvable polynomial rings that has first been introduced by [El From 1983] and Gröbner bases in these rings by [Kandri-Rody, Weispfenning 1988]. They can be characterized as commutative polynomial rings with a new non-commutative multiplication $*$, such that the $*$-product of two polynomials is a sum of a commutative polynomial, smaller with respect to a fixed quasi order on the polynomials and a head monomial which is is equal to a scalar multiple of the head term of the commutative product. There are several types of rings that can be treated within this framework: commutative polynomial rings, enveloping algebras of finite dimensional Lie algebras and iterated Ore extensions of a field $\mathbf{K}$ introducing only K-derivations.

The concrete guideline of the current work is the following problem:

> how much can the axioms of solvable polynomials be relaxed such that we can still compute with the elements and there is still a sufficiently interesting amount of commutative ring and ideal theory which can be carried over to these generalized solvable polynomial rings.

Thus the main topics with which we are concerned are:

1. solvable polynomial rings where the coefficients may not commute with the variables, conditions on the parameters of multiplication imposed by the associativity of solvable polynomial rings, conditions for the validity a Hilbert's basis theorem, structure of the center;
2. left, right, two-sided ideals and the existence of confluent reduction relations and Gröbner bases;
3. applications: elimination ideals, syzygies, homogeneous ideals, partial Gröbner bases, modules over solvable polynomial rings, subalgebras of solvable polynomial rings;
4. implementation issues of the computation in solvable polynomial rings, sample computations;
5. properties of Gröbner bases under specialization of the coefficients, existence of comprehensive Gröbner bases;
6. Nullstellensätze, existentially closed structures and model theory.

Solvable polynomial rings in the present sense are axiomatically characterized in chapter 3. In the earlier works of [El From 1983] and [Kandri-Rody, Weispfenning 1988] it is assumed, that the coefficients commute with the variables of the polynomial ring; we generalize this theory to solvable polynomial rings where the coefficients may not commute with the variables. We will continue to call the rings satisfying the modified axioms:

'solvable polynomial rings'. With this more general concept we can treat the theory of difference rings, differential rings and arbitrary Ore extension rings over a (non-commutative) field in our framework. Furthermore we give conditions, when homomorphic images of free associative algebras are solvable polynomial rings.

Using a combination of Dickson's lemma and a variant of Königs tree lemma we give a proof of a 'Hilbert basis theorem' for solvable polynomial rings over Noetherian coefficient rings. Next the structure of the center of a solvable polynomial ring is determined and by linear algebra methods, ways to compute elements in the center are investigated. This has important applications concerning the determination of the so called 'Casimir invariants' in the theory of Lie algebras. In chapter 6 we apply our methods and programs to examples from the literature.

In the chapter **Ideals and Gröbner bases** 4 we discuss appropriate reduction relations and standard representations. We define Gröbner bases as ideal bases such that the corresponding reduction relation is confluent and we show that solvable polynomial rings admit the construction of left (right, two-sided) Gröbner bases The proofs are based on standard representaion methods, since the respective reduction relation methods seemed to be too tedious to apply. Furthermore we give a proof of the second Buchberger criterion in order to avoid the consideration of unnecessary critical pairs (S-polynomials).

Applications and further topics in the theory of solvable polynomial are treated in chapter 5. We show that the 'classical' applications of Gröbner bases, such as, elimination ideals, residue class rings and generators for syzygy modules hold for solvable polynomial rings as well. Moreover we discuss graded solvable polynomial rings and homogeneous ideals with partial Gröbner bases. Here a difficulty arises, since the $*$-product of homogeneous polynomials is in general no more homogeneous, so only homogeneity respecting gradings can be used. These results are then applied to free (left) modules over solvable polynomial rings. Finally we treat bases for subalgebras of solvable polynomial rings. We remark, that the tag variable method to solve the subalgebra membership problem can not be used in case of subalgebras of solvable polynomial rings. However we are able to show that a basis completion method exists, such that there exists a semi-decision procedure to solve the subalgebra membership problem.

Implementation issues of the **computation in solvable polynomial rings** are discussed in chapter 6. We present an implementation of the $*$-product, left and (improved) two-sided Gröbner bases algorithms in the MAS computer algebra system developed by the author. Much attention is put on a fast implementation of the $*$-product using the method of relation tables, which memorizes and reuses partial products to avoid to many recomputations. Also some computing time statistics and some notes on the complexity are given. In the implemented algorithms we assume that the coefficients commute with the variables. Part of this chapter has been presented in [Kredel 1990a]. Furthermore we present algorithms for the computation of elements in the center and the computation of univariate polynomials of minimal degree in an ideal. The programs are applied to various examples (centers, minimal generating systems) found in physics journals in order to demonstrate the workability of the methods.

Comprehensive Gröbner bases are treated in chapter 7. In this chapter we restrict the

solvable polynomial rings to the case where the coefficients commute with the variables. Comprehensive Gröbner bases for commutative polynomial rings have been introduced by [Weispfenning 1990]. Comprehensive Gröbner bases are characterized as ideal bases, such that for every specialization of the parameters in the coefficients of the polynomials, the resulting ideal base is a Gröbner base in the specialized solvable polynomial ring.

In this context, we consider solvable polynomial rings over rings containing parameters and show that a product lemma holds. Also reductions and S-polynomials can be defined in this parametric case. We show that comprehensive Gröbner bases exist for ideals in solvable polynomial rings and that they can be constructed in a finite number of steps. Consequences are, that there exist (for every fixed degree bound) ideal bases, such that *all* Gröbner bases can be obtained simply by specialization from them. Part of this chapter is a joint work with V. Weispfenning and has been presented in [Kredel, Weispfenning 1990].

Nullstellensätze and some model theory of solvable polynomial rings are discussed in chapter 8. Here we prove first a 'weak Nullstellensatz' based on the results that in iterated Ore extensions over the rational numbers prime ideals are completely prime.

Using the amalgamation property of skew fields and comprehensive Gröbner bases we obtain furthermore axiomatizability and eliminaton of existential quantifiers for algebraically closed skew fields 'compatible' with solvable polynomial rings. Furthermore we prove 'strong Nullstellensätze' for existentially (and algebraically) closed skew fields 'compatible' with solvable polynomial rings. Using the parametric ideal membership test provided by comprehensive Gröbner bases we show, that there exists uniform bounds on the degrees of polynomials required to represent a polynomial as member of an ideal.

In chapter 2 we recall and fix some definitions from universal algebra. In a second section we prove some (known) basic properties of two-sided ideals in non-commutative rings used in later. The whole chapter may be skipped by those readers familiar with universal algebra and non-commutative ring theory, or read when necessary.

In appendix A we discuss the requirements for more **general solvable polynomial rings**, where the condition that the head term of the polynomials under the $*$-product is equal to the head term of the commutative product is dropped. Prominent structures in this class are Grassmann (exterior) algebras (it is known, that Gröbner bases exist in this case). However not much positive results have been achieved with this concept. But in chapter 3 we show that Grassmann and Clifford algebras can be treated as residue rings of solvable polynomial rings.

The **main results** of this work are

- We show that the 'classical' topics of (computational) commutative polynomial ring and ideal theory can be transfered to the theory of suitable solvable polynomial rings. We specify the conditions under which this is possible and we identify methods not applicable in the theory of solvable polynomial rings.
- We develop the method of comprehensive Gröbner bases for solvable polynomial rings and use it in the model theory of (Q-) algebraically closed structures in order to show that they are axiomatizable and allow elimination of existential quantifiers.

1.2 Sources and Related Work

The main sources of this work are: (commutative) Gröbner base theory, non-commutative Noetherian rings and model theory. In this section we attempt to trace down the background and the work of other people.

Text books and surveys are:

commutative algebra:
[V. d. Waerden 1971] and [Zariski, Samuel 1958/60]

commutative algebraic geometry:
[Gröbner 1968/70], [Kunz 1980]

survey on computer algebra:
[Buchberger *et. al.* 1982]

non-commutative (Noetherian) fields, rings and modules:
[Cohn 1971], [Anderson, Fuller 1974], [Cohn 1977],
[McConnell, Robson 1987] and [Goodearl, Warfield 1989]

categories:
[Blyth 1986]

universal algebra:
[Ihringer 1988] and [Cohn 1981]

model theory:
[Robinson 1974], [Hirschfeld, Wheeler 1975], [Potthoff 1981], [Prestel 1986]
and [Cohn 1981]

Lie algebras and enveloping algebras of Lie algebras:
[Jacobson 1962], [Dixmier 1974], [Bohro, Gabriel, Rentschler 1973]

differential algebras and difference algebras:
[Ritt 1950], [Kolchin 1973] and [Cohn 1965]

Gröbner base theory of commutative polynomial rings has been invented and developed by [Buchberger 1965] and subsequent publications; a survey on this topic including further references is given in [Buchberger 1985]. A text book of computational algebra with Gröbner bases will be available with [Becker, Weispfenning 1992].

Confluent *reduction relations* in ring theory are discussed by [Bergman 1978] and in a general setting by [Huet 1980]. The basic termination criterion on which all proofs rely has been provided by [Dickson 1913]. Detection of superfluous critical pairs is discussed by various authors, e.g. by [Buchberger 1979] and [Becker 1991].

Ring and *ideal theory* of non-commutative Noetherian domains has been studied among others by [Noether, Schmeidler 1920], [Ore 1931] and [Ore 1933]. Conditions under

which an associative algebra is *Noetherian* have been given in [Lesieur, Croisot 1963], [Lesieur 1978] and also [Gateva-Ivanova 1988].

The theory of Gröbner bases for *free* non-commutative polynomial rings has been studied by [Mora 1985], [Mora 1986], [Mora 1988]. Free non-commutative polynomial rings modulo some non-commutative Gröbner bases have been investigated by [Apel 1988]. It is shown, that enveloping algebras of Lie algebras can be handled within this framework. The construction of *matrix representations* for finitely presented (also free) non-commutative algebras is presented by [Labonté 1990]. As mentioned already, ring, ideal and dimension theory of solvable polynomial rings has been studied by [El From 1983] and Gröbner bases in these rings by [Kandri-Rody, Weispfenning 1988].

Lie algebras are of general importance in mathematics and physics. For an introduction and overview see [Jacobson 1962]; universal *enveloping algebras* of Lie algebras are treated in [Bohro, Gabriel, Rentschler 1973] and [Dixmier 1974]. Gröbner base theory of enveloping algebras has been introduced by [Lassner 1985] and furthermore by [Apel, Lassner 1988], [Apel 1988].

The structure of the *center* of finite dimensional Lie algebras, and of enveloping algebras of Lie algebras, is discussed by [Abellanas, Martinez 1975], [Beck *et. al.* 1976], [Conatser, Huddleston 1976] and also by [Patera *et. al.* 1976], [Zassenhaus 1976]. Elements of the center are important invariants, which can be used to label irreducible representations of a given Lie algebra. The authors give characterizations of the center and show how to compute elements in the center by means of solving partial differential equations. In particular Casimir invariants (elements of the enveloping algebra of Lie algebra under consideration, i.e. polynomials) are determined. Furthermore they determine also functional invariants (in terms of exponential functions of rational functions). They present tables of those invariants for low dimensional Lie algebras. They do not determine non-functional invariants like distributions with their methods. The computation of polynomial invariants lies within the scope of our methods and we veryfied the results of the authors in these cases.

Properties of *Weyl algebras*, in particular the number of generators of ideals, are discussed in [Dixmier 1968/70] and [Stafford 1978] (who showed, that any left ideal in a Weyl algebra is generated by at most two elements). A special class of algebras similar to the enveloping algebra of $sl(2)$ is treated in depth by [Smith 1990]. Especially the structure of its center and the structure of two-sided ideals is determined.

Gröbner bases of ideals of *differential operator* rings especially of Weyl algebras are discussed by [Galligo 1985]. Gröbner bases for *modules* of differential and *difference* rings are discussed in [Pankrat'ev 1989]. For overviews on the theory of differential algebras see [Ritt 1950], [Kolchin 1973] and on the theory of difference algebras see [Cohn 1965].

Exploiting the fact, that *exterior algebras* (Grassmann algebras) are finite dimensional vector spaces, [Stokes 1989] developed Gröbner bases for this class of algebras.

Applications of Gröbner base theory to the computation of generators of the *syzygy module* of a set of polynomials is discussed in [Zacharias 1978]. Computation of *univariate polynomials* of minimal degree in zero dimensional ideals is reported in [Böge *et. al.* 1986].

Canonical bases for *modules* over commutative polynomial rings are discussed in [Armbruster, Kredel 1986], [Möller, Mora 1986] and [Furukawa *et. al.* 1986]. *Subalgebra* membership and canonical subalgebra bases are treated by tag variable methods in [Shannon, Sweedler 1988], by standard representations in [Robbiano, Sweedler 1988] and by term rewrite completion methods in [Kapur, Madlener 1989].

Implementation issues for computing in non-commutative polynomial rings are addressed by [Apel, Klaus 1990], [Apel, Klaus 1991] and [Petermann, Apel 1988]. Implementation issues for the *Buchberger algorithm* for the computation of Gröbner bases are discussed by [Winkler *et. al.* 1985] (and various others). Our implementation is based on the 'ALDES/SAC-2' computer algebra system by [Collins, Loos 1980], the distributive polynomial system by [Gebauer, Kredel 1983] and an implementation of Buchberger's algorithm [Gebauer, Kredel 1984], [Kredel 1988a]. The recent implementation is in the 'MAS Modula-2 algebra system' by [Kredel 1988], [Kredel 1990] and [Kredel 1991]. An implementation of the algorithms for syzygy computations is given in [Philipp 1991].

Some special cases of *parametric problems* in commutative theory, such as parametric linear equations are discussed by [Sit 1991] and parametric equations by [Gao, Chou 1991]. Properties of Gröbner bases under *specialization* are discussed by [Gianni 1987]. The algorithms for comprehensive Gröbner bases in the commutative case are implemented in [Schönfeld 1991].

The theory of Ore extensions and in particular the question under which conditions prime ideals are *completely* prime are discussed in [Lorenz 1981], [Sigurdsson 1984] and [Dixmier 1974] (for the case of solvable Lie algebras). For an overview see [Goodearl, Warfield 1989].

The question under which conditions a ring can be *embedded* in a field are discussed by [Malcev 1937], [Cohn 1971], [Hirschfeld, Wheeler 1975] and [Cohn 1977] with a survey in [Cohn 1981].

Model theory of algebraically closed non-commutative groups and fields is discussed in [Robinson 1971], [Bacsich 1972], [Simmons 1972] and [Bacsich 1973]. A model theoretic framework for *Nullstellensätze*, using syntactic characterizations of radicals and radical membership, is presented in [Weispfenning 1977]. Non-commutative existentially closed structures and a non-commutative Nullstellensatz is given in [Hirschfeld, Wheeler 1975]. Aspects of quantifier elimination relative to sets of formulas and relative to formular preserving morphisms are discussed in [Weispfenning 1983]. This article also gives an overview over (relative) quantifier elimination in various algebraic theories. Non-commutative *geometry* is discussed e.g. in [Manin 1991] and also in several articles in Physics journals and lecture notes.

1.3 Future Perspectives and Open Problems

There are several topics in commutative Gröbner base theory, which have not been discussed in the present work. The most notable are:

1. Development of a theory of solvable polynomial rings over *Euclidean* coefficient domains, or Dedekind domains. (We deliberately omit references.)

2. Gröbner bases with respect to every term order, so called *universal Gröbner bases*, stability of Gröbner bases under change of the term ordering [Robbiano 1985], [Weispfenning 1987], [Weispfenning 1987] and [Schwartz 1988].

3. Dimension theory for solvable polynomial rings as in the commutative case [Kredel, Weispfenning 1988], Hilbert function, Gelfand-Kirillov dimension.

4. Ideal *decomposition* theory for solvable polynomial rings. (We deliberately omit references.)

5. Using the framework of [Becker 1990] to derive solvable *power series rings* and also comprehensive Gröbner bases for power series rings.

6. Implementation of algorithms for solvable polynomial rings where the variables do not commute with the coefficients. Implementation of algorithms for the construction of comprehensive Gröbner bases for solvable polynomial rings .

7. The class of solvable polynomial rings over computable rings provides a computational domain with Gröbner bases as complete constraint solvers for the theory of *constrained logic programming* (CLP) [Jaffar, Lassez 1987].

1.4 Summary

For easy orientation we place this section, which contains a summary and draws some conclusions, at the end of the introduction. The section is however intended to be read after the other chapters. We will deliberately use (also technical) notations from the rest of the work.

In the following two subsections we give a summary of the results about solvable polynomial rings and extension fields 'compatible' with solvable polynomial rings obtained in this work. In the third subsection we draw some conclusions.

1.4.1 Solvable Polynomial Rings

In table 1.1 we summarize various properties and results on solvable polynomial rings.

The table is organized such that the row boxes surround the chapters, which can be easily identified. The column boxes show first an abbreviation of properties and/or results and then the main characteristics of solvable polynomial rings as there are the coefficient field $\mathbf{K}$ and then the commutator relations Q respectively Q'.

The entries in the column labelled $\mathbf{K}$ indicate what kind of restriction is placed on the coefficient field

'skew' means, that **K** may be a skew field.

'comm.' means, that **K** must be a commutative field.

'ring' means, that **K** may be a ring, possibly with some further restriction.

The entries in the columns labelled Q and Q' indicate whether the results hold for arbitrary commutator relations or hold only for relations where Q' specifies commutativity. I.e. 'yes' means, that the result holds (for arbitrary commutator relations), 'no' means, that the result does not hold (i.e. it holds only for relations where Q' specifies commutativity), 'not considered' means, that the result has not been considered and a reference means that the result holds and was proven in the reference.

The further entries read as follows:

'(old)' means, that the corresponding result has been known, together with an abbreviated reference who obtained it.

'(new)' means, that the corresponding result was obtained in this work.

'(?)' means, it is not known, if the corresponding result holds, together with an indication about our opinion if it could hold.

The references have the following meaning:
AL = [Apel, Lassner 1988], KW = [Kandri-Rody, Weispfenning 1988] and
W = [Kredel, Weispfenning 1990]. 'GB' stands as abbreviation for Gröbner base. '**Q**' denotes the field of rational numbers.

The notes in table 1.1 are explained as follows:

[1] the coefficient rings must be skew fields or the commutator relations must be such, that the c_{ij} respectively the c_{ai} are contained in a subfield of the center of **K**,

[2] only if $\alpha_i : a \mapsto c_{ai}a$ is an automorphism,

[3] if $Q' \neq \emptyset$, then construction only if **K** is a finitely generated algebra over its center,

[4] only for $*$-compatible inverse lexicographical term orders,

[5] only for $*$-homogeneity compatible gradings,

[6] in general infinite objects, a semi-decision procedure for subalgebra membership.

[7] with parametric commutator relations,

[8] only for certain commutator relations.

[9] for fixed Q, Q' and coefficient rings 'compatible' with Q'.

$$\mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$$

properties, results	$\mathbf{K}$	Q	Q'
variety	ring	yes	yes[9]
$*$-product	skew (new)	KW (old)	yes (new)
Ore extensions	skew (new)	KW (old)	yes (new)
Hilbert Basissatz	restr. ring[1] (new)	yes[1] (new)	yes (new)
center structure	comm. (new)	yes (new)	no (?)
left Gröbner bases	skew (new)	KW (old)	yes (new)
BBEC criterion	skew (new)	yes (new)	yes (new)
BBGC criterion	skew (new)	no, AL (old)	no
right Gröbner bases	skew (new)	KW (old)	restriction[2] (new)
two-sided Gröbner bases	skew (new)	KW (old)	restriction[2] (new)
t-s GB, contruction	restriction[3] (new)	KW (old)	restriction[2] (new)
elimination ideals	skew (new)	KW[4] (old)	yes[4] (new)
residue class ring bases	skew (new)	KW (old)	yes (new)
basis for syzygies	skew (new)	KW (old)	yes (new)
partial Gröbner bases	skew (new)	yes[5] (new)	yes[5] (new)
module Gröbner bases	skew (new)	yes (new)	yes (new)
subalgebra GB[6]	comm. (new)	yes (new)	no (?)
parametric solvable rings	parm. ring	with W[7] (new)	(?)
comprehensive left GB	parm. ring	with W (new)	(?)
comp. two-sided GB	parm. ring	with W (new)	(?)
par. ideal membership	parm. ring	with W (new)	(?)
implementation			
$*$-product	**Q** (new)	yes (new)	not considered
left Gröbner bases	**Q** (new)	yes (new)	not considered
two-sided GB	**Q** (new)	yes (new)	not considered
BBEC criterion	**Q** (new)	yes (new)	not considered
elements of the center	**Q** (new)	yes (new)	not considered
generalized axioms		zero divisors	zero divisors
$*$-product	skew (new)	yes (new)	yes (new)
left reduction		no	not considered
left saturated reduction		yes[8]	not considered
left Gröbner base		yes ?	not considered

Table 1.1: Summary of Solvable Polynomial Rings

In the sequel we will give some further remarks.

The field **K** is mostly of arbitrary characteristic. Some times it must be of characteristic 0 so that **Q** is contained in the center. The term order $<$ is always fixed, admissible and $*$-compatible.

We adapted the method of standard representations for solvable polynomial rings. In our opinion this method makes the proofs of the construction of (left) Gröbner bases much more intelligible and could be also be used for the proof of the BBEC criterion.

1.4.2 Nullstellensätze

A schematic summary of the results of this work in respect to various 'Nullstellensätze' is contained in table 1.2.

The references have the following meaning: HW = [Hirschfeld, Wheeler 1975]. The other entries have the same meaning as in the preceding section.

A listing of properties of existentially closed classes for various algebraic structures can be found in [Hirschfeld, Wheeler 1975](pp 134–136).

properties, results	existential	Q-algebraic	Q-existential
existance of roots			
in extension field	yes, HW (old)	yes (new)	yes (new)
in all closed extensions	yes, HW (old)	yes (new)	yes (new)
one cl.ext $\rightarrow$ all cl.ext.	no, HW (old)	yes (new)	yes (new)
exist. of degree bounds[3]	no, HW (old)	yes (new)	no (?)
Rabinowich trick		no[1]	no[1]
EC			
elementary class	no	no	no
axiomatizable class	no, HW (old)	yes (new)	no (?)
quantifier elimination	no, HW (old)	yes[2] (new)	no (?)

Table 1.2: Summary of Nullstellensätze

The notes in table 1.2 are explained as follows:

[1] only true, if one accepts infinite formulas,

[2] only existential quantifiers.

[3] uniform bounds on the degrees of the polynomials which are used to represent a polynomial as member of an ideal.

In the sequel we will give some further remarks.

The field **K** must be of characteristic 0, i.e. an extension of **Q**. The term order $<$ is always fixed, admissible, $*$-compatible and strict lexicographic.

1.4.3 Concluding Remarks

One of the main problems was to find a suitable notion of 'most general' solvable polynomial rings. Our first idea to allow also zero divisors (to be able to incorporate e.g. exterior algebras) was not fruitful. Although a product lemma holds for arbitrary polynomials a suitable (saturated) reduction could only be defined for special cases of commutator relations. The rests of these attempts have been included in the appendix A and may become useful later.

The most fruitful concept was to consider solvable polynomial rings

$$S = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$$

characterized as polynomial rings over skew fields $\mathbf{K}$ in variables $X_1, \ldots, X_n$, $n \geq 0$, together with a new non-commutative product '$*$', defined by means of commutator relations

$$Q = \{X_j * X_i = c_{ij} X_i X_j + p_{ij} \ : \ 0 \neq c_{ij} \in \mathbf{K},\ X_i X_j > p_{ij} \in S,\ 1 \leq i < j \leq n\}$$

between the variables and commutator relations

$$Q' = \{X_i * a = c_{ai} a X_i + p_{ai} \ : \ 0 \neq c_{ai} \in \mathbf{K},\ p_{ai} \in \mathbf{K},\ 1 \leq i \leq n,\ a \in \mathbf{K}\}$$

between the variables and the coefficients with respect to a $*$-compatible term order $<$, such that the ring $(S, 0, 1, +, -, *)$ is associative.

We showed, that many of the properties of commutative polynomial rings and solvable polynomial rings as defined by [Kandri-Rody, Weispfenning 1988] could be carried over to these 'more general' solvable polynomial rings. Although at a first glance this kind of generalization may appear to be a 'routine' task, many subtle investigations showed up cases, where a corresponding result for the more general solvable polynomial rings is false (e.g. construction of two-sided Gröbner bases, subalgebra membership test by tag variables, etc.). Moreover the successful cases often required (tedious) proofs by Noetherian induction over the remainders generated by the $*$-product (e.g. for the $*$-product for polynomials).

In the chapter on the Nullstellensätze we used methods from different areas of mathematics to establish axiomatizability and quantifier elimination for the class of Q-algebraically closed extension fields of $\mathbf{Q}$. Most notably are methods from algebra (differential operator rings, Ore domains, non-commutative Noetherian rings, free product of skew fields), computer algebra (Gröbner bases, comprehensive Gröbner bases) and model theory (existentially and algebraically closed structures, quantifier elimination). Furthermore the efficient implementations for computations in solvable polynomial rings and the implementations (by [Schönfeld 1991]) for computations of comprehensive Gröbner bases in commutative polynomial rings give hope for an efficient and practicable quantifier elimination procedure in Q-algebraically closed extension fields of $\mathbf{Q}$.

Chapter 2

Non-commutative Rings

In this chapter we first summarize some definitions and notations about universal algebra and non-commutative rings. Then we prove some basic properties of (two-sided) ideals of non-commutative rings. Notably a separation lemma of an ideal with respect to a multiplicatively closed set. Furthermore we include some facts on semiprime ideals. The results of this section are mainly used in chapter 8.

2.1 Notations and Definitions

We assume the basic notations and properties of sets, relations and functions. $\mathbf{N}$ denotes the set of natural numbers (including zero) and $\mathbf{Z}$ denotes the set of integers (integral numbers). $|A|$ denotes the cardinality of the set A. $A \times B$ denotes the cartesian product of the sets A and B.

A formal language L is characterized by a tuple (R, F, σ, C, V), where R is a set of relation symbols, F is a set of function symbols, σ is the arity function, C is a set of constants and V is an enumerable set of variables. Let L be a formal language, let A be an algebraic structure, then A is called an L-structure, if all operator symbols of the language L have an interpretation in A. A homomorphism between L-structures is a mapping that respects the operations. Substructures and extension structures are defined as usual and we write $A \sqsubseteq B$ for A is a substructure of B.

For a given language and set of variables, the set of first order terms is denoted by $\mathtt{Tm}$ and the set of first order formulas is denoted by $\mathtt{Fm}$, respectively by $\mathtt{PFm}$ for prime or atomic formulas. For terms $t \in \mathtt{Tm}$ and formulas $\varphi \in \mathtt{PFm}$ we define the set of *free variables* $\mathtt{FV}(t)$, $\mathtt{FV}(\varphi)$ and the set of *bound variables* $\mathtt{BV}(t)$, $\mathtt{BV}(\varphi)$ as usual.

Let **true** and **false** be two objects distinct from the universe of A. For a formula $\varphi \in \mathtt{Fm}(L, V)$ we write $A \models \varphi$ if for all variable assignments $\alpha : V \longrightarrow A$, φ^α holds in A, i.e. $\varphi^\alpha = \mathbf{true}$. In this case we say '$A$ satisfies φ' or also 'A is a model of φ'. We write $A \models \varphi(a_1, \ldots, a_n)$ if 'φ holds at $(a_1, \ldots, a_n)$ in A'. If Φ is a set of formulas, we write

$A \models \Phi \iff A \models \varphi$ for all $\varphi \in \Phi$. In this case we say 'A satisfies Φ' or also 'A is a model Φ'.

An *unitary ring* is a structure $(R, +, -, \cdot, 0, 1)$ with universe R, functions $+, -, \cdot$ and distinguished constants $0, 1$. A *commutative ring* is an (unitary) ring, where $\cdot$ is commutative. An *integral domain* or for short a *domain* is an (unitary) ring that has no zero divisors. Since all rings which we will consider are unitary rings, we drop the word 'unitary' from now on. We will furthermore assume that always $1 \neq 0$ holds.

A field K is a ring, such that for every $0 \neq a \in K$ there exists a $b \in K$ such that $ab = 1$. Note, that fields are in general not necessary commutative. Some authors denote this fact by speaking explicitly of *skew fields* when they refer to non (necessarily) commutative fields. Here however we will state explicitly when we require a field to be commutative.

For a ring R a left unitary R-module with universe M will be denoted by ${}_RM = (M, +, -, 0, 1, R)$. Again we will drop 'unitary' since we consider only unitary R-modules. Let K be a field. Then the K-module M is called a *vector space*. For rings R and S a *unitary R-S-bimodule* is denoted by ${}_RM_S = (M, +, -, 0, 1, R, S)$.

Let $(R, +, -, \cdot, 0, 1)$ be a ring. An *R-algebra* is denoted by $A_R = (A, +, -, \cdot, 0, 1, R)$. Let R be a ring, X a set of variables. A *polynomial ring over R in the variables X* is denoted by $R[X]$. If $X = \{X_1, \ldots, X_n\}$ is finite, we write also

$$R[X_1, \ldots, X_n]$$

for a polynomial ring. We assume that the variables commute with the coefficients, but we do not assume, that the coefficient ring itself is commutative in general.

Definition 2.1.1 (Ideal) *A* left ideal *in a ring $(R, +, -, \cdot, 0, 1)$ is a subset I of R such that*

I0: $0 \in I$,

Ia: *if $a, b \in I$, then $a + b \in I$,*

Il: *if $a \in I$, $r \in R$ then $ra \in I$.*

A right ideal *in a ring $(R, +, -, \cdot, 0, 1)$ is a subset I of R such that*

I0: $0 \in I$,

Ia: *if $a, b \in I$, then $a + b \in I$,*

Ir: *if $a \in I$, $r \in R$ then $ar \in I$.*

A two-sided ideal *in a ring $(R, +, -, \cdot, 0, 1)$ is a subset I of R such that*

I0: $0 \in I$,

Ia: *if $a, b \in I$, then $a + b \in I$,*

It: *if $a \in I$, $r \in R$ then $ra \in I$ and $ar \in I$.*

Since R is assumed to be unitary, 'It' can also be written as

It': *if $a \in I$, $r, s \in R$ then $ras \in I$.*

Definition 2.1.2 *We say a left (right, two-sided) ideal is* generated by a set F, $F \subseteq R$ *if it is of the form:*

$$\begin{aligned}
\mathrm{ideal}_l(F) &= \{ \sum_{i\in\Lambda} r_i a_i \ : \ r_i \in R, a_i \in F, \Lambda \textit{ finite} \}, \\
\mathrm{ideal}_r(F) &= \{ \sum_{i\in\Lambda} a_i r_i \ : \ r_i \in R, a_i \in F, \Lambda \textit{ finite} \}, \\
\mathrm{ideal}_t(F) &= \{ \sum_{i\in\Lambda} r_i a_i s_i \ : \ r_i, s_i \in R, a_i \in F, \Lambda \textit{ finite} \}.
\end{aligned}$$

If an ideal I is generated by a set F we also say F is a basis for I. *An left (right, two-sided) ideal I is called* trivial, *if $I = \{0\}$ and it is called* proper, *if $I \neq R$.*

If $F = \{f_1, \ldots, f_n\} \subseteq R$ is finite, then we write also $\mathrm{ideal}_{l,r,t}(f_1, \ldots, f_n)$ *for* $\mathrm{ideal}_{l,r,t}(F)$. *In particular if I is an ideal, then $I = \mathrm{ideal}(I)$.*

Definition 2.1.3 *Let $F_1, F_2 \subseteq R$ then we define*

$$\begin{aligned}
\mathrm{ideal}(F_1) + \mathrm{ideal}(F_2) &= \mathrm{ideal}(F_1 \cup F_2) \\
\mathrm{ideal}(F_1) \cdot \mathrm{ideal}(F_2) &= \mathrm{ideal}(F), \text{ with } F = \{f_1 f_2 \ : \ f_1 \in F_1, f_2 \in F_2\}.
\end{aligned}$$

2.2 General Properties of Ideals

In this section we prove some basic properties of two-sided ideals and multiplicatively closed sets of a (non-commutative) ring **R** with 1. See also [Goodearl, Warfield 1989] chapter 2 and the references therein (e.g. to Krull and McCoy for the separation lemma).

The proofs are mainly based on Zorn's lemma:

Lemma 2.2.1 (Zorn) *A non empty partially ordered set in which every chain (a totally ordered subset) has an upper bound, has a maximal element.*

For completeness we also state a generalized principle of induction, which will be used in later sections.

Lemma 2.2.2 (Noetherian Induction) *Let A be a quasi ordered set, such that every non empty subset has a minimal element. Let B be a subset of A which contains any element of $a \in A$ whenever it contains all the elements $x \in A$ such that $x < a$. Then $B = A$.*

Definition 2.2.3 *Let $J \subseteq \mathbf{R}$ be a proper two-sided ideal.*

1. *J is called* prime *ideal if, for $a, b \in \mathbf{R}$, $a\mathbf{R}b \subseteq J$ implies $a \in J$ or $b \in J$,*
2. *J is called* complete prime *ideal if, for $a, b \in \mathbf{R}$, $ab \in J$ implies $a \in J$ or $b \in J$,*
3. *J is called* maximal *ideal if for any two-sided ideal I, $J \subseteq I \subseteq \mathbf{R}$ implies $J = I$ or $I = \mathbf{R}$.*

The importance of complete prime ideals stems from the fact, that the residue class ring modulo a complete prime is a domain. In commutative rings all prime ideals are completely prime. An equivalent characterization of a prime ideal J is: for all ideals A, B, $AB \subseteq J$, implies that $A \subseteq J$ or $B \subseteq J$.

Lemma 2.2.4 *Any two-sided maximal ideal is a prime ideal.*

Proof: Let $M \subset \mathbf{R}$ be a maximal ideal. Assume for a contradiction that M is not prime. Then there exist $a, b \in \mathbf{R}$ with $a\mathbf{R}b \subseteq M$ but neither $a \in M$ nor $b \in M$.

Let $J_1 = \text{ideal}_t(a, M)$ and $J_2 = \text{ideal}_t(b, M)$ then $J_1 \neq M$ and $J_2 \neq M$ and so by the maximality of M we have $J_1 = J_2 = \mathbf{R}$. Then $J_1 J_2 = \text{ideal}_t(a, M)\ \text{ideal}_t(b, M) = \text{ideal}_t(a\mathbf{R}b, M)$ that is $\mathbf{R} = \text{ideal}_t(a\mathbf{R}b, M) = \text{ideal}_t(M) = M$ which contradicts the maximality of M. □

Lemma 2.2.5 *Let I be a proper two-sided ideal in $\mathbf{R}$. Then I is contained in a two-sided maximal ideal. More precisely there exists a maximal element M in the set*

$$A = \{J \mid J \text{ two-sided ideal in } \mathbf{R}, J \neq \mathbf{R}, I \subseteq J\}$$

and M is a maximal ideal.

Proof: We are going to show that A satisfies all assumptions of Zorn's lemma, so A contains a maximal element.

First $I \in A$ and so $A \neq \emptyset$. The set inclusion '$\subseteq$' defines a partial order on the set of ideals of $\mathbf{R}$ and also on A. Let $K = \{J_i\}_{i \in \Lambda} \subseteq A$ be a chain of ideals; that is K is totally ordered. Let $J^* = \bigcup_{i \in \Lambda} J_i$. If we can show, that J^* is an upper bound of K in A all assumptions of Zorn's lemma are fulfilled and we can conclude that A has a maximal element.

Note that $J_i \subseteq J^*$ for any $i \in \Lambda$ and so J^* is an upper bound for K. To see that J^* is in A, observe that

1. $I \subseteq J_i$ for $i \in \Lambda$ and so $I \subseteq \bigcup_{i\in\Lambda} J_i = J^*$,
2. $J^* \neq \mathbf{R}$, since otherwise from $J^* = \mathbf{R}$ it would follow that there is $1 \in J^*$, and so $1 \in J_i$ for some $i \in \Lambda$ which contradicts the choice of J_i.
3. J^* is a two-sided ideal, since a) $0 \in I \subseteq J^*$, b) for $a, b \in J^*$, there exists $i, j \in \Lambda$, such that $a \in J_i$ and $b \in J_j$; now K is a chain so wlog. $a \in J_i \subseteq J_j$ and so $a+b \in J_j \subseteq J^*$, c) for $a \in J^*$, $r, s \in \mathbf{R}$, there exists $i \in \Lambda$ with $a \in J_i$; so $ras \in J_i \subseteq J^*$.

Clearly M is a maximal ideal, since the the existence of an ideal J with $M \subset J \subset \mathbf{R}$, would imply that $J \in A$, which would contradict the maximality of M in A. □

Lemma 2.2.6 *Let I be a proper two-sided ideal in $\mathbf{R}$, M be a subset of $\mathbf{R}$ with $M \cap I = \emptyset$. Then there exists a maximal element in the set*

$$A = \{J \mid J \text{ two-sided ideal in } \mathbf{R}, M \cap J = \emptyset, I \subseteq J\}.$$

Proof: We are going to show that A satisfies all assumptions of Zorn's lemma, so A contains a maximal element.

First $I \in A$ and so $A \neq \emptyset$. The set inclusion '$\subseteq$' defines a partial order on the set of ideals of $\mathbf{R}$ and also on A. Let $K = \{J_i\}_{i\in\Lambda} \subseteq A$ be a chain of ideals; that is K is totally ordered. Let $J^* = \bigcup_{i\in\Lambda} J_i$. If we can show, that J^* is an upper bound of K in A, all assumptions of Zorn's lemma are fulfilled and we can conclude that A has a maximal element.

Note that $J_i \subseteq J^*$ for any $i \in \Lambda$ and so J^* is an upper bound for K. The see that J^* is in A observe that

1. $I \subseteq J_i$ for $i \in \Lambda$ and so $I \subseteq \bigcup_{i\in\Lambda} = J^*$,
2. $J^* \cap M = \emptyset$, since otherwise from $J^* \cap M \neq \emptyset$ it would follow $J_i \cap M \neq \emptyset$ for some $i \in \Lambda$ which contradicts the choice of J_i.
3. J^* is a two-sided ideal, since a) $0 \in I \subseteq J^*$, b) for $a, b \in J^*$, there exists $i, j \in \Lambda$, such that $a \in J_i$ and $b \in J_j$; now K is a chain so wlog. $a \in J_i \subseteq J_j$ and so $a+b \in J_j \subseteq J^*$, c) for $a \in J^*$, $r, s \in \mathbf{R}$, there exists $i \in \Lambda$ with $a \in J_i$; so $ras \in J_i \subseteq J^*$.

Observe, that in general I is not a maximal ideal. □

2.2.1 Multiplicatively Closed Sets

In this section we discuss the relation between complete prime ideals, multiplicatively closed subsets and prime ideals and m-sets.

Definition 2.2.7 *A non-empty set $M \subseteq \mathbf{R}$ is called* multiplicatively closed, *if for any $a, b \in M$ also $ab \in M$. A non empty set $M \subseteq \mathbf{R}$ is called an* m-set, *if for any $a, b \in M$ there exists $r \in \mathbf{R}$ such that $arb \in M$.*

Clearly in a ring with 1 a multiplicatively closed set is a m-set.

Lemma 2.2.8 *Let J be a two-sided* complete prime *ideal in $\mathbf{R}$. Then the set $M = \mathbf{R} \setminus J$ is multiplicatively closed.*

Proof: Assume for a contradiction, that M is not multiplicatively closed. Then there exist $m_1, m_2 \in M$ such that $m_1 m_2 \notin M$. So $m_1 m_2 \in J$ and since J is a complete prime ideal we must have $m_1 \in J$ or $m_2 \in J$. But this contradicts $m_1 \in M$ or $m_2 \in M$ and proves the lemma. □

Lemma 2.2.9 *Let J be a two-sided* prime *ideal in $\mathbf{R}$. Then the set $M = \mathbf{R} \setminus J$ is an m-set.*

Proof: Assume for a contradiction, that M is not a m-set. Then there exist $m_1, m_2 \in M$ such that $m_1 r m_2 \notin M$ for all $r \in \mathbf{R}$. So $m_1 \mathbf{R} m_2 \subseteq J$ and since J is a prime ideal we must have $m_1 \in J$ or $m_2 \in J$. But this contradicts $m_1 \in M$ or $m_2 \in M$ and proves the lemma. □

Lemma 2.2.10 (Separation) *Let I be a proper two-sided ideal in $\mathbf{R}$, M be a m-set in $\mathbf{R}$. If $M \cap I = \emptyset$ then there exists an ideal J maximal with respect to the property $I \subseteq J$ and $M \cap J = \emptyset$. Furthermore any such J is prime.*

Proof: By lemma 2.2.6 let J be a two-sided ideal maximal with respect to $M \cap J = \emptyset$ and $I \subseteq J$. Since $M \neq \emptyset$, J is proper. We claim that J is a prime ideal.

Assume for a contradiction that J is not prime. Then there exist $a, b \in \mathbf{R}$ such that $a\mathbf{R}b \subseteq J$, but $a \notin J$ and $b \notin J$. Let $J_1 = \{cad + j \mid c, d \in \mathbf{R}, j \in J\}$, and $J_2 = \{c'bd' + j' \mid c', d' \in \mathbf{R}, j' \in J\}$. Now $J \subsetneq J_1$ and $J \subsetneq J_2$ (since $a, b \notin J$ and J_1, J_2 are ideals) and so by the maximality of J we have $J_1 \cap M \neq \emptyset$ and $J_2 \cap M \neq \emptyset$. Let $m_i \in J_i \cap M$, $i = 1, 2$, with $m_1 = cad + j$ and $m_2 = c'bd' + j'$. Since M is a m-set there exists $r \in \mathbf{R}$ such that $m_1 r m_2 \in M$ holds.

So $m_1 r m_2 = (cad + j)r(c'bd' + j') = cadrc'bd' + jrc'bd' + cadrj' + jrj'$. Now $jrc'bd'$, $cadrj'$, $jrj' \in J$ since J is a two-sided ideal. Furthermore $a\mathbf{R}b \subseteq J$ so $a(drc')b \in J$ and consequently $c(adrc'b)d' \in J$. This shows $m_1 r m_2 \in J$ which contradicts the fact $M \cap J = \emptyset$ and proves the lemma. □

Specializing $J = \{0\}$ we obtain:

Corollary 2.2.11 *Let M be a m-set of $\mathbf{R}$, and assume $0 \notin M$. Then there exists a maximal element I in the set*

$$A = \{J \mid J \text{ two-sided ideal in } \mathbf{R}, J \subseteq \mathbf{R} \setminus M\},$$

and I is a prime ideal.

Note, that in the special case $M = \{1\}$ the ideal I is a maximal ideal (cf. 2.2.5).

As a corollary we also note lemma 2.2.10 for multiplicatively closed sets in the form it is used later.

Corollary 2.2.12 *Let I be a proper two-sided ideal in $\mathbf{R}$, M be a multiplicatively closed set in $\mathbf{R}$. If $M \cap I = \emptyset$ then there exists a prime ideal J with $I \subseteq J$ and $M \cap J = \emptyset$. Furthermore J is maximal with respect to this property.*

2.2.2 Semiprime Ideals

Definition 2.2.13 *Let $\mathbf{R}$ be a ring. An ideal I which is an intersection of prime ideals is called* semiprime. *That is $I = \bigcap_{i\in\Lambda} J_i$ with J_i prime ideals. The* prime radical *of an ideal I is the intersection of all prime ideals which contain I. The prime radical is denoted by*

$$\mathrm{rad}(I) = \bigcap_{I\subseteq J_i} J_i$$

with J_i prime ideals.

Definition 2.2.14 *Let $\mathbf{R}$ be a ring. An ideal I which is an intersection of complete prime ideals is called* completely semiprime. *That is $I = \bigcap_{i\in\Lambda} J_i$ with J_i complete prime ideals. The* complete prime radical *of an ideal I is the intersection of all complete prime ideals which contain I. The complete prime radical is denoted by*

$$\text{c-rad}(I) = \bigcap_{I\subseteq J_i} J_i$$

with J_i complete prime ideals.

Lemma 2.2.15 *Let $\mathbf{R}$ be a ring and let I be an ideal in $\mathbf{R}$. If $a \in \mathrm{rad}(I)$ then there exists $0 < k \in \mathbf{N}$ such that $a^k \in I$.*

Proof: Assume for a contradiction $a \in \mathrm{rad}(I)$ and $a^k \notin I$ for all $0 < k \in \mathbf{N}$. Then the set $M = \{a^k : 0 < k \in \mathbf{N}\}$ is multiplicatively closed and disjoint to I: $M \cap I = \emptyset$. Now by the separation lemma 2.2.12 there exists a prime ideal P which contains I: $I \subseteq P$ and still satisfies $M \cap P = \emptyset$. This shows $a \notin P$. Now P must occur in the intersection $\bigcap_{I\subseteq P_i} P_i = \mathrm{rad}(I)$ and therefore $a \notin \bigcap_{I\subseteq P_i} P_i$. This contradicts the assumption $a \in \mathrm{rad}(I)$ and thus proves the lemma. □

Lemma 2.2.16 *Let $\mathbf{R}$ be a ring such that every prime ideal is completely prime. Let I be an ideal in $\mathbf{R}$ and let $a \in \mathbf{R}$. If $a^k \in I$ for some $0 < k \in \mathbf{N}$ then $a \in \mathrm{rad}(I)$.*

Proof: Let $\mathrm{rad}(I) = \bigcap_{I \subseteq P_i} P_i$, where each P_i is a complete prime ideal. Let $0 < k \in \mathbf{N}$ such that $a^k \in I$. Then $a^k \in \mathrm{rad}(I)$ and therefore $a^k \in P_i$ for each P_i. Now P_i is completely prime and since $a^k = aa^{k-1}$ it follows either $a \in P_i$ or $a^{k-1} \in P_i$. This implies in both cases by induction on k that $a \in P_i$ for all P_i. This shows $a \in \bigcap_{I \subseteq P_i} P_i$ which is the prime radical of I. $\square$

If prime ideals are not completely prime, then the situation is considerably more difficult. So only if $a\mathbf{R}a \subseteq I$ (and not merely $a^k \in I$) we can conclude that $a \in \mathrm{rad}(I)$, as can be seen from the following theorem.

Theorem 2.2.17 (Levitzki, Nagata) *Let* $\mathbf{R}$ *be a ring. An ideal* I *is semiprime if and only if*

Whenever $a \in \mathbf{R}$ *with* $a\mathbf{R}a \subseteq I$ *then* $a \in I$.

Proof: See [Goodearl, Warfield 1989](p 27). $\square$

Corollary 2.2.18 *Let* I *be a semiprime ideal in a ring* $\mathbf{R}$ *and let* J *be a right, left or two-sided ideal in* $\mathbf{R}$. *If there exists a positive integer* n *such that* $J^n \subseteq I$ *then* $J \subseteq I$.

Proof: See [Goodearl, Warfield 1989](p 29). $\square$

Chapter 3

Solvable Polynomial Rings

In this chapter we discuss the axioms of solvable polynomial rings and some consequences of the axioms. We do not assume that the coefficients commute with the variables. With this more general concept we can treat the theory of difference rings, differential rings and arbitrary Ore extension rings over a (non-commutative) field in our framework. Furthermore we give conditions, when homomorphic images of free associative algebras are solvable polynomial rings.

Using a combination of Dickson's lemma and a variant of Königs tree lemma we give a proof of a 'Hilbert basis theorem' for solvable polynomial rings over Noetherian coefficient rings. Next the structure of the center of a solvable polynomial ring is determined and by linear algebra methods, ways to compute elements in the center are investigated. This has important applications in the determination of so called 'Casimir invariants' in the theory of Lie algebras.

3.1 Polynomial Rings

Let $\mathbf{K}$ be a skew field, that is a not necessarily commutative field. From now on we will assume that all fields are not necessarily commutative (and we will drop the 'skew' in front of field) unless otherwise stated. $\mathbf{Q}$ denotes the set of rational numbers. An *inverse* of an element $a \in \mathbf{K}$ will be denoted by a^{-1}, that means $a^{-1}a = 1$ holds.

Let R be a polynomial ring $R = \mathbf{K}[X_1, \ldots, X_n]$ over the field $\mathbf{K}$ in the commuting variables (indeterminates) $X_1, \ldots, X_n$ for some $n \in \mathbf{N}$, $n \geq 0$. All elements of $\mathbf{K}$ are assumed to commute with the indeterminates $X_1, \ldots, X_n$ but $\mathbf{K}$ need not be itself commutative. So R is in general not a commutative ring.

Let T denote the set of terms (power-products of indeterminates)

$$T = \{X_1^{e_1} \cdot \ldots \cdot X_n^{e_n} \in R \ : \ e_i \in \mathbf{N}, 1 \leq i \leq n\}.$$

Then there is a bijection $e : T \longrightarrow \mathbf{N}^n$ between T and n-tuples of natural numbers, defined

by

$$\begin{aligned} e(X_1^{e_1} \cdot \ldots \cdot X_n^{e_n}) &= (e_1, \ldots, e_n) \\ e^{-1}((e_1, \ldots, e_n)) &= X_1^{e_1} \cdot \ldots \cdot X_n^{e_n}. \end{aligned}$$

An important property of the divisibility relation of terms respectively the componentwise order of $\mathbf{N}^n$ is known as Dickson's lemma and is fundamental for most termination proofs of polynomial algorithms.

Lemma 3.1.1 (Dickson's Lemma) *Let $(\mathbf{N}^n, \leq_n)$ be the direct product of n copies of the natural numbers $(\mathbf{N}, \leq)$ with their natural ordering. Then every subset M of $\mathbf{N}^n$ has a finite subset B such that for every $(m_1, \ldots, m_n) \in M$, there exists $(b_1, \ldots, b_n) \in B$ with $b_i \leq m_i$ for $1 \leq i \leq n$.*

Proof: See [Dickson 1913]. □

Stated for terms:

Corollary 3.1.2 *Let $(T, |)$ be the set of terms T partially ordered by divisibility $|$. Then every subset S of T has a finite subset V such that for every $s \in S$ there exists $v \in V$ with $v \mid s$.*

Proof: Let $(\mathbf{N}^n, \leq_n)$ be as in Dickson's lemma, $e : T \longrightarrow \mathbf{N}^n$ be the bijection between T and $\mathbf{N}^n$. Then for $s, t \in T$: $s \mid t$ iff $e(s) \leq_n e(t)$, since $s = X_1^{e_1} \cdot \ldots \cdot X_n^{e_n} \mid X_1^{e'_1} \cdot \ldots \cdot X_n^{e'_n} = t$ $\iff e_i \leq e'_i$ for $1 \leq i \leq n \iff e(s) = (e_1, \ldots, e_n) \leq_n (e'_1, \ldots, e'_n) = e(t)$. So the claim follows by Dicksons's lemma 3.1.1. □

Beside this partial divisibility order on the terms, we assume that the set T is linearly (totally) ordered by a suitable order compatible with divisibility, which is denoted by $<_T$ or simply by $<$. Note such linear orders are well-founded orders (for every non empty subset of T there exists a unique minimal element). The compatibility condition is defined as follows.

Definition 3.1.3 *An ordering $<_T$ on the set of terms T is called* admissible *if for all $r, s, t \in T$:*

1. $1 <_T r$,
2. $r <_T s$ *implies* $rt <_T st$.

For elements $f \in R$, the set of terms of f will be denoted by $T(f)$. The quasi-order induced by $<_T$ on R will also be denoted by $<_T$ or simply by $<$. It is defined as follows: for $f, g \in R$ let $f < g$ if the highest term in $T(g) \setminus T(f)$ is greater then the highest term in $T(f) \setminus T(g)$ or $T(f) \setminus T(g)$ is empty.

For a subset $X \subseteq \{X_1, \ldots, X_n\}$ we denote by $T(X)$ the set of terms in the variables X. For a subset $V \subseteq T$ we denote by $\text{mult}(V) = \{sv \ : \ s \in T, v \in V\}$ the set of multiples of V.

Let $<$ be an admissible order on T, $f \in R$, then $\text{HT}(f)$ denotes the *head term* of f that is the highest term in f with respect to $<$. For $t \in T$ we denote the *coefficient* of t in f by $\text{coeff}(t, f)$. A *monomial* is a polynomial of the form at with $0 \neq a \in \mathbf{K}$ and $t \in T$. The *head monomial* of f, denoted by $\text{HM}(f)$, is defined by $\text{coeff}(\text{HT}(f), f)\text{HT}(f)$. $\text{coeff}(\text{HT}(f), f)$ is also denoted by $\text{HC}(f)$. A polynomial f is called *monic*, if $\text{HC}(f) = 1$. A set of polynomials F is called *monic*, if every $f \in F$ is monic.

Other concepts form commutative polynomial rings, like the *degree* of univariate polynomials or the *degree in the variable* X_i, etc. are defined as usual.

3.2 Axioms for Solvable Polynomial Rings

Let $\mathbf{K}$ be a skew field. A solvable polynomial ring over $\mathbf{K}$ is a polynomial ring $R = \mathbf{K}[X_1, \ldots, X_n]$ equipped with a new (in general non-commutative) multiplication $*$. In this section we first state the axioms of the $*$-product for elements of T and $\mathbf{K}$ and then we determine the $*$-product for arbitrary elements of R. The axiom set generalizes [Kandri-Rody, Weispfenning 1988] in that respect, that $\mathbf{K}$ can now be non-commutative and the elements of $\mathbf{K}$ need not commute with the variables (axioms 3.2.1(4) are new). An even more general set of axioms is discussed in the appendix A.1.

Axioms 3.2.1 *For a fixed term order $<_T$, $(R, *)$ is called a solvable polynomial ring if the following axioms for $*$ are satisfied:*

1. *$(R, 0, 1, +, -, *, <)$ is an associative ring with 1 and with admissible term order $<$.*
2. *(a) For all $a, b \in \mathbf{K}$, $t \in T(X_1, \ldots, X_n)$, $a * b * t = a * (bt) = (a \cdot b) \cdot t = abt$.*
   (b) For all $1 \leq i \leq n$, $s \in T(X_1, \ldots, X_i)$, $t \in T(X_i, \ldots, X_n)$, $s * t = st$.
3. *For all $1 \leq i < j \leq n$ there exist $0 \neq c_{ij} \in \mathbf{K}$ and $p_{ij} \in R$, $p_{ij} <_T X_i X_j$ such that*
$$X_j * X_i = c_{ij} X_i X_j + p_{ij}.$$
4. *For all $1 \leq i \leq n$ and all $0 \neq a \in \mathbf{K}$ there exist $0 \neq c_{ai} \in \mathbf{K}$ and $p_{ai} \in \mathbf{K}$, such that*
$$X_i * a = c_{ai} a X_i + p_{ai}.$$

$*$ will denote the new multiplication, the (non-commutative) multiplication in $\mathbf{K}$ and the commutative multiplication in $\mathbf{K}[X_1, \ldots, X_n]$ will be denoted by $\cdot$ or juxtaposition of elements. If it is clear from the context we will even drop the $*$ for the non-commutative

multiplication in the later chapters. Solvable polynomial rings will be denoted by $R = \mathbf{K}\{X_1, \ldots, X_n\}$, or by

$$\mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$$

if

$$Q = \{X_j * X_i = c_{ij}X_iX_j + p_{ij} \ : \ 0 \neq c_{ij} \in \mathbf{K},\ X_iX_j > p_{ij} \in S,\ 1 \leq i < j \leq n\},$$

denotes the set of commutator relations of axiom 3.2.1(3) and

$$Q' = \{X_i * a = c_{ai}aX_i + p_{ai} \ : \ 0 \neq c_{ai} \in \mathbf{K},\ p_{ai} \in \mathbf{K},\ 1 \leq i \leq n,\ a \in \mathbf{K}\}$$

denotes the set of commutator relations of axiom 3.2.1(4). Note furthermore, that Q is finite; Q' is infinite if $\mathbf{K}$ is infinite and Q' is enumerable if if $\mathbf{K}$ is enumerable. If we assume that the variables commute with the coefficients, then we indicate this by dropping the Q' from the notation of the solvable polynomial ring: $\mathbf{K}\{X_1, \ldots, X_n; Q\}$.

3.2.1 Alternative Axioms

Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring over $\mathbf{K}$. The requirement that $\mathbf{K}$ has to be a skew field seems to be rather restrictive. Examining the proofs in this chapter one finds that at least the condition

- $\mathbf{K}$ is any domain, but all $c_{ij} = 1$ for $1 \leq i < j \leq n$ and all $c_{ai} = 1$ for $1 \leq i \leq n$, $a \in \mathbf{K}$

is sufficient for the claims in this chapter to hold.

Let $\mathrm{cen}(R)$ denote the center of the ring R ($\mathrm{cen}(R) = \{a \in R \ : ar = ra, \text{ for all } r \in R\}$, see 3.6.1). Other conditions such that

1. $\mathbf{K}$ is a commutative domain or
2. all $c_{ij}, c_{ai} \in \mathrm{cen}(\mathbf{K})$ or even
3. all $c_{ij}, c_{ai} \in \mathrm{cen}(S)$

are sufficient to prove the $*$-product lemma 3.2.5. However they are not sufficient to prove e.g. the Hilbert basis theorem 3.5.12. The condition required in this theorem is

- all $c_{ij}, c_{ai} \in \mathbf{L}$, where $\mathbf{L} \subseteq \mathrm{cen}(\mathbf{K})$ is a subfield of $\mathrm{cen}(\mathbf{K})$.

In other words, the c_{ij} and c_{ai} must be invertible and must commute with all elements of $\mathbf{K}$.

On the other hand the condition that $\mathbf{K}$ is a skew field does not require the c_{ij} and c_{ai} to commute with all elements of $\mathbf{K}$. So the condition that $\mathbf{K}$ is a skew field seems the least

restrictive requirement and we leave the axioms 3.2.1 of solvable polynomials as stated. Furthermore we will make use of $\mathbf{K}$ being a skew field in all proofs. But keeping these hints in mind when examining the proofs in this chapter will show that the respective claims are true also when $\mathbf{K}$ is a domain and the commutator relations satisfy the above conditions.

Definition 3.2.2 *Let* $S = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ *be a solvable polynomial ring over* $\mathbf{K}$. *We say that* S satisfies the extended axioms *if*

1. $\mathbf{K}$ *is a skew field, or*
2. $\mathbf{K}$ *is any domain and there exists* $\mathbf{L} \subseteq \mathrm{cen}(\mathbf{K})$ *such that* $\mathbf{L}$ *is a subfield of* $\mathrm{cen}(\mathbf{K})$, *and all* $0 \neq c_{ij} \in \mathbf{L}$ *for* $1 \leq i < j \leq n$ *and all* $0 \neq c_{ai} \in \mathbf{L}$ *for* $1 \leq i \leq n$, $0 \neq a \in \mathbf{K}$.

3.2.2 Computability

It is known, that one can compute in a commutative polynomial ring over a ring $\mathbf{K}$ if one can compute in the ring $\mathbf{K}$. If moreover the term order is computable (or decidable) (i.e. for any $t, s \in T$ we can decide by an algorithm if $t = s$ or if $t <_T s$) we can compute normalforms of reduction relations. Here 'computability' means 'effective computability': That is, there exists a Turing maschine which takes the appropriate 'inputs', performs a finite number of 'steps' and terminates after producing the respective 'output'.

To compute in solvable polynomial rings we have the additional requirement, that we can compute with the commutator relations. To compute with the commutator relations between the variables can be done already if we can compute in the commutative polynomial ring.

To compute with the commutator relations between the variables and the coefficients requires, that the mappings $a \mapsto c_{ai}a$ and $a \mapsto p_{ai}$ are given algorithmically. This is e.g. the case when the mappings are given by *polynomial functions* which could be evaluated at a to find $c_{ai}a$ and p_{ai}. In case when $a \mapsto c_{ai}a$ has to be an automorphism (e.g. when we consider right ideals) we require moreover, that the inverse mapping is given algorithmically.

By this considerations we can compute in a solvable polynomial ring provided the $*$ product of two polynomials can be computed. The computation of $*$-products of polynomials is shown in lemma 3.2.5 later in this section.

So **from now on** whenever we discuss algorithms and claim some properties about algorithms we make the assumptions about computability stated above. Further remarks on computability can be found in chapter 6 on algorithm implementation and in the appendix on algorithmic notation.

3.2.3 $*$-compatible Orders

Any admissible order satisfying condition (3) of axioms 3.2.1 will be called $*$-*compatible*.

Let $<_L$ be the *lexicographical order* on T defined by $X_1 < X_2 < \ldots < X_n$. Let $R = \mathbf{K}\{X_1, \ldots, X_n\}$, be a solvable polynomial ring with respect to $<_L$, such that $<_L$ is $*$-compatible. R is of *strictly lexicographical type*, if for the commutator relations Q in the axioms 3.2.1(3) we have

$$p_{ij} <_L X_j.$$

In other words we require $p_{ij} \in \mathbf{K}[X_1, \ldots, X_{j-1}]$. R is of *strictly monic lexicographical type*, if for the commutator relations Q in the axioms 3.2.1(3) we have

$$c_{ij} = 1 \text{ and } p_{ij} <_L X_j.$$

The set of commutator relations Q is in this case also called to be of *strictly lexicographical type* respectivly of *strictly monic lexicographical type*.

An admissible $*$-compatible ordering $<$ on T is called *degree compatible* if for $s, t \in T$

$$\deg(s) <_{\mathbf{N}} \deg(t) \implies s < t.$$

3.2.4 $*$-products of Polynomials

In this subsection we extend the computation of the $*$-product from variables and coefficients to arbitrary polynomials of R. We proceed in several steps. The following lemma determines left multiplication by field elements and right multiplication by (special) terms.

Lemma 3.2.3 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring.*

1. *Let $a \in \mathbf{K}$, $f \in R$. Then $a * f = af$.*
2. *Let $0 \leq i \leq j \leq k \leq n$ and let $f \in \mathbf{K}[X_i, \ldots, X_j]$, $t \in T(X_j, \ldots, X_k)$. Then $f * t = ft \in \mathbf{K}[X_i, \ldots, X_k]$.*

In particular for $i = j = k$, $t = X_i^e$, $0 \leq e \in \mathbf{N}$: $f * X_i^e = fX_i^e \in \mathbf{K}[X_i]$.

Proof: By Noetherian induction on f with respect to the quasiorder $<$ on R induced by $<$ on T.

(1) Let $f = b \in \mathbf{K}$, then by axiom 3.2.1(2,a) $a * b = ab$. For $f = bt + f'$, $bt = \mathrm{HM}(f)$ we get $a * f = a * (bt + f') = a * bt + a * f'$. By induction assumption and axiom 3.2.1(2,a) this is equal to $abt + af' = af$.

(2) Let $f = b \in \mathbf{K}$, then by axiom 3.2.1(2,a) $f * t = a * t = at$. Let $f = bt' + f'$, $bt' = \mathrm{HM}(f)$, then $f * t = (bt' + f') * t = bt' * t + f' * t$. Then by axiom 3.2.1(2,b) we have $t' * t = t't \in T(X_i, \ldots, X_k)$. So $f * t = bt't + f' * t = bt't + f't = ft$ using induction assumption on $f' * t$. $\square$

The next lemma considers products of polynomials having terms with 'increasing' sets of variables. In particular right multiplication with field elements is considered.

Lemma 3.2.4 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, let $0 \leq i \leq j \leq k \leq n$ and let $f \in \mathbf{K}[X_i, \ldots, X_j]$, $g \in \mathbf{K}[X_j, \ldots, X_k]$.*

1. *Then there exists $0 \neq c_{gf} \in \mathbf{K}$ and $h \in \mathbf{K}[X_i, \ldots, X_k]$, $h < \mathrm{HT}(fg)$ such that*

$$f * g = c_{gf} fg + h.$$

   In particular $f * g \in \mathbf{K}[X_i, \ldots, X_k]$ and $\mathrm{HT}(f * g) = \mathrm{HT}(fg)$.

2. *For $g = a \in \mathbf{K}$ we note as a special case: there exists $0 \neq c_{af} \in \mathbf{K}$ and $h \in \mathbf{K}[X_i, \ldots, X_j]$, $h < \mathrm{HT}(f)$ such that*

$$f * a = c_{af} fa + h.$$

   In particular $f * a \in \mathbf{K}[X_i, \ldots, X_j]$ and $\mathrm{HT}(f * a) = \mathrm{HT}(f)$.

3. *If the coefficients commute with the variables, we note as a special case: if $c_{al} = 1$, $p_{al} = 0$, for $1 \leq l \leq n$ and $0 \neq a \in \mathbf{K}$, then*

$$f * g = fg.$$

   In particular $f * g \in \mathbf{K}[X_i, \ldots, X_k]$.

Proof: We prove (1) by Noetherian induction on fg with respect to the quasiorder $<$ on R induced by $<$ on T. (2) and (3) follow since they are special cases of (1).

Case 1: Let $f = b \in \mathbf{K}$ then by lemma 3.2.3 $f * g = b * g = bg = 1bg + 0$. So the claim holds with $c_{gf} = 1$ and $h = 0$.

Case 2: Let $g = a \in \mathbf{K}$ and assume the claim holds for all $f'g' < fa$. For $f = bt + f'$, $bt = \mathrm{HM}(f)$ we get $f * a = (bt + f') * a = bt * a + f' * a$. By induction assumption let $f' * a = c'_{af'} f' + h'$. For the first term let $1 \leq k \leq j$ maximal such that $e_k \geq 0$ in $t = t' X_k^{e_k+1}$ and let $t = t' X_k^{e+1} = u * X_k = t' X_k^e * X_k$.

By axiom 3.2.1(4) for $X_k * a = c_{ak} a X_k + p_{ak}$ we have $bt * a = b(u * X_k) * a = bu * (X_k * a)$ $= bu * (c_{ak} a X_k + p_{ak}) = b(u * c_{ak} a) X_k + b(u * p_{ak}) = bt'(X_k^e * c_{ak} a) X_k + bt'(X_k^e * p_{ak})$.

By twofold application of the induction assumption to $X_k^e * (c_{ak} a) = c'_1 (c_{ak} a) X_k^e + p_1$ and $X_k^e * p_{ak} = c'_2 p_{ak} X_k^e + p_2$ we get (setting $c_1 = c'_1 c_{ak} a$ and $c_2 = c'_2 p_{ak}$): $bt * a = b(t' * c_1 X_k^e + t' p_1) X_k + b(t' * c_2 X_k^e + t' p_2)$.

Using induction assumption we get $t' * c_1 = c_3 t' + p_3$ and $t' * c_2 = c_4 t' + p_4$ (again simplifying the coefficients to c_3 and c_4). Furthermore since $p_1 \in \mathbf{K}[X_k]$ we can conclude by induction assumption that $g_1 = bt' * p_1 = d_1 g_1' + q_1' \in \mathbf{K}[X_i, \ldots, X_k]$. And again by lemma 3.2.3 $g_1 * X_k = g_1 X_k \in \mathbf{K}[X_i, \ldots, X_k]$. By the same arguments, since $p_2 \in \mathbf{K}[X_k]$, $g_2 = bt' * p_2 \in \mathbf{K}[X_i, \ldots, X_k]$. So the second and fourth summand can be combined to $h_1 = g_1 * X_k + g_2$, and we get $bt * a = b(c_3 t' + p_3) X_k^{e+1} + b(c_4 t' + p_4) X_k^e + h_1$.

Now $t' * X_k^{e+1} = t' X_k^{e+1} = t$ and $t' * X_k^e = t' X_k^e$ by axiom 3.2.1(2,b), and again $bp_3 \in \mathbf{K}[X_i, \ldots, X_{k-1}]$, $bp_4 \in \mathbf{K}[X_i, \ldots, X_{k-1}]$ and using lemma 3.2.3 on $bp_3 * X_k^{e+1}$ and $bp_4 * X_k^e$ the term $bt * a$ becomes $bc_3 t + h_2$, where h_2 denotes the sum of the remaining parts. Finally since $\mathbf{K}$ is a (skew) field, we can find $c_{af} \in \mathbf{K}$ such that $c_{af} b = bc_3$ and with $h = h_2 + h' + (c' - c_{af}) f'$, and we arrive at $f * a = bt * a + c' f' + h' = c_{af} bt + h_2 + c' f' + h' = c_{af} f + h$ as claimed.

Case 3: Let $g = bt + g'$, $bt = \mathrm{HM}(g)$, then $f * g = f * (bt + g') = (f * b) * t + f * g'$. By induction assumption: $f * b = c' f + h'$, where $0 \neq c' \in \mathbf{K}$ and $f > h' \in \mathbf{K}[X_i, \ldots, X_j]$. So we obtain $(c' f + h') * t + f * g' = c' f * t + h' * t + f * g'$.

Now by lemma 3.2.3(2): $f * t = ft$, $h' * t = h't$ and $f * g' = c'' fg' + h''$ by induction assumption. with $0 \neq c'' \in \mathbf{K}$ and $fg' > h'' \in \mathbf{K}[X_i, \ldots, X_k]$. So $f * g = c' ft + h't + c'' fg' + h'' = cfg + h$ with $0 \neq c'' = c_{gf} \in \mathbf{K}$ and $fg > h \in \mathbf{K}[X_i, \ldots, X_k]$. □

The following lemma treats products of arbitrary polynomials.

Proposition 3.2.5 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, and let $f, g \in R$. Then there exists $h \in R$ and $0 \neq c_{fg} \in \mathbf{K}$, such that*

$$f * g = c_{fg} fg + h$$

and $h <_T \mathrm{HT}(fg)$. Moreover, c and h are uniquely determined by f and g.

Proof: The proof generalizes [Kandri-Rody, Weispfenning 1988] lemma 1.4. Uniqueness: Let $f * g = cfg + h = c' fg + h'$. Since $h, h' < \mathrm{HT}(fg)$, $\mathrm{HT}(fg)$ cannot be cancelled by some term in h or h', so $c = c'$. Then by subtraction of cfg on both sides we see that $h = h'$.

Existence: Follows by Noetherian induction on fg with respect to $<$. Let $f = a \in \mathbf{K}$, then by lemma 3.2.3: $a * g = ag + 0$. Let $g = b \in \mathbf{K}$, then by lemma 3.2.4: $f * b = cbf + h$.

For the general case let $f = as + f'$, $g = bt + g'$ with $as = \mathrm{HM}(f)$, $bt = \mathrm{HM}(g)$. Then by distributivity of $*$ and 3 fold application of the induction assumption we get

$$f * g = as * bt + as * g' + f' * bt + f' * g' = as * bt + d_1 asg' + d_2 f'bt + d_3 f'g' + h',$$

where $d_1, d_2, d_3 \in \mathbf{K}$, $h' \in R$, $h' < st = \mathrm{HT}(fg)$. When we have proved that

$$as * bt \;=\; cabst + h'', \tag{3.1}$$

with $c \in \mathbf{K}$ and $h'' < st = \mathrm{HT}(fg)$, we can set $d_i' = d_i - c$, $h = h'' + d_1' asg' + d_2' f'bt + d_3' f'g' + h'$ and the claim $f * g = cfg + h$ follows.

It remains to show, that equation (3.1) holds. Assume, that $s \in T(X_h, \ldots, X_j)$ and $t \in T(X_i, \ldots, X_k)$ with h, i maximal and j, k minimal with $1 \leq h \leq j \leq n$, $1 \leq i \leq k \leq n$. We distinguish 4 cases:

Case $j \leq i$**:** We can apply lemma 3.2.4 to obtain $as * bt = cabst + h''$, with $st > h'' \in \mathbf{K}[X_h, \ldots, X_j]$. and $0 \neq 0 \in \mathbf{K}$.

Case $h \leq i$**:** Let $s = X_h^{e+1} s'' = X_h * X_h^e s'' = X_h * s'$ with $s'' \in T(X_{h+1}, \ldots, X_j)$. Now $s' < s$ and by induction assumption let $s' * bt = c_2 bs't + h_2$. We get $as * bt = aX_h * (s' * bt) = aX_h * (c_2 bs't + h_2) = a(X_h * c_2 b)s't + aX_h * h_2$. Since $h_2 < s't$, induction assumption can be applied to the last summand giving $aX_h * h_2 = h_3$ with $h_3 < X_h s't = st$.

By axiom 3.2.1(4) there exist $c_3, p_3 \in \mathbf{K}$ with $X_h * c_2 b = c_3(c_2 b)X_h + p_3$. Let $c_4 \in \mathbf{K}$ such that $c_4 ab = ac_3 c_2 b$ and let $p_4 = ap_3$ then $as * bt = a(c_3(c_2 b)X_h + p_3)s't + h_3 = c_4 ab(X_h * s't) + p_4 * s't + h_3 = c_4 abX_h * (X_h^{e+d} s''t') + p_4 s't + h_3 = c_4 ab(X_h * X_h^{e+d}) * s''t' + h'' = c_4 abc_5(X_h^{e+1+d} * s''t') + h'' = cabst + h''$. Using axiom 3.2.1(2,a) for products with coefficients, $X_h * s' = s$, $c \in \mathbf{K}$ with $ca = ac_4$ and $h'' = p_4 s't + h_3 < st$.

Furthermore using that the (commutative) term $s't$ can be written as $X_h^{e+d} s''t' = X_h^{e+d} * s''t'$ by axiom 3.2.1(2,b), ($d \geq 0$ the degree of X_k in t) and using that by axiom 3.2.1(2,b) $X_h * X_h^{e+d} = X_h^{e+1+d}$ and again by axiom 3.2.1(2,b) $X_h^{e+1+d} * s''t' = X_h^{e+1+d} s''t' = st$. Finally by taking $c = c_4$ the claim follows.

Case $j \leq k$**:** Let $t = t' X_k^{e+1} = t' X_k^e * X_k = u * X_k$ with $t' \in T(X_i, \ldots, X_{k-1})$. Now $t' < t$ and by induction assumption let $s * bt' = c_2 bst' + h_2$. We get $as * bt = a(s * bt')X_k^e * X_k = a(c_2 bst' + h_2)X_k^e * X_k = a(c_2 bst' * X_k^e) * X_k + (h_2 * X_k^e) * X_k$

Since $h_2 < st'$ we can apply induction assumption on both products in the second summand yielding $h_4 = (h_2 * X_k^e) * X_k < st' X_h^{e+1} = st$. Furthermore we can apply induction assumption to $st' * X_k^e = c_3 st' X_k^e + h_3$, since $st' X_k^e < st$. This gives $as * bt = ac_2 b(c_3 st' X_k^e + h_3) * X_k + h_4 = ac_2 bc_3(st' X_k^e) * X_k + ac_2 bh_3 * X_k + h_4$ Again the second summand can be handled by induction assumption since $h_3 < st' X_k^e < st$, let $h_5 = ac_2 bh_3 * X_k + h_4 < st$.

Now use, that the (commutative) term $st' X_k^e$ can be written as $s't' X_k^{e+d} = s't' * X_k^{e+d}$ by axiom 3.2.1(2,b), ($d \geq 0$ the degree of X_k in s). Furthermore by axiom 3.2.1(2,b) we have $X_k^{e+d} * X_k = X_k^{e+1+d}$ thus $as * bt = ac_2 bc_3 s't' * X_k^{e+1+d} + h_5 = c_5 ab(s't')X_k^{e+1+d} + h_5$, using $c_5 ab = ac_2 bc_3$. By axiom 3.2.1(2,b) $s't' * X_k^{e+1+d} = s't' X_k^{e+1+d} = st$ With $0 \neq c = c_5 \in \mathbf{K}$ and $h'' = h_5$ we get $as * bt = cabst + h_5 = cabst + h''$ as claimed.

Case $i < h \;\&\; k < j$**:** We use that $s = s'' X_j^{e+1} = u * X_j = s'' X_j^e * X_j$, $t = X_i^{d+1} t'' = X_i * X_i^e t'' = X_i * t'$, with $s'' \in T(X_h, \ldots, X_{j-1})$, $t' \in T(X_{i+1}, \ldots, X_k)$ and with $e \geq 0$ and $d \geq 0$ by axioms 3.2.1(2,b).

Lemma 3.2.4 applied to $s * b$ gives $c_3 bs + h_1$, $h_1 < s$. We obtain $as * bt = a(s * b)X_i * t' = a(c_3 bs + h_1) * X_i * t' = c_4 ab(s * X_i) * t' + ah_1 * X_i * t' = c_4 ab(s'' X_j^e) * (X_j * X_i) * t' + h_2$.

Where we used two times induction assumption on $ah_1 * X_i * t' = h_2 < st$ and $c_4 \in \mathbf{K}$ with $c_4ab = ac_3b$.

By axiom 3.2.1(3) let $X_j * X_i = c_{ij}X_iX_j + p_{ij}$ so the first summand becomes $as * bt = c_4ab(s''X_j^e) * (c_{ij}X_iX_j + p_{ij}) * t' + h_2 = c_4abs''(X_j^e * c_{ij}) * X_iX_j * t' + c_4ab(s''X_j^e) * p_{ij} * t' + h_2$.

For the first summand lemma 3.2.4 can be used to obtain $X_j^e * c_{ij} = c_5X_j^e + h_3$, $h_3 < X_j^e$. The second summand can be handled by induction assumption and combined with h_2 to form $h_4 = c_4ab(s''X_j^e) * p_{ij} * t' + h_2 < st$, so: $as * bt = c_4abs''(c_5X_j^e + h_3) * X_iX_j * t' + h_4 = c_4ab(s''c_5)X_j^e * X_iX_j * t' + c_4abs'' * h_3 * X_iX_j * t' + h_4$.

Using lemma 3.2.4 for $s''c_5 = c_6s'' + h_5$, $h_5 < s''$ and application of 3 times induction assumption to the second summand and combination with h_4 giving $h_6 = c_4abs'' * h_3 * X_iX_j * t' + h_4 < st$, we obtain $as * bt = c_4ab(c_6s'' + h_5)X_j^e * X_iX_j * t' + h_6 = c_4abc_6(s''X_j^e * X_i) * (X_j * t') + c_4abh_5X_j^e * X_iX_j * t' + h_6$.

From now on let $s''X_j^e = s'$ by axiom 3.2.1(2,b). Since $s'X_i < s'X_jX_i \leq st$ and $X_jt' < X_jX_it' \leq st$ induction assumption can be applied to the first and last product of the first summand: $s' * X_i = c_8X_is' + h_8$, $h_8 < s'X_i$ and $X_j * t' = c_9t'X_j + h_9$, $h_9 < X_jt'$. For the second summand we use again induction assumption $h_7 = c_4abh_5X_j^e * X_iX_j * t' + h_6 < st$. So we get $as * bt = c_7ab(c_8X_is' + h_8) * (c_9t'X_j + h_9) + h_7 = c_7ab(c_8(X_is' * c_9)t'X_j + c_8X_is' * h_9 + h_8 * c_9t'X_j + h_8 * h_9) + h_7 = c_7abc_8(X_is' * c_9)t'X_j + h_{10}$. Using several induction assumptions and simplifications on the second to fourth summand, such that $h_{10} = c_7ab(c_8X_is' * h_9 + h_8 * c_9t'X_j + h_8 * h_9) + h_7$, $h_{10} < st$.

Using lemma 3.2.4 we can write $X_is' * c_9 = c_9X_is' + h_{11}$, $h_{11} < X_is'$. With further simplifications we get: $as * bt = c_7abc_8(c_9X_is' + h_{11})t'X_j + h_{10} = c_7abc_8c_9(X_is') * (t'X_j) + c_7abc_8h_{11} * t'X_j + h_{10} = c_{10}abX_i(s' * t')X_j + h_{12}$. Using $h_{12} = c_7abc_8h_{11} * t'X_j + h_{10} < st$, and $c_{10} \in \mathbf{K}$ such that $c_{10}ab = c_7abc_8c_9$.

Since $s't' < st$ we can apply induction assumption to the middle product $s' * t' = c_{11}s't' + h_{13}$, so $as * bt = c_{10}abX_i(c_{11}s't' + h_{13})X_j = c_{10}ab(X_ic_{11})s't'X_j + c_{10}abX_i * h_{13} * X_j + h_{12} = c_{10}ab(c_{12}X_i + h_{14})(s't')X_j + c_{10}abX_i * h_{13} * X_j + h_{12} = c_{10}abc_{12}X_i * (s't') * X_j + c_{10}ab * h_{14} * (s't') * X_j + h_{15} = c_{13}abX_i * (s't') * X_j + h_{15}$, using induction assumptions on the second summands, $X_ic_{11} = c_{12}X_i + h_{14}$, coefficient products and collecting the rests in $h_{15} < st$.

Now by the hypothesis of this case, $s't' \in T(X_i, \ldots, X_j)$ and we can write $s't' = X_i^ds''t''X_j^e = X_i^d * s''t'' * X_j^e$ using axiom 3.2.1(2,b). By axiom 3.2.1(2,b) we can write $X_i^{d+1} * s''t'' = X_i^{d+1}s''t''$. Finally again by axiom 3.2.1(2,b) $X_i^{d+1}s''t'' * X_j^{e+1} = X_i^{d+1}s''t''X_j^{e+1} = st$ and with $0 \neq c = c_{13} \in \mathbf{K}$ and $h'' = h_{15}$ we obtain $as * bt = cabst + h''$ as desired.

So in all cases we have proved (3.1) and so the lemma. □

Corollary 3.2.6 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring with respect to a $*$-compatible admissible term order. Then the $*$ multiplication on R is uniquely determined by Q and Q'.*

The last lemma of this section shows that solvable polynomial rings have no zero-divisors and deals with the $*$-product and the quasi-order $<$.

Lemma 3.2.7 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, and let $f, g \in R$. Then*

1. $\mathrm{HT}(f * g) = \mathrm{HT}(f)\mathrm{HT}(g) = \mathrm{HT}(fg) = \mathrm{HT}(g)\mathrm{HT}(f) = \mathrm{HT}(g * f)$,
2. *there exists* $0 \neq c \in K$, *such that* $\mathrm{HM}(f * g) = c\mathrm{HM}(f)\mathrm{HM}(g)$,
3. *For* $h \in R$, $\mathrm{HT}(f) < \mathrm{HT}(g)$ *implies* $\mathrm{HT}(f*h) < \mathrm{HT}(g*h)$ *and* $\mathrm{HT}(h*f) < \mathrm{HT}(h*g)$.

In particular R has no zero-divisors.

Proof: (1) The assumptions of proposition 3.2.5 are fulfilled, so $f * g = cfg + h$ with $h < fg$, and we have $\mathrm{HT}(f * g) = \mathrm{HT}(cfg) = \mathrm{HT}(fg) = \mathrm{HT}(f)\mathrm{HT}(g)$ and similarly $\mathrm{HT}(g * f) = \mathrm{HT}(c'gf) = \mathrm{HT}(gf) = \mathrm{HT}(fg)$.

(2) As in (1) let $f*g = cfg+h$ with $0 \neq c \in \mathbf{K}$, then $\mathrm{HM}(f*g) = \mathrm{HM}(cfg) = c\mathrm{HM}(fg) = c\mathrm{HM}(f)\mathrm{HM}(g)$.

(3) If $\mathrm{HT}(f) < \mathrm{HT}(g)$, then by (1) and since $<$ is admissible, we have $\mathrm{HT}(f * h) = \mathrm{HT}(f)\mathrm{HT}(h) < \mathrm{HT}(g)\mathrm{HT}(h) = \mathrm{HT}(g * h)$ and $\mathrm{HT}(h * f) = \mathrm{HT}(h)\mathrm{HT}(f) < \mathrm{HT}(h)\mathrm{HT}(g) = \mathrm{HT}(h * g)$. □

3.3 Associativity

The axioms 3.2.1(2, 3, 4) alone do not guarantee the associativity of the $*$-product. So axiom 3.2.1(1) imposes some restrictions on the values of the c_{ai}, p_{ai}, c_{ij} and the coefficients of the p_{ij}. We are going to show that these restrictions can be stated as a set of polynomial equations between these elements.

Consider R as a $\mathbf{K}$ bi-module generated by the elements of T.

Definition 3.3.1 *Let R be a ring, $\alpha : R \longrightarrow R$ be an endomorphism. $\delta : R \longrightarrow R$ is called an* α-derivation *if for all $a, b \in R$:*

1. $\delta(a + b) = \delta(a) + \delta(b)$,
2. $\delta(ab) = \alpha(a)\delta(b) + \delta(a)b$.

If α is the identity, then δ satisfies the usual sum and product rule of derivations.

Necessary conditions for the c_{ai} and p_{ai} are noted in the following lemma.

Lemma 3.3.2 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring, then for $1 \leq i \leq n$ the mappings*

$$\alpha_i : \mathbf{K} \longrightarrow \mathbf{K}, \quad a \longmapsto \alpha_i(a) = c_{ai}a$$

must be injective endomorphisms *and the mappings*

$$\delta_i : \mathbf{K} \longrightarrow \mathbf{K}, \quad a \longmapsto \delta_i(a) = p_{ai}$$

must be α_i-derivations. *That is for all $a, b \in \mathbf{K}$ and $1 \leq i \leq n$ the images of α_i and δ_i satisfy the following equations:*

1. $c_{a+b,i}(a+b) = c_{a,i}a + c_{b,i}b$,
2. $c_{ab,i}ab = c_{a,i}ac_{b,i}b$,
3. $p_{a+b,i} = p_{a,i} + p_{b,i}$,
4. $p_{ab,i} = c_{a,i}ap_{b,i} + p_{a,i}b$.

Proof: By distributivity of $*$ over $+$, $X_i * (a+b) = X_i * a + X_i * b$, so we get:

$$c_{a+b,i}(a+b)X_i + p_{a+b,i} = (c_{a,i}a + c_{b,i}b)X_i + p_{a,i} + p_{b,i}.$$

And by the associativity of $*$, $X_i * (ab) = (X_i * a) * b$, so:

$$c_{ab,i}abX_i + p_{ab,i} = (c_{a,i}ac_{b,i}b)X_i + c_{a,i}ap_{b,i} + p_{a,i}b.$$

Comparing coefficients the claim follows.

To show injectivity, assume for a contradiction that $c_{ai}a = c_{a'i}a'$ for some $a \neq a'$, $a, a' \in \mathbf{K}$. Then $(a - a') \neq 0$ and by axiom 3.2.1(4) $0 \neq c_{(a-a')i}(a - a') = (c_{ai}a - c_{a'i}a') = 0$ a contradiction. □

If R is of strict lexicographical type, we obtain similarly necessary conditions for the c_{ij} and p_{ij}.

Corollary 3.3.3 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring of strict lexicographical type. Let $R_j = \mathbf{K}\{X_1, \ldots, X_{j-1}; Q_j, Q'_j\}$ be the restriction of R to $\mathbf{K}[X_1, \ldots, X_{j-1}]$. By the product lemma 3.2.5, let $0 \neq c_{fj} \in \mathbf{K}$ and $h_{fj} \in R$ with $h_{fj} < fX_j$ such that*

$$X_j * f = c_{fj}fX_j + h_{fj}.$$

If $f \in R_j$ it follows from the strict lexicographical condition that $h_{fj} \in R_j$. Thus R_j is again a solvable polynomial ring of strict lexicographical type and so for $1 \leq j \leq n$ the mappings

$$\alpha_j : R_j \longrightarrow R_j, \quad f \longmapsto \alpha_j(f) = c_{fj}f$$

must be injective endomorphisms *and the mappings*

$$\delta_i : R_j \longrightarrow R_j, \quad f \longmapsto \delta_j(f) = h_{fj}$$

must be α_j-derivations. *That is for all $f, g \in R_j$ for $1 \leq j \leq n$ the images of α_j and δ_j satisfy the following equations:*

1. $c_{f+g,j}(f+g) = c_{f,j}f + c_{g,j}g$,
2. $c_{fg,j}fg = c_{f,j}fc_{f,j}g$,
3. $h_{f+g,j} = h_{f,j} + h_{g,j}$,
4. $h_{fg,j} = c_{f,j}fh_{f,j} + h_{f,j}b$.

Proof: As in the previous lemma. □

Further necessary conditions for the c_{ij} and c_{ai} are given by:

Lemma 3.3.4 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring. Then for $1 \leq i < j < k \leq n$ the c_{ai}, c_{ij}, c_{ik} and c_{jk} must satisfy the following equation:*

$$c_{jk}c_{c_{ik},j}c_{ik}c_{ij} = c_{c_{ij},k}c_{ij}c_{ik}c_{c_{jk},i}c_{jk},$$

Proof: The claim follows from comparing coefficients of the head terms in

$$(X_k * X_j) * X_i = c_{jk}c_{c_{ik},j}c_{ik}c_{ij}X_iX_jX_k + \text{smaller order terms}$$

and

$$X_k * (X_j * X_i) = c_{c_{ij},k}c_{ij}c_{ik}c_{c_{jk},i}c_{jk}X_iX_jX_k + \text{smaller order terms}.$$

□

A sufficient condition can be obtained as follows:

Lemma 3.3.5 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a not necessary associative $\mathbf{K}$-algebra, satisfying axioms 3.2.1(2, 3, 4), T the set of terms of R.*

$$R \text{ is associative} \Longleftrightarrow \alpha r * (\beta s * \gamma t) = (\alpha r * \beta s) * \gamma t$$

for all $\alpha, \beta, \gamma \in \mathbf{K}$ and all $r, s, t \in T$.

Proof: $\Longrightarrow$ If R is associative, then clearly $\alpha r * (\beta s * \gamma t) = (\alpha r * \beta s) * \gamma t$.

$\Longleftarrow$ Assume that for all $\alpha, \beta, \gamma \in \mathbf{K}$ and all $r, s, t \in T$: $\alpha r * (\beta s * \gamma t) = (\alpha r * \beta s) * \gamma t$. Let $f, g, h \in R$, $f = \sum \alpha_{rf} r$, $g = \sum \beta_{sg} s$ and $h = \sum \gamma_{th} t$. Then by distributivity of $*$ over $+$

$$\begin{aligned}(f * g) * h &= \sum_{r,s,t} (\alpha_{rf} r * \beta_{sg} s) * \gamma_{th} t \\ &= \sum_{r,s,t} \alpha_{rf} r * (\beta_{sg} s * \gamma_{th} t) \\ &= f * (g * h).\end{aligned}$$

This shows that $*$-products of arbitrary elements of R are associative. □

More important is the following proposition, which states that there exists a set of equations between the c_{ai}, p_{ai}, c_{ij}, the coefficients of the p_{ij} and elements of $\mathbf{K}$, that holds iff R is associative.

Proposition 3.3.6 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable ring, satisfying axioms 3.2.1(2, 3, 4), T the set of terms of R. Then R is associative $\Longleftrightarrow$ the c_{ai}'s, p_{ai}'s, c_{ij}'s and the coefficients of the p_{ij}'s, satisfy the following set of equations:*

$$\sum_{v \in T} \delta_{\delta_{(\alpha,r,\beta,s,v)},v,\gamma,t,u} = \sum_{v \in T} \delta_{\alpha,r,\delta_{(\beta,s,\gamma,t,v)},v,u}$$

for all $\alpha, \beta, \gamma \in \mathbf{K}$ and all $r, s, t, u \in T$. Here the δ's are derived as polynomials in the c_{ai}'s, p_{ai}'s, c_{ij}'s, the coefficients of the p_{ij}'s and elements of $\mathbf{K}$.

To see that the δ's can also be derived as polynomials over $\mathbf{K}$ in the indeterminates c_{ai}'s, p_{ai}'s, c_{ij}'s and the coefficients of the p_{ij}'s see 7.1.2.

Proof: By lemma 3.3.5 R is associative iff for all for all $\alpha, \beta, \gamma \in \mathbf{K}$ and all $r, s, t \in T$: $\alpha r * (\beta s * \gamma t) = (\alpha r * \beta s) * \gamma t$. We expand the products by proposition 3.2.5: For $\alpha, \beta \in \mathbf{K}$ and $r, s \in R$ let $\alpha r * \beta s = \sum_{v \in T} \delta_{\alpha,r,\beta,s,v} v$. Note that the sums are finite. Now

$$(\alpha r * \beta s) * \gamma t = (\sum_{v \in T} \delta_{\alpha,r,\beta,s,v} v) * \gamma t = \sum_{v \in T, u \in T} \delta_{\delta_{(\alpha,r,\beta,s,v)},v,\gamma,t,u} u$$

and

$$\alpha r * (\beta s * \gamma t) = \alpha r * (\sum_{v \in T} \delta_{\beta,s,\gamma,t,v} v) = \sum_{v \in T, u \in T} \delta_{\alpha,r,\delta_{(\beta,s,\gamma,t,v)},v,u} u.$$

Since the $u \in T$ are linearly independent, the coefficients of the u's must vanish exactly when the associativity condition on the products of the terms are fulfilled. □

3.3.1 Ring Extensions

In this subsection we discuss under what conditions on the commutator relations of solvable polynomial rings, new variables can be added such that the extension ring is still a solvable polynomial ring.

The next lemma shows that we may add commuting variables and still have a solvable polynomial ring.

Lemma 3.3.7 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$ with respect to a $*$-compatible admissible term order $<$. Let $Y_1, \ldots, Y_m$ be new variables that commute with all X_i, among themselves and with the elements of $\mathbf{K}$. Furthermore extend the term order $<$ to a term order $<'$ on $T(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ in such a way, that the restriction of $<'$ to $T(X_1, \ldots, X_n)$ coincides with $<$. That is we let $Q_1 = Q \cup \{Y_j * X_i = X_i Y_j \ : \ X_i < Y_j, 1 \leq i \leq n, \ 1 \leq j \leq m\} \cup \{X_i * Y_j = Y_j X_i \ : \ Y_j < X_i, 1 \leq i \leq n, \ 1 \leq j \leq m\} \cup \{Y_k * Y_j = Y_j Y_k \ : \ 1 \leq j < k \leq m\}$ and $Q_1' = Q_1 \cup \{Y_j * a = a Y_j \ : \ a \in \mathbf{K}, \ 1 \leq j \leq m\}$.*

Then $R_1 = \mathbf{K}\{X_1, \ldots, X_n, Y_1, \ldots, Y_m; Q_1, Q_1'\}$ is a solvable polynomial ring over the field $\mathbf{K}$ with respect to the $*$-compatible admissible term order $<'$.

Proof: By construction the polynomial ring $R[Y_1, \ldots, Y_m]$ is associative with respect to $\cdot$. Define $*$ on $R[Y_1, \ldots, Y_m]$ by $\cdot$ and by Q_1 and Q_1' then $*$ satisfies axioms (2,3,4) of solvable polynomial rings 3.2.1. This implies with the associativity of $*$ on the old variables the associativity of $*$ on the combined set of old and new variables. With lemma 3.3.5 this shows the associativity of $*$ in the ring R_1, so R_1 also satisfies axiom (1) of solvable polynomial rings 3.2.1. □

We turn now to some examples of solvable polynomial rings.

3.4 Examples of Solvable Polynomial Rings

We show in this section, that several algebraic structures satisfy the axioms 3.2.1 for special values of the c_{ij}, p_{ij}, c_{ai} and p_{ai}.

Clearly commutative polynomial rings are solvable polynomial rings. Let $R = \mathbf{K}[X_1, \ldots, X_n]$ be a commutative polynomial ring in the commuting indeterminates $X_1, \ldots, X_n$. $\mathbf{K}$ a (commutative) field, commuting with the indeterminates. Then R satisfies the axioms 3.2.1 if we define

$c_{ij} = 1$, $p_{ij} = 0$, $1 \leq i \leq j \leq n$, and
$c_{ai} = 1$, $p_{ai} = 0$ $1 \leq i \leq n$, $a \in \mathbf{K}$.

3.4.1 Ore Extensions

To define Ore extensions we need some preparations.

Proposition 3.4.1 *Let R be a ring, let α be an endomorphism of R, let δ be an α-derivation of R and let X be an indeterminate not commuting with R. Then there exists a unique ring S, containing R as a subring, such that S is a free left R-module with a basis of the form $1, X, X^2, \ldots$ and multiplication $*$ such that*

$$X * r = \alpha(r)X + \delta(r)$$

for all $r \in R$.

Proof: See [Goodearl, Warfield 1989](p 8). □

Note, that if for all $0 \neq r \in R$ the highest terms on both sides are equal and R is a domain (i.e. R has no zero divisors) this implies that α is injective. (Since otherwise the $1, X, X^2, \ldots$ would be linearly dependent.) As we consider mostly domains, the assumption of α being injective will be no loss of generality.

Definition 3.4.2 (Ore extension) *The ring S of the preceding proposition is denoted by*

$$R[X; \alpha, \delta]$$

and is called an Ore extension of R. *An* iterated Ore extension *is a ring S defined by*

$$R[X_1;\alpha_1,\delta_1][X_2;\alpha_2,\delta_2]\ldots[X_n;\alpha_n,\delta_n]$$

where α_2 is now an endomorphism of $R[X_1;\alpha_1,\delta_1]$ and δ_2 is an α_2-derivation of $R[X_1;\alpha_1,\delta_1]$ etc.

Ore extensions have first been studied by [Ore 1933] as an unifying approach to differential and difference rings.

As a special case of Ore extensions we note the definition of differential operator rings.

Definition 3.4.3 (Differential operator ring) *Let $S = R[X;\alpha,\delta]$ be an Ore extension of R. If α is the identity map on R, then S is denoted by $R[X;\delta]$ and is called a (formal)* differential operator ring.

Let $S = R[X_1;\alpha_1,\delta_1][X_2;\alpha_2,\delta_2]\ldots[X_n;\alpha_n,\delta_n]$ be an iterated Ore extension of R. If the α_i are the identity maps of the respective rings we obtain an iterated differential operator ring*: $R[X_1;\delta_1][X_2;\delta_2]\ldots[X_n;\delta_n]$, denoted by*

$$R[X_1,X_2,\ldots,X_n;\delta_1,\delta_2,\ldots\delta_n].$$

For more information on differential operator rings see the books [Kolchin 1973] or the older [Ritt 1950].

As a special case of differential operator rings we obtain algebras of partial derivatives:

Definition 3.4.4 (Weyl algebra) *Let $R = \mathbf{R}[X_1,\ldots,X_n]$ be a polynomial ring over a ring $\mathbf{R}$. Then the formal partial derivatives $\delta_i = \partial/\partial_{X_i}$ $(1 \leq i \leq n)$ are commuting derivations on R. The* n-th Weyl algebra over $\mathbf{R}$ *is defined as the formal differential operator ring:*

$$\mathbf{R}[X_1,\ldots,X_n;Y_1,\ldots,Y_n;\partial/\partial_{X_1},\ldots\partial/\partial_{X_n}].$$

As a further special case of Ore extensions we note the definition of difference rings.

Definition 3.4.5 (Difference ring) *Let $S = R[X;\alpha,\delta]$ be an Ore extension of R. If α is an injective endomorphism of R and δ is the zero derivation, then S is denoted by $R[X;\alpha]$ and is called a (formal)* difference ring.

Let $S = R[X_1;\alpha_1,\delta_1][X_2;\alpha_2,\delta_2]\ldots[X_n;\alpha_n,\delta_n]$ be an iterated Ore extension of R. If the α_i are injective endomorphisms of the respective rings and all δ_i are zero, we obtain an iterated difference ring*: $R[X_1;\alpha_1][X_2;\alpha_2]\ldots[X_n;\alpha_n]$, denoted by*

$$R[X_1,X_2,\ldots,X_n;\alpha_1,\alpha_2,\ldots\alpha_n].$$

For more information on difference rings see the book [Cohn 1965].

The following theorems adapted from [Kandri-Rody, Weispfenning 1988] show under which conditions iterated Ore extensions are solvable polynomial rings. Note that with the (new) axioms 3.2.1 we are no more restricted to **K**-derivations for Ore extensions.

Theorem 3.4.6 *Let R be a field. Let $S = R[X_1;\alpha_1,\delta_1][X_2;\alpha_2,\delta_2]\ldots[X_n;\alpha_n,\delta_n]$ be an iterated Ore extension such that the endomorphisms α_i satisfy $\alpha_j(X_i) = c_{ij}X_i$ with $0 \neq c_{ij} \in R$ for $1 \leq i < j \leq n$. Since R is a field, the $\alpha_{j|R}$ are injective.*

Define commutator relations $Q = \{X_j * X_i = c_{ij}X_iX_j + p_{ij} \ : \ 1 \leq i < j \leq n\}$ and $Q' = \{X_j * a = c_{ai}aX_j + p_{ai} \ : \ 1 \leq i \leq n, a \in R\}$ by

$$c_{ij}X_i = \alpha_j(X_i),\ p_{ij} = \delta_j(X_i) \text{ for } 1 \leq i < j \leq n \text{ and}$$
$$c_{ai}a = \alpha_j(a),\ p_{ai} = \delta_j(a) \text{ for } 1 \leq i \leq n,\ a \in R.$$

Then $S' = R\{X_1,\ldots,X_n;Q,Q'\}$ is a solvable polynomial ring of strictly lexicographical type.

Proof: The proof is by induction on n. In case $n = 0$ nothing is to prove.

For $n > 0$, let $S = R'[X_n;\alpha_n,\delta_n]$ be such that by induction assumption R' is already a solvable polynomial ring of strict lexicographical type.

Since R is a field, the equation $\alpha_n(a) = c_{an}a$ is solvable for $0 \neq a \in R$ and determines $0 \neq c_{ai} \in R$. Furthermore define $p_{in} = \delta_n(X_i)$ for $1 \leq i < n$, and $p_{an} = \delta_n(a)$ for $a \in R$. The α_i are by assumption endomorphisms with the suitable definition of c_{in}. Furthermore $\delta_n(X_i) \in R[X_1,\ldots,X_{n-1}]$ so the strict lexicographical term order condition is fulfilled.

We define the $*$-product by

$$X_n * X_i = \alpha_n(X_i)X_n + \delta_n(X_i)$$

therefore satisfying axioms 3.2.1(3) and by

$$X_n * a = \alpha_n(a)X_n + \delta_n(a)$$

so satisfying axioms 3.2.1(4). The axioms 3.2.1(1,2) hold by definition of an Ore extension.

So the $*$-product satisfies all axioms 3.2.1 and this makes S' indeed a solvable polynomial ring as claimed. □

We remark, that in case R is not a field we have to add the condition $c_{ai}a = \alpha_j(a)$ such that $0 \neq c_{ai} \in R$ for $1 \leq i \leq n$, $0 \neq a \in R$ to show the claim of the theorem.

Theorem 3.4.7 *Let R be a field. Let $S' = R\{X_1,\ldots,X_n;Q,Q'\}$ be a solvable polynomial ring of strictly lexicographical type with $Q = \{X_j * X_i = c_{ij}X_iX_j + p_{ij} \ : \ 1 \leq i < j \leq n\}$ and $Q' = \{X_j * a = c_{ai}aX_j + p_{ai} \ : \ 1 \leq i \leq n, a \in R\}$.*

Define (mappings) α_i and δ_i by

$\alpha_j(X_i) = c_{ij}X_i$, $\delta_j(X_i) = p_{ij}$ *for* $1 \leq i < j \leq n$ *and*
$\alpha_j(a) = c_{ai}a$, $\delta_j(a) = p_{ai}$ *for* $1 \leq i \leq n$, $a \in R$.

Then $S = R[X_1; \alpha_1, \delta_1][X_2; \alpha_2, \delta_2] \ldots [X_n; \alpha_n, \delta_n]$ *is an iterated Ore extension.*

Proof: The proof is by induction on n. In case $n = 0$ nothing is to prove.

For $n > 0$, by the strict lexicographical condition we have $p_{in} \in R[X_1, \ldots, X_{n-1}]$. So by restriction $R_1' = R\{X_1, \ldots, X_{n-1}; Q^*, Q'^*\}$ is also a solvable polynomial ring of strict lexicographical type.

Now we know by lemmas 3.3.3 and 3.3.2 that the $\alpha_n(X_i) = c_{in}X_i$ for $1 \leq i < n$ and the $\alpha_n(a) = c_{an}a$ for $a \in R$ define injective endomorphisms of the respective rings. Furthermore the $\delta_n(X_i) = p_{in}$ for $1 \leq i < n$ and the $\delta_n(a) = p_{an}$ for $a \in R$ define (α_n)-derivations.

So the given definitions for α_n and δ_n satisfy all conditions of proposition 3.4.1 for an Ore extension $R_1'[X_n; \alpha_n, \delta_n]$. By induction assumption we may assume that the corresponding R_1 is an iterated Ore extension which completes the proof. □

The conditions of theorems 3.4.6 and 3.4.7 are in particular fulfilled if the α_j are the identity mapping on the respective rings. So we obtain the following corollaries for differential operator rings.

Corollary 3.4.8 *Let R be a field. Let $S = R[X_1 \ldots X_n; \delta_1 \ldots \delta_n]$ be an iterated differential operator ring. Define commutator relations $Q = \{X_j * X_i = X_iX_j + p_{ij} \ : \ 1 \leq i < j \leq n\}$ and $Q' = \{X_j * a = aX_j + p_{ai} \ : \ 1 \leq i \leq n, a \in R\}$ by*

$p_{ij} = \delta_j(X_i)$ *for* $1 \leq i < j \leq n$ *and*
$p_{ai} = \delta_j(a)$ *for* $1 \leq i \leq n$, $a \in R$.

Then $S' = R\{X_1, \ldots, X_n; Q, Q'\}$ is a solvable polynomial ring of strictly lexicographical type.

Especially Weyl algebras are iterated differential operator rings, so they are solvable polynomials rings with $p_{ij} = 1$ for $1 \leq i < j \leq n$ and $p_{ai} = 0$ for $1 \leq i \leq n$, $a \in R$.

Corollary 3.4.9 *Let R be a field. Let $S' = R\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring of strictly lexicographical type with $Q = \{X_j * X_i = X_iX_j + p_{ij} \ : \ 1 \leq i < j \leq n\}$ and $Q' = \{X_j * a = aX_j + p_{ai} \ : \ 1 \leq i \leq n, a \in R\}$.*

Define (mappings) δ_i by

$\delta_j(X_i) = p_{ij}$ *for* $1 \leq i < j \leq n$ *and*
$\delta_j(a) = p_{ai}$ *for* $1 \leq i \leq n$, $a \in R$.

Then $S = R[X_1 \ldots X_n; \delta_1 \ldots \delta_n]$ is an iterated differential operator ring.

The conditions of theorems 3.4.6 and 3.4.7 are in particular fulfilled if the α_j are injective endomorphisms of the respective rings and the δ_j are zero. Then also the condition on the strict lexicographical term order can be dropped and we obtain the following corollaries for difference rings.

Corollary 3.4.10 *Let R be a field. Let $S = R[X_1, \ldots, X_n; \alpha_1 \ldots \alpha_n]$ be an iterated difference ring such that the endomorphisms α_i satisfy $\alpha_j(X_i) = c_{ij}X_i$ with $0 \neq c_{ij} \in R$ for $1 \leq i < j \leq n$. Since R is a field, the $\alpha_{j|R}$ are injective.*

Define commutator relations $Q = \{X_j * X_i = c_{ij}X_iX_j \ : \ 1 \leq i < j \leq n\}$ and $Q' = \{X_j * a = c_{ai}aX_j \ : \ 1 \leq i \leq n, a \in R\}$ by

$c_{ij}X_i = \alpha_j(X_i)$ *for* $1 \leq i < j \leq n$ *and*
$c_{ai}a = \alpha_j(a)$ *for* $1 \leq i \leq n$, $a \in R$.

Then $S' = R\{X_1, \ldots, X_n; Q, Q'\}$ is a solvable polynomial ring.

Again note, that in case R is not a field we have to add the condition $\alpha_j(a) = c_{ai}a$ such that $0 \neq c_{ai} \in R$ for $1 \leq i \leq n$, $0 \neq a \in R$ to show the claim of the corollary.

Corollary 3.4.11 *Let R be a field. Let $S' = R\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring with $Q = \{X_j * X_i = c_{ij}X_iX_j \ : \ 1 \leq i < j \leq n\}$ and $Q' = \{X_j * a = c_{ai}aX_j \ : \ 1 \leq i \leq n, a \in R\}$.*

Define (mappings) α_i by

$\alpha_j(X_i) = c_{ij}X_i$ *for* $1 \leq i < j \leq n$ *and*
$\alpha_j(a) = c_{ai}a$ *for* $1 \leq i \leq n$, $a \in R$.

Then $S = R[X_1, \ldots, X_n; \alpha_1 \ldots \alpha_n]$ is an iterated difference ring.

Since R is a field (so a domain) the condition that α is injective is automatically fulfilled by our definition of solvable polynomial rings.

3.4.2 Enveloping Algebras of Lie Algebras

For the case of enveloping algebras of Lie algebras we do not obtain more in our current framework for solvable polynomial rings 3.2.1. We therefore state the results from [Kandri-Rody, Weispfenning 1988]. Enveloping algebras of Lie algebras are examples of solvable polynomial rings, which are not of strictly lexicographical type.

Definition 3.4.12 (Lie algebra) *Let $L = (L, +, -, \cdot, 0, 1, \mathbf{K})$ be a vector space over a field $\mathbf{K}$. Let $\times$ be a bi-linear composition on L, that is the $\times$ operation satisfies the following formulas:*

Lb1: $(x_1 + x_2) \times y = x_1 \times y + x_2 \times y$,

Lb2: $y \times (x_1 + x_2) = y \times x_1 + y \times x_2$,

Lb3: $a(x \times y) = a(x) \times y = x \times a(y)$,

where $x_1, x_2, y \in L$ *and for* $a \in \mathbf{K}$, $a : L \longrightarrow L$ *is the left scalar multiplication by* a.
L *is a called a* Lie algebra *if the* $\times$ *operation satisfies in addition the formulas*

Lb4: $x \times x = 0$,

Lb5: $(x \times y) \times z + (y \times z) \times x + (z \times x) \times y = 0$,

where $x, y, z \in L$. *'Lb5' is called* Jacobi identity.

Definition 3.4.13 *For any associative algebra* $A = (A, +, -, \cdot, *, 0, 1, \mathbf{K})$ *we can define a Lie algebra* $A_L = (A, +, -, \cdot, \times, 0, 1, \mathbf{K})$ *by defining* $\times : A^2 \longrightarrow A$ *by*

$$x \times y = [x, y] = x * y - y * x$$

for $x, y \in A$. $[x, y]$ *is called the* Lie product *or* commutator *of* x *and* y.

It is easily verified, that the definition of the $\times$ function satisfies all conditions of the $\times$ operation of a Lie algebra.

Definition 3.4.14 (Universal envelope) *Let* L *be a Lie algebra over a (commutative) field* $\mathbf{K}$. *An associative algebra* $U(L)$ *together with an injective homomorphism* $\phi : L \longrightarrow U(L)_L$ *is called an* universal enveloping algebra of L *if the following conditions are satisfied:*

If A *is any associative algebra and* $\psi : L \longrightarrow A_L$ *is an injective homomorphism, then there exists a unique injective homomorphism* $\varphi : U(L) \longrightarrow A$ *such that* $\psi = \varphi \circ \phi$.

For every Lie algebra L there exists a universal enveloping algebra $U(L)$, which is unique up to isomorphism. The construction of $U(L)$ is described in [Jacobson 1962](p 155).

Theorem 3.4.15 (Poincaré-Birkhoff-Witt) *Let* L *be a Lie algebra over a (commutative) field* $\mathbf{K}$, *finitely generated with basis* $X_1, \ldots, X_n$. *Furthermore let* $U(L)$ *be the universal enveloping algebra of* L. *Then the elements of* $U(L)$ *can be represented uniquely as commutative polynomials in* $\mathbf{K}[X_1, \ldots, X_n]$.

Proof: See [Jacobson 1962](p 159). □

For the product $*$ in $U(L)$ we have

$$X_j * X_i - X_i * X_j = [X_i, X_j] = p_{ij}$$

for $1 \leq i < j \leq n$. And since $X_i, X_j \in L$ we have $[X_i, X_j] \in L$, so that p_{ij} is a linear combination of the $X_1, \ldots, X_n$. So $\deg(p_{ij}) \leq 1 < 2 = \deg(X_i X_j)$ and for a degree compatible order $<$ on T it follows $p_{ij} < X_i X_j$ for $1 \leq i < j \leq n$.

If L is a *solvable* Lie algebra then for a suitable choice of the basis $X_1, \ldots, X_n$ of L it holds that $p_{ij} \in \mathbf{K}[X_1, \ldots, X_{j-1}]$. See [Jacobson 1962](p 50) and [Dixmier 1974]. So in this case also for the lexicographical order $X_1 < \ldots < X_n$ we have $p_{ij} < X_j$ for $1 \leq i < j \leq n$.

We can now define the commutator relations Q, Q' for a solvable polynomial ring as:

$$X_j * X_i = X_i X_j + p_{ij}$$

that is $c_{ij} = 1$, $p_{ij} = \sum_{k=1}^{n} a_{ijk} X_k = [X_i, X_j]$, $a_{ijk} \in \mathbf{K}$, $1 \leq i \leq j \leq n$, $1 \leq k \leq n$, and $c_{ai} = 1$, $p_{ai} = 0$ for $1 \leq i \leq n$, $a \in \mathbf{K}$.

In all cases the algebra $U(L)$ satisfies the axioms 3.2.1 and so we obtain theorem 1.14 of [Kandri-Rody, Weispfenning 1988]:

Theorem 3.4.16 *Let L be a finite dimensional Lie algebra with basis $X_1, \ldots, X_n$ over a field $\mathbf{K}$. Then the universal enveloping algebra $U(L)$ of L is a solvable polynomial ring $\mathbf{K}\{X_1, \ldots, X_n; Q\}$ with respect to any degree compatible admissible order $<$ on T. Moreover, if L is solvable, then for a suitable choice of the basis $X_1, \ldots, X_n$ the order $<$ may be taken as lexicographical order.*

Almost Normalizing Extensions

In [McConnell, Robson 1987](p 28), a generalization of skew polynomial rings and enveloping algebras is introduced as follows.

Definition 3.4.17 *Let S be a finitely generated extension of a ring R with generators $X_1, \ldots, X_n$. Assume the generators satisfy the following conditions*

1. *$RX_i = X_i R + R$, for $1 \leq i \leq n$,*
2. *$X_i X_j - X_j X_i \in \sum_{k=1,\ldots,n} X_k R \; + R$, for $1 \leq i, j \leq n$.*

Then S is called an almost normalizing extension of R.

The motivation for this definition is that the 'head terms' of the elements of S behave like the head terms of commutative polynomials. (The associated graded module $\mathrm{gr}(S) = R[\hat{X}_1, \ldots, \hat{X}_n]$ is commutative.)

It is clear, that such rings can be considered as solvable polynomial rings, if we take a degree compatible term order on the X_i.

3.4.3 Quotients of Free Associative Algebras

In this section we discuss under which conditions a homomorphic image of a free associative algebra is a solvable polynomial ring. As a special case, we obtain the results of [Kandri-Rody, Weispfenning 1988] in the case that the variables commute with the coefficients in the definition of a solvable polynomial ring.

Let $P = \mathbf{K}\ll X_1, \ldots, X_n\gg$, be a free associative ring, generated by $\mathbf{K}$ and non-commuting variables $X_1, \ldots, X_n$. Let $Q = \{q_{ij} = X_jX_i - c_{ij}X_iX_j - p_{ij} \ : \ c_{ij} \in \mathbf{K} \setminus \{0\},\ p_{ij} \in P,\ 1 \leq i < j \leq n\}$, where the p_{ij} are commutative polynomials and $p_{ij} < X_iX_j$ for a fixed admissible term (word) order $<$. Furthermore let $Q' = \{q_{ai} = X_ia - c_{ai}aX_i - p_{ai} \ : \ c_{ai} \in \mathbf{K} \setminus \{0\},\ p_{ai} \in \mathbf{K},\ a \in \mathbf{K},\ 1 \leq i < j \leq n\}$, where the p_{ai} are elements of $\mathbf{K}$.

$Q \cup Q'$ is called a *commutation system* for $(P, <)$. For definitions of admissible word orders $<$ see e.g. [Mora 1985].

Definition 3.4.18 *Let* $\mathrm{ideal}_t(Q \cup Q')$ *denote the two-sided ideal generated by* $Q \cup Q'$ *in* P. *Then let (NoCg) denote the following hypothesis about* $\mathrm{ideal}_t(Q \cup Q')$*:*

(NoCg) $\mathrm{ideal}_t(Q \cup Q')$ *contains no non-zero commutative polynomial.*

Theorem 3.4.19 *Let* P *be a free associative ring generated by* $\mathbf{K}$ *and* $X_1, \ldots, X_n$*, for a field* $\mathbf{K}$. *Let* $Q \cup Q'$ *be a commutation system for* $(P, <)$ *and let* $R = P/\mathrm{ideal}_t(Q \cup Q')$. *Denote the residue class of* X_i *mod* $\mathrm{ideal}_t(Q \cup Q')$ *by* x_i *and let* $R = \mathbf{K}\ll x_1, \ldots, x_n\gg$ *be the free associative ring generated by* $\mathbf{K}$ *and* $x_1, \ldots, x_n$.

Then $Q \cup Q'$ *satisfies hypothesis (NoCg) if and only if* R *is canonically isomorphic to a solvable polynomial ring* $S = \mathbf{K}\{Y_1, \ldots, Y_n; \bar{Q}, \bar{Q}'\}$ *with respect to* $<$ *and the multiplication* $*$ *of* S *under an isomorphism fixing* $\mathbf{K}$ *pointwise and mapping* x_i *onto* Y_i. *Where* $\bar{Q}$, $\bar{Q}'$ *denote the commutator relations* Q, Q' *written in the variables* Y_i.

Proof: "$\Longrightarrow$" Let $S' = \mathbf{K}[Y_1, \ldots, Y_n]$ and let $R' = \mathbf{K}[x_1, \ldots, x_n]$. Furthermore let $R = \mathbf{K}\ll x_1, \ldots, x_n\gg = P/\mathrm{ideal}_t(Q \cup Q')$. So $R' \subseteq R$ and we have the situation

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & \searrow & \\ \pi & & R & \longleftrightarrow & S \\ & & & \psi & \end{array}$$

Where π is the canonical homomorphism and ψ is defined as follows

$$\begin{array}{rcll} \psi : \mathbf{K}[Y_1, \ldots, Y_n] & \longrightarrow & \mathbf{K}\ll x_1, \ldots, x_n\gg & \\ Y_i & \mapsto & x_i, & i = 1, \ldots, n \\ a & \mapsto & a, & a \in \mathbf{K} \end{array}$$

We are going to show, that ψ is bijective and preserves the $*$-product.

By assumption $\text{ideal}_t(Q \cup Q')$ does not contain a commutative polynomial, so every non-zero element (a commutative polynomial) of S maps to a non-zero element of R, i.e. ψ is an embedding. So $\psi(S) = R' \subseteq R$. Denote the multiplication in R' by $\cdot$ and in R by $*$, i.e. $f(x_1, \ldots, x_n) * g(x_1, \ldots, x_n) = f(X_1, \ldots, X_n)g(X_1, \ldots, X_n) + \text{ideal}_t(Q \cup Q')$.

We claim, that R' is closed under $*$. By definition of R and $*$ we have $x_j * x_i = X_jX_i + \text{ideal}_t(Q \cup Q') = (c_{ij}X_iX_j + p_{ij}) + \text{ideal}_t(Q \cup Q') = c_{ij}x_ix_j + p_{ij}$ and $x_i * a = X_ia + \text{ideal}_t(Q \cup Q') = (c_{ai}aX_i + p_{ai}) + \text{ideal}_t(Q \cup Q') = c_{ai}ax_i + p_{ai}$. That is, R' satisfies all axioms of 3.2.1, except possibly the closedness under $*$. So the product proposition 3.2.5 holds in R' and we have $f * g = c \cdot f \cdot g + h$ for $f, g, h \in R'$ and $0 \neq c \in \mathbf{K}$. But this shows that $f * g \in R'$.

Finally every element of R is a sum over $*$-products of the $x_1, \ldots, x_n$ and elements of $\mathbf{K}$. This shows $R' = R$ as sets which implies, that ψ is surjective and hence is bijective. By definition of the $*$-product in S and in R we see that ψ is also a $*$-homomorphism, which completes the proof of this direction.

"$\Longleftarrow$" Assume R and S are canonically isomorphic by an isomorphism $\phi : R \longrightarrow S$. Let $f \neq 0 \in P$ be a commutative polynomial. Since f is a non-zero commutative polynomial and the $Y_1, \ldots, Y_n$ together with the $a \in \mathbf{K}$ do not satisfy a commutative relation in S, we have $f(Y_1, \ldots, Y_n) \neq 0$ in S. Since ϕ is an isomorphism, also $0 \neq \phi^{-1}(f(Y_1, \ldots, Y_n)) = f(x_1, \ldots, x_n)$. This shows, that $0 \neq f$ in R and so $f \notin \text{ideal}_t(Q \cup Q')$. $\square$

Corollary 3.4.20 *Let P be a free associative ring generated by $\mathbf{K}$ and $X_1, \ldots, X_n$, for a field $\mathbf{K}$. Let $\phi : P \longrightarrow S$ be the canonical homomorphism between P and a solvable polynomial ring $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$. Let $Q \cup Q'$ be a commutation system for $(P, <)$, then $Q \cup Q'$ satisfies hypothesis (NoCg).*

Proof: Since ϕ is a canonical homomorphism we have $\ker(\phi) = \text{ideal}_t(Q \cup Q')$ so by theorem 3.4.19 $Q \cup Q'$ must satisfy hypothesis (NoCg). $\square$

The results from [Kandri-Rody, Weispfenning 1988] are a special case of the foregoing for solvable polynomial rings in which the variables commute with the coefficients.

Let $P = \mathbf{K}\langle X_1, \ldots, X_n \rangle$ be a free associative algebra over $\mathbf{K}$, generated by non-commuting variables $X_1, \ldots, X_n$, which commute with the elements of $\mathbf{K}$. Let $Q = \{q_{ij} = X_jX_i - c_{ij}X_iX_j - p_{ij} \ : \ c_{ij} \in \mathbf{K} \setminus \{0\},\ p_{ij} \in P,\ 1 \leq i < j \leq n\}$. Where the p_{ij} are commutative polynomials and

$p_{ij} < X_iX_j$ for a fixed admissible term (word) order $<$. Q is called a *commutation system* for $(P, <)$.

Definition 3.4.21 *Let* $\text{ideal}_t(Q)$ *denote the two-sided ideal generated by Q in P. Then let (NoC) denote the following hypothesis about* $\text{ideal}_t(Q)$*:*

(NoC) $\text{ideal}_t(Q)$ *contains no non-zero commutative polynomial.*

Corollary 3.4.22 *([Kandri-Rody, Weispfenning 1988] th 1.7) Let P be a free associative algebra generated by $X_1, \ldots, X_n$ over a field $\mathbf{K}$. Let Q be a commutation system for $(P, <)$ and let $R = P/\mathrm{ideal}_t(Q)$. Denote the residue class of X_i mod $\mathrm{ideal}_t(Q)$ by x_i and let $R = \mathbf{K}\langle x_1, \ldots, x_n\rangle$. Then Q satisfies hypothesis (NoC) if and only if R is canonically isomorphic to a solvable polynomial ring $S = \mathbf{K}\{Y_1, \ldots, Y_n; \bar{Q}\}$ with respect to $<$ and the multiplication $*$ of S under an isomorphism fixing $\mathbf{K}$ pointwise and mapping x_i onto Y_i. Where $\bar{Q}$ denotes the commutator relations Q written in the variables Y_i.*

Corollary 3.4.23 *Let P be a free associative algebra generated by $X_1, \ldots, X_n$ over a field $\mathbf{K}$. Let $\phi : P \longrightarrow S$ be the canonical homomorphism between P and a solvable polynomial ring $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$. Let Q be a commutation system for $(P, <)$, then Q satisfies hypothesis (NoC).*

Commutation Systems with (NoC)

Using results from [Mora 1986], [Kandri-Rody, Weispfenning 1988] prove the following characterization of commutation systems satisfying (NoC). It is an open problem, if the results from Mora can be generalized to free associative rings and commutation systems satisfying hypothesis (NoCg).

Theorem 3.4.24 (Mora) *Let Q be a commutation system for $(P, <)$. Then hypothesis (NoC) holds for Q if and only if Q is a (free) Gröbner base for $\mathrm{ideal}_t(Q)$ with respect to the order $<$.*

Proof: See [Kandri-Rody, Weispfenning 1988](th 1.11). □

Moreover the condition if hypothesis (NoC) holds for Q can be checked algorithmically by the (free) Gröbner base algorithm of [Mora 1986].

Corollary 3.4.25 *Let $<$ be an admissible term order on T that can be extended to a positive term order on the words $W(X_1, \ldots, X_n)$ such that $t <' X_j X_i$ for $j > i$ and $t \in T(X_1, \ldots, X_j)$. Then there is an algorithm that decides for any commutation system Q for $(P, <)$ whether Q satisfies hypothesis (NoC).*

Using the product lemma 3.2.5 together with a strict lexicographical term order we can also allow for more general commutation system for P.

Theorem 3.4.26 *Let P be a free associative algebra generated by $X_1, \ldots, X_n$. Let Q be a commutation system for $(P, <)$ such that the possibly non-commutative polynomials $p_{ij} = p_{ij}(X_1, \ldots, X_{j-1}) \in P$ depend only on $X_1, \ldots, X_{j-1}$ and the $c_{ij} = 1$. Then $R = P/\mathrm{ideal}_t(Q)$ is a solvable polynomial ring of strict lexicographical type if and only if hypothesis (NoC) holds for Q.*

Proof: See [Kandri-Rody, Weispfenning 1988](th 1.13). □

Definition 3.4.27 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{K}$ and let I be a two-sided ideal in R. Then $A = R/I$ is called an* algebra of solvable type over $\mathbf{K}$ *generated by $a_1, \ldots, a_n$, where $a_i = X_i + I$ for $1 \leq i \leq n$.*

An important class of $\mathbf{K}$-algebras that satisfy the assumptions of this section are the so called Clifford and Grassmann algebras which we will discuss next.

Clifford and Grassmann Algebras

Definition 3.4.28 *Let $R = \mathbf{K}[X_1, \ldots, X_n]$ be a (commutative) polynomial ring over a (commutative) field $\mathbf{K}$. Let $q \in R$ be a quadratic form defined as*

$$q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq n} q_i X_i^2 + \sum_{1 \leq i < j \leq n} q_{ij} X_i X_j,$$

where $q_i, q_{ij} \in \mathbf{K}$ for $1 \leq i < j \leq n$. Then let C be the $\mathbf{K}$-algebra generated by $X_1, \ldots, X_n$ and multiplication defined by

$$\begin{aligned} U * U &= q(U) \\ U * V - V * U &= q(U + V) - q(U) - q(V), \end{aligned}$$

where $U, V \in C$ with $U = \sum_{1 \leq i \leq n} u_i X_i$, $V = \sum_{1 \leq i \leq n} v_i X_i$ and $q(U)$ defined as $q(u) = q(u_1 X_1, \ldots, u_n X_n)$.
The algebra C defined by extension of $*$ is called Clifford algebra. *If $q \equiv 0$ then C is called* Grassmann algebra.

See e.g. [V. d. Waerden 1971](sec 93.5) for details and properties.

Proposition 3.4.29 *[Kandri-Rody, Weispfenning 1988] Let*

$$q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq n} q_i X_i^2 + \sum_{1 \leq i < j \leq n} q_{ij} X_i X_j,$$

be a quadratic form. Let $R = \mathbf{K}\langle X_1, \ldots, X_n \rangle / \mathrm{ideal}_t(Q)$ where Q is the commutation system defined by

$$Q = \{X_j X_i + X_i X_j - q_{ij} \ : \ 1 \leq i < j \leq n\}.$$

Then R is a polynomial ring of solvable type and $R = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ with commutator relations Q. Furthermore let

$$P = \{X_i^2 - q_i \ : \ 1 \leq i \leq n\}.$$

Then $C = R/\mathrm{ideal}_t(P)$ is a Clifford algebra determined by q.

Proof: Since $q_{ij} \in \mathbf{K}$, Q is already a Gröbner base in $\mathbf{K}\langle X_1, \ldots, X_n \rangle$. So Q satisfies hypothesis (NoC) and so by theorem 3.4.22 R is a solvable polynomial ring.

Now P is already a Gröbner base in R since all S-polynomials reduce to 0 with respect to P (and the commutator relations Q). Now $f \in R$ is in normal form with respect to P, iff f is at most linear in each X_i, $1 \leq i \leq n$. This shows that $R/\mathrm{ideal}_t(P)$ is a Clifford algebra defined by q. $\square$

3.5 A Hilbert Basis Theorem

In this section we are going to establish that solvable polynomial rings are so called Noetherian rings. To show this we prove a version of Hilbert's Basis Satz for solvable polynomial rings. Note that this theorem cannot be proved by iterated Ore extensions unless $R\{X_1, \ldots, X_n; Q, Q'\}$ is a solvable polynomial ring of strictly lexicographical type. We use a combination of Dickson's lemma and a variant of Königs tree lemma in the proof of 'Hilbert basis theorem'.

Definition 3.5.1 (Noetherian ring) *A ring R is called a left (right)* Noetherian ring *if it satisfies the following equivalent conditions*

ACC *There does not exist an infinite sequence of left (right) ideals such that every ideal is properly contained in its successor.*

MAX *Every non empty family of left (right) ideals of R has a maximal element.*

HIB *Every left (right) ideal of R is finitely generated.*

If R is both left and right Noetherian it is called Noetherian.

For a proof of the equivalence of this conditions see e.g. [Goodearl, Warfield 1989]. Condition 'HIB' is also known as Hilbert's Basis Satz, condition 'ACC' is called the *ascending chain condition* and condition 'MAX' is called the maximality condition.

Troughout this section let R be a (non-commutative) domain with 1 and let $S = R\{X_1, \ldots, X_n; Q, Q'\}$ be a (non-commutative) polynomial ring of solvable type over R in the variables $X_1, \ldots, X_n$ with respect to the extended axioms 3.2.2.

> In case we consider right ideals we will make the global assumption in this section, that the mapping $a \mapsto c_{ai}a$ is an automorphism.

Recall that T denotes the set of terms (power products) of variables and that the elements of T are totally ordered by an fixed admissible order $<$. Furthermore for $f \in S$, $\mathrm{HT}(f) = \mathrm{HT}_<(f)$ denotes the highest term (head term) in f with respect to a given term order $<$ and that $\mathrm{HC}(f) = \mathrm{coeff}(\mathrm{HT}(f), f)$ is the coefficient of the head term of f.

Definition 3.5.2 *Let J be a subset of S. For $t \in T$ let*

$$J_t = \{\mathrm{HC}(f) \ : \ f \in J, \mathrm{HT}(f) = t\} \cup \{0\}.$$

Lemma 3.5.3 *Let J be a left (right) ideal in S with respect to the extended axioms (and for right ideals the mapping $a \mapsto c_{ai}a$ is an automorphism). Then for every $t \in T$, J_t is a left (right) ideal in R.*

Proof: Let $t \in T$. Let $0 \neq a, b \in J_t$ and let $f, g \in J$ with $\mathrm{HC}(f) = a$ and $\mathrm{HC}(g) = b$. To show $a - b \in J_t$ let $c = a - b$ and let $h = f - g$. Now either $c \neq 0$ and since $h \in J$ and $\mathrm{HT}(h) = t$ we have $\mathrm{HC}(h) = c \in J_t$, or $c = 0$ then by definition $0 \in J_t$. For a left ideal we show $\alpha a \in J_t$ for $\alpha \in R$. Let $c = \alpha a$ and let $h = \alpha f \in J$. Now either $c \neq 0$ and since $h \in J$ and $\mathrm{HT}(h) = t$ we have $\mathrm{HC}(h) = c \in J_t$, or $c = 0$ then by definition $0 \in J_t$.

For a right ideal we show $a\alpha \in J_t$ for $\alpha \in R$. Let $c = a\alpha$ and let $h = f\alpha' \in J$ for α' so that $\mathrm{HC}(f * \alpha') = a\alpha$. Now either $c \neq 0$ and since $h \in J$ and $\mathrm{HT}(h) = t$ we have $\mathrm{HC}(h) = c \in J_t$, or $c = 0$ then by definition $0 \in J_t$. □

Lemma 3.5.4 *Let J be a left (right) ideal in S and let S satisfy the extended axioms. Furthermore let $t, t' \in T$. If $t \mid t'$ then $J_t \subseteq J_{t'}$.*

Proof: Let $t' = ut$ for some $u \in T$. Let $a \in J_t$, $f \in J$ with $\mathrm{HC}(f) = a$. Then $u * f \in J$ with $\mathrm{HT}(u * f) = t'$.

Now S is assumed to satisfy the extended axioms, so either R is a skew field and for $c = \mathrm{HC}(u*f)$ there exists $0 \neq b \in R$, such that $\mathrm{HC}(bu*f) = bc = a$, with $bu*f \in J$. This shows $a \in J_{t'}$. In the other case all c_{ij} and all c_{ai} are contained in a subfield of the center. By the product lemma 3.2.5 we have $\mathrm{HC}(u * f) = ca$, where $0 \neq c$ is a product of some c_{ij} and some c_{ai}. So c is invertible, say by c' and we obtain $\mathrm{HC}(c'u * f) = c'ca = 1a = a$. Again $c'u * f \in J$ and so $a \in J_{t'}$. Similarly for right ideals. □

Definition 3.5.5 *Let J be a left (right) ideal in S. Let B_J denote the set of ideals J_t. Define a partial order on B_J by set inclusion $\subseteq$. Let $J_1, J_2 \in B_J$, then we call J_2 an immediate successor of J_1 if $J_1 \subseteq J_2$, $J_1 \neq J_2$ and there is no $J_3 \in B_J$, such that $J_1 \subseteq J_3 \subseteq J_2$ and $J_1 \neq J_2 \neq J_3$. We write $J_1 \subset J_2$ if $J_1 \subseteq J_2$ and $J_1 \neq J_2$.*

Lemma 3.5.6 *Let J be a left (right) ideal in S and let S satisfy the extended axioms. Let $(B_J, \subseteq)$ denote the partially ordered set of ideals J_t. Then B_J has only finitely many minimal elements and each $J_t \in B_J$ has only finitely many immediate successors.*

Proof: First let $U = \{u \in T \ : \ J_u \in B_J\}$, then by Dickson's lemma 3.1.1 there exists a finite subset $U^* \subseteq U$ such that every $u \in U$ is a multiple of some $u' \in U^*$. This shows that $\{J_{u'} \ : \ u' \in U^*\}$ is a finite set of minimal elements in B_J.

Next for $t \in T$, let $A = \{J_u \ : \ J_t \subset J_u, J_t \neq J_u\}$ be the set of successors of J_t and let $U = \{u \in T \ : \ J_u \in A\}$. By Dickson's lemma 3.1.1 there exists a finite subset $U^* \subseteq U$ such that every $u \in U$ is a multiple of some $u' \in U^*$. This shows that the set $A^* = \{J_{u'} \ : \ u' \in U^*\}$ of immediate successors of J_t is finite. So there are only finitely many immediate successors for each element of B_J. □

To proceed we need a partial order version of König's tree lemma:

Lemma 3.5.7 *Let the partial order $(B_J, \subseteq)$ be infinite and assume that B_J has only finitely many minimal elements and that for any element there are only finitely many immediate successors. Then there exists an infinite sequence $F = J_{t_1} \subset J_{t_2} \subset J_{t_3} \subset \ldots$ in B_J, such that each J_{t_i} has infinitely many successors.*

Proof: Let J_{t_1} be one of the finitely many minimal elements, such that J_{t_1} has infinitely many successors. Such a choice is possible, since B_J is infinite and so there must be one element which has infinitely many successors.

Let $j > 0$ and assume J_{t_j} has already been chosen such that J_{t_j} has infinitely many successors. By assumption for any element there are only finitely many immediate successors, say $J_{s_1}, \ldots, J_{s_k}$ for J_{t_j}. Since B_J is infinite and J_{t_j} has infinitely many successors, there must be one $1 \leq i \leq k$ such that J_{s_i} has infinitely many successors. Then for $j+1$ define $t_{j+1} = s_i$. So by the axiom of choice there exists an infinite sequence $J_{t_1} \subset J_{t_2} \subset J_{t_3} \subset \ldots$. □

Lemma 3.5.8 *Let J be a left (right) ideal in S and let S satisfy the extended axioms. Let $(B_J, \subseteq)$ denote the partially ordered set of ideals J_t. If R is left (right) Noetherian then B_J is finite.*

Proof: Assume for a contradiction, that the set B_J is infinite. Then by lemma 3.5.6 the assumptions of lemma 3.5.7 are fulfilled and so there exists an infinite sequence $F = J_{t_1} \subset J_{t_2} \subset J_{t_3} \subset \ldots$ in B_J. Since the J_t are ideals in R – which is left (right) Noetherian – any sequence of the J_t becomes stationary. So the sequence F is finite. This contradicts our assumption that B_J is infinite and so proves the lemma. □

Lemma 3.5.9 *Let J be an left (right) ideal in S and let S satisfy the extended axioms. Let $(B_J, \subseteq)$ denote the partially ordered set of ideals J_t. Let R be left (right) Noetherian, so that B_J is finite. Then there exists a finite set $T_J \subset T$, such that the following condition holds:*

For all $J_s \in B_J$ there exists $t \in T_J$ with $J_t = J_s$ and $t \mid s$.

Proof: For $s \in T$ such that $J_s \in B_J$ let $A_s = \{t' \in T \ : \ J_{t'} = J_s, t' \mid s\}$. By Dickson's lemma 3.1.1 there exists a finite basis A_s^* of A. Now let

$$T_J = \bigcup_{J_s \in B_J} A_s^*$$

Then T_J is finite, since each A_s^* is finite and by assumption B_J is finite. The condition on T_J holds by construction. □

Definition 3.5.10 *Since R is left (right) Noetherian, each J_t is finitely generated. Let $J_t = \mathrm{ideal}_l(a_{i_1}, \ldots, a_{i_t})$ and let $F_t = \{f_{i_1}, \ldots, f_{i_t}\}$, where each $f_{i_k} \in J$ is chosen such that $\mathrm{HT}(f_{i_k}) = t$ and $\mathrm{HC}(f_{i_k}) = a_{i_k}$. Let*

$$F_J = \bigcup_{t \in T_J} F_t.$$

Since T_J is finite and each F_t is finite, F_J is finite too.

Lemma 3.5.11 *Let J be a left (right) ideal in S and let S satisfy the extended axioms. Let R be left (right) Noetherian and let F_J be defined as before. Then any $f \in J$ has a representation*

$$f = \sum_{i \in \Lambda} \alpha_i u_i * f_i \qquad (f = \sum_{i \in \Lambda} f_i * \alpha_i u_i),$$

where $\alpha_i \in R$, $u_i \in T$ and $f_i \in F_J$ for $i \in \Lambda$, $|\Lambda| < \infty$. Thus J is finitely generated by F_J.

Proof: Assume for a contradiction that the claim does not hold. Then there exists a polynomial $f \in J$, $\mathrm{HT}(f)$ minimal, such that f has no such representation. Let $\mathrm{HC}(f) = a$ and $\mathrm{HT}(f) = t$. By lemma 3.5.9 there exists $s \in T_J$ such that $s \mid t$ and $a \in J_s$. Let $t = us$ for some $u \in T$. So $a = \sum_{j=i_1,\ldots,i_s} \beta_j a_j$. Let $f_j \in F_J$ with $\mathrm{HC}(f_j) = a_j$. Now S satisfies the extended axioms and so the head coefficients of the $u * f_j$ are either equal to a_j (in this case let $\alpha_j = \beta_j$) or there exist $\alpha_j \in R$ such that $\beta_j a_j = \alpha_j \mathrm{HC}(u * f_j)$ for $j = i_1, \ldots, i_s$. Then for the polynomial

$$f' = f - \sum_{j=i_1,\ldots,i_s} \alpha_j u * f_j$$

we have $\mathrm{coeff}(t, f') = 0$ and so $\mathrm{HT}(f') < \mathrm{HT}(f)$. Now by assumption on f we know that f' has a representation $\sum_{i \in \Lambda'} \alpha_i u_i * f_i$ with respect to F_J. But then $f = \sum_{j=i_1,\ldots,i_s} \alpha_j u * f_j + \sum_{i \in \Lambda'} \alpha_i u_i * f_i$ is a representation of f with respect to F_J. This contradicts the existence of such an f and thus proves that f has a representation with respect to F_J. Finally $J = \mathrm{ideal}_l(F_J)$ since each f has a representation with respect to F_J. A similar reasoning establishes the claim for right ideals. □

Theorem 3.5.12 (Hilbert Basis Satz) *If R is left (right) Noetherian, then any polynomial ring of solvable type $S = R\{X_1, \ldots, X_n; Q, Q'\}$ which satisfies the extended axioms (and for right ideals the mapping $a \mapsto c_{ai}a$ is an automorphism) is left (right) Noetherian. If R is Noetherian, then S is Noetherian.*

Proof: By lemma 3.5.11 any left (right) ideal in S is finitely generated. So S is left (right) Noetherian. □

Note, that the theorem holds not only if S is an iterated Ore extension.

3.6 Center of Solvable Polynomial Rings

Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over a commutative field $\mathbf{R}$ in the variables $X_1, \ldots, X_n$, such that the coefficients commute with the variables (i.e. $c_{ai} = 1$ and $p_{ai} = 0$ for $1 \leq i \leq n$, $0 \neq a \in \mathbf{R}$; in some cases we will moreover assume that $c_{ij} = 1$ for $1 \leq i < j \leq n$). Furthermore let $\mathrm{char}(\mathbf{R})$ denote the characteristic of $\mathbf{R}$.

An immediate fact is that the center of such a solvable polynomial ring consists exactly of all polynomials which commute with all variables. Furthermore we show how to determine all elements of the center up to a given degree bound and that non-commuting variables have only trivial centralizer in case the underlying field has characteristic zero.

Definition 3.6.1 *Let S be a ring. The* center of S *is the set of all elements of S which commute with all elements of S:*

$$\mathrm{cen}(S) = \{a \in S \ : \ ab = ba \text{ for all } b \in S\}.$$

Let I be a subset of S. The centralizer of I in S *is the set of all elements of S which commute with all elements of I:*

$$\mathrm{cen}_S(I) = \{a \in S \ : \ ab = ba \text{ for all } b \in I\}.$$

For $a, b \in S$, $[a,b] = ab - ba$ denotes the commutator of a and b.

Proposition 3.6.2 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$. Then*

$$\mathrm{cen}(S) = \mathrm{cen}_S(X).$$

Proof: "$\subseteq$" holds, since X is a subset of S.

"$\supseteq$" Let $f \in \mathrm{cen}_S(X)$, we show $f \in \mathrm{cen}(S)$. We must show $f * g = g * f$ for all $g \in S$. Assume first, that $g = u = X_1^{e_1} \ldots X_n^{e_n} \in T(X)$. Then we have

$$\begin{aligned}
f * u &= f * (X_1^{e_1} \ldots X_n^{e_n}) \\
&= f * (\underbrace{X_1 \ldots X_1}_{e_1} \ldots \underbrace{X_n \ldots X_n}_{e_n}) \\
f \in \mathrm{cen}_S(X) \quad &= (\underbrace{X_1 \ldots X_1}_{e_1} \ldots \underbrace{X_n \ldots X_n}_{e_n}) * f \\
&= (X_1^{e_1} \ldots X_n^{e_n}) * f \\
&= u * f.
\end{aligned}$$

In other words $f \in \mathrm{cen}_S(T(X))$. Now let $g \in S$ be arbitrary, $g = \sum_k \alpha_k u_k$, where $\alpha_k \in \mathbf{R}$ and $u_k \in T(X)$. Then we have

$$\begin{aligned}
f * g &= f * (\sum_k \alpha_k u_k) = \sum_k \alpha_k f * u_k \\
f \in \mathrm{cen}_S(T(X)) \quad &= \sum_k \alpha_k u_k * f \\
&= (\sum_k \alpha_k u_k) * f \\
&= g * f.
\end{aligned}$$

This shows $f \in \mathrm{cen}(S)$ and completes the proof. □

An immediate consecuence of the foregoing proposition is that center membership is decidable.

Proposition 3.6.3 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Assume $\mathbf{R}$ is computable and the term order is decidable. Then there exists an algorithm which decides for any $f \in S$ if $f \in \mathrm{cen}(S)$.*

Proof: Let $X = \{X_1, \ldots, X_n\}$. By proposition 3.6.2 $f \in \mathrm{cen}(S)$ iff $f \in \mathrm{cen}_S(X)$ iff

$$f * X_i - X_i * f = 0, \qquad 1 \leq i \leq n.$$

This condition can clearly be decided if we can compute in the solvable polynomial ring S. $\square$

3.6.1 Computation of Elements in the Center

Proposition 3.6.2 provides moreover a means to determine elements in the center up to any degree bound. One takes a polynomial f with indeterminate coefficients, then a necessary and sufficient condition for $f \in \mathrm{cen}(S)$ is that f must commute with all variables X_i, $i = 1, \ldots, n$. This gives a system of linear equations for the coefficients of f. Solving it answers the question if for some values of the coefficients $f \in \mathrm{cen}(S)$.

Proposition 3.6.4 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Assume $\mathbf{R}$ is computable and the term order is decidable. Let $X = \{X_1, \ldots, X_n\}$.*

Given a finite set of terms $T' = \{t_1, \ldots, t_k\}$ $k \in \mathbf{N}$ in $T(X_1, \ldots, X_n)$, then there is an algorithm, which decides if there is a polynomial

$$f = \sum_{i=1}^{k} a_i t_i \ \in \ \mathrm{cen}(S)$$

for some $a_i \in \mathbf{R}$, $1 \leq i \leq k$. Moreover the algorithm computes a $\mathbf{K}$-vector space basis of

$$\mathrm{cen}(S) \cap \mathbf{K}[t_1, \ldots, t_k].$$

Proof: Consider S as a $\mathbf{R}$-module $\mathbf{R}[X_1, \ldots, X_n]$. Let $f \in S$, then by proposition 3.6.2 $f \in \mathrm{cen}(S) \Longleftrightarrow f \in \mathrm{cen}_S(X)$. Furthermore $f \in \mathrm{cen}_S(X) \Longleftrightarrow [f, X_j] = f * X_j - X_j * f = 0$ for $1 \leq j \leq n$. By proposition 3.2.5 $f * X_j - X_j * f = h_j \in S$. Since the terms form a $\mathbf{R}$-basis of the $\mathbf{R}$-module S, $h_j = 0$ if and only if all coefficients of the terms in h_j vanish. This gives a system of linear equations for the coefficients of f.

$$\begin{aligned} [f, X_j] &= f * X_j - X_j * f \\ &= (\sum_{i=1}^{k} a_i t_i) * X_j - X_j * (\sum_{i=1}^{k} a_i t_i) \end{aligned}$$

$$\begin{aligned} &= \sum_{i=1}^{k} a_i(t_i * X_j - X_j * t_i) \\ &= \sum_{i=1}^{k} a_i(h_{ij}) \\ &= \sum_{i=1}^{k} a_i(\sum_{l=1}^{k_{ij}} b_{ijl} t_{ijl}) \\ &= \sum_{l=1}^{k_{ij}} (\sum_{i=1}^{k} a_i b_{ijl}) t_{ijl}. \end{aligned}$$

This yields a system of homogeneous linear equations for the a_i

$$\sum_{i=1}^{k} a_i b_{ijl} = 0 \qquad 1 \leq l \leq k_{ij}, 1 \leq i \leq k, 1 \leq j \leq n.$$

If this system is solvable in the a_i $1 \leq i \leq k$ then $f = \sum_{i=1}^{k} a_i t_i \in \mathrm{cen}_S(X) = \mathrm{cen}(S)$. Moreover let $M = \{(a'_{1m}, \ldots, a'_{km}) : 1 \leq m \leq m'\}$ be a basis of the solution space. Let $f_m = \sum_{i=1}^{k} a'_{im} t_i$ for $1 \leq m \leq m'$, then all linear combinations of the f_m are again in the center of S. Furthermore any polynomial in the terms T' in the center satisfies the above homogeneous system of linear equations and so it is a linear combination of the f_m. □

Proposition 3.6.5 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Assume $\mathbf{R}$ is computable and the term order is decidable.*

There exists a (non-terminating) procedure to compute a set of polynomials which generate the center of S.

Proof: Let $X = \{X_1, \ldots, X_n\}$ and let $\{T_i\}_{i \in \mathbf{N}}$ be an enumeration of the set of subsets of the terms $T(X)$. Then for $i = 0, 1, 2, 3, \ldots$ determine the set of center polynomials $P_i = \{f_{ij} \ : \ 1 \leq j \leq k_i\}$ by the algorithm in proposition 3.6.4. Then $P = \bigcup_{i \in \mathbf{N}} P_i$ is a set of generating polynomials in the center of S. □

If there are known bounds on the degrees of generating polynomials one may compute only elements in the center up to this bound and the terminate the algorithm. So without such information this is a non-terminating procedure.

3.6.2 Structure of the Center

We are going to show that non-commuting variables have only a trivial centralizer (i.e. the centralizer of these non-commuting variables is equal to $\mathbf{R}$ in case $\mathrm{char}(\mathbf{R}) = 0$). Therefore we need to prepare some technical lemmas. Note that we additionally assume $c_{ij} = 1$ in some cases.

Lemma 3.6.6 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$.*

Let $x, y \in X$ such that $x < y$ and $y * x = xy + p$ with $xy > p \in S$. Then for $0 \leq m \in \mathbf{N}$ and $1 \leq \ell \in \mathbf{N}$ the following identities hold:

$$[x^\ell, x^m y] = [x^{\ell-1}, x^{m+1} y] - x^m * p * x^{\ell-1}$$

and

$$[xy^m, y^\ell] = [xy^{m+1}, y^{\ell-1}] - y^{\ell-1} * p * y^m.$$

Proof: A short computation yields:

$$\begin{aligned}
[x^\ell, x^m y] &= x^\ell (x^m y) - (x^m y) * x^\ell \\
&= x^{\ell-1}(x^{m+1} y) - x^m (y * x) * x^{\ell-1} \\
&= x^{\ell-1}(x^{m+1} y) - x^m (xy + p) * x^{\ell-1} \\
&= x^{\ell-1}(x^{m+1} y) - (x^{m+1} y) * x^{\ell-1} - x^m * p * x^{\ell-1} \\
&= [x^{\ell-1}, x^{m+1} y] - x^m * p * x^{\ell-a}.
\end{aligned}$$

The second identity is proved similarly. □

Lemma 3.6.7 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$.*

Let $x, y \in X$ such that $x < y$ and $y * x = xy + p$ with $xy > p \in S$. Then for $0 \leq m \in \mathbf{N}$ and $1 \leq \ell \in \mathbf{N}$ the following identities hold:

$$[x^\ell, x^m y] = -\sum_{k=0}^{\ell-1} x^{m+k} * p * x^{\ell-k-1}$$

and

$$[xy^m, y^\ell] = -\sum_{k=0}^{\ell-1} y^{\ell-k-1} * p * y^{m+k}.$$

Proof: By induction on ℓ. We get for the case $\ell = 1$:

$$\begin{aligned}
[x, x^m y] &= [x^0, x^{m+1} y] - x^m * p * x^0 \\
&= -x^m * p
\end{aligned}$$

using the preceding lemma and by the formula

$$\begin{aligned}
[x, x^m y] &= -\sum_{k=0}^{0} x^{m+k} * p * x^{1-k-1} \\
&= -x^m * p * x^0 = -x^m * p
\end{aligned}$$

as claimed. In case $\ell > 1$ a short computation using the preceding lemma and the induction hypothesis establishes:

$$\begin{aligned}
[x^{\ell+1}, x^m y] &= [x^\ell, x^{m+1}y] - x^m * p * x^\ell \\
&= -\sum_{k=0}^{\ell-1} x^{m+1+k} * p * x^{\ell-k-1} - x^m * p * x^\ell \\
&= -\sum_{k=1}^{\ell} x^{m+k} * p * x^{\ell-k} - x^m * p * x^\ell \\
&= -\sum_{k=0}^{\ell} x^{m+k} * p * x^{\ell-k}.
\end{aligned}$$

The second identity is proved similarly. □

Corollary 3.6.8 *For the case $m = 0$ we note*

$$[x^\ell, y] = -\sum_{k=0}^{\ell-1} x^k * p * x^{\ell-k-1}$$

and

$$[x, y^\ell] = -\sum_{k=0}^{\ell-1} y^{\ell-k-1} * p * y^k.$$

Lemma 3.6.9 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$.*

Let $x, y \in X$ such that $x < y$ and $y * x = xy + p$ with $xy > p \in S$. Then for $1 \leq \ell \in \mathbf{N}$ the following holds:

$$\mathrm{HM}([x^\ell, y]) = -\ell \mathrm{HM}(p * x^{\ell-1})$$

and

$$\mathrm{HM}([x, y^\ell]) = -\ell \mathrm{HM}(y^{\ell-1} * p).$$

Proof: A short computation yields:

$$\begin{aligned}
\mathrm{HM}([x^\ell, y]) &= \mathrm{HM}(-\sum_{k=0}^{\ell-1} x^k * p * x^{\ell-k-1}) \\
&= \mathrm{HM}(-\sum_{k=0}^{\ell-1} \mathrm{HM}(x^k * p * x^{\ell-k-1})) \\
&= \mathrm{HM}(-\sum_{k=0}^{\ell-1} \mathrm{HM}(px^{\ell-1})) \\
&= \mathrm{HM}(-\ell \mathrm{HM}(px^{\ell-1})) \\
&= -\ell \mathrm{HM}(px^{\ell-1})
\end{aligned}$$

where we used the above corollary and the fact, that the multiplication of head terms behaves like commutative multiplication of head terms. The second identity is proved similarly. □

Lemma 3.6.10 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$.*

Let $x, y \in X$ such that $x < y$ and $y * x = xy + p$ with $xy > p \in S$. If $p \neq 0$ and $\mathrm{char}(\mathbf{R}) = 0$, then for $1 \leq \ell, m \in \mathbf{N}$ with $\ell \neq m$ the following holds:

$$\mathrm{HM}([x^\ell, y]) \neq \mathrm{HM}([x^m, y])$$

and

$$\mathrm{HM}([x, y^\ell]) \neq \mathrm{HM}([x, y^m]).$$

Proof: Since ℓ and m are not equal to zero in $\mathbf{R}$ we have

$$\mathrm{HM}([x^\ell, y]) = -\ell \mathrm{HM}(p * x^{\ell-1}) \neq -m\mathrm{HM}(p * x^{m-1}) = \mathrm{HM}([x^m, y]).$$

The second identity is proved similarly. □

Proposition 3.6.11 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$.*

Let $x, y \in X$ such that $x < y$ and $y * x = xy + p$ with $xy > p \in S$. If $p \neq 0$ and $\mathrm{char}(\mathbf{R}) = 0$, then the following holds:

$$\mathrm{cen}(S) \cap \mathbf{R}[x, y] = \mathbf{R}.$$

Note that this does not necessarily imply that $\mathrm{cen}(S) = \mathbf{R}$. E.g. for any variable $z \in X$, $z \neq x, y$, which commutes with all other variables we have $\mathbf{R}[z] \subseteq \mathrm{cen}(S)$ by proposition 3.6.2.

Proof: Assume $f \in \mathrm{cen}(S) \cap \mathbf{R}[x, y]$ with $x < y$. Let $f = \sum_{k=1}^{k_f} \alpha_k x^{e_k} y^{a_k}$ with $\alpha_k \in \mathbf{R}$ and $e_k, a_k \in \mathbf{N}$. Since $f \in \mathrm{cen}(S)$, we must have $[f, x] = [f, y] = 0$. Expanding $[f, y]$ and $[f, x]$ we obtain

$$\begin{aligned}
0 = [f, y] &= [\sum_{k=1}^{k_f} \alpha_k x^{e_k} y^{a_k}, y] \\
&= \sum_{k=1}^{k_f} \alpha_k [x^{e_k} y^{a_k}, y] = \sum_{k=1}^{k_f} \alpha_k [x^{e_k}, y] y^{a_k} \\
&= \sum_{k=1}^{k_f} \alpha_k (-e_k \mathrm{HM}(p * x^{e_k - 1}) + \mathrm{rest}) y^{a_k} \\
&= \sum_{k=1}^{k_f} (\alpha_k (-e_k) \mathrm{HM}(p * x^{e_k - 1}) * y^{a_k} + \alpha_k \ \mathrm{rest} \ * y^{a_k}), \\
0 = [f, x] &= [\sum_{k=1}^{k_f} \alpha_k x^{e_k} y^{a_k}, x]
\end{aligned}$$

$$\begin{aligned} &= \sum_{k=1}^{k_f} \alpha_k [x^{e_k} y^{a_k}, x] = \sum_{k=1}^{k_f} \alpha_k x^{e_k} [y^{a_k}, x] \\ &= \sum_{k=1}^{k_f} \alpha_k x^{e_k} (-a_k \mathrm{HM}(y^{a_k - 1} * p) + \mathrm{rest}) \\ &= \sum_{k=1}^{k_f} (\alpha_k (-a_k) x^{e_k} * \mathrm{HM}(y^{a_k - 1} * p) + \alpha_k x^{e_k} * \ \mathrm{rest}\ ). \end{aligned}$$

Consider S as a $\mathbf{R}$-module $\mathbf{R}[X_1, \ldots, X_n]$. Then the two expansions define a system of k_f homogeneous equations for the α_k. By assumption only $e_0 = a_0 = 0$ and for $k > 0$ not both $e_k = 0$ and $a_k = 0$. Since $\mathrm{char}(\mathbf{R}) = 0$ we have $e_k \neq 0$ or $a_k \neq 0$ in $\mathbf{R}$ for $1 \leq k \leq k_f$ and $e_k \neq 0$ respectively $a_k \neq 0$ in $\mathbf{N}$. In case $e_k, e_j \neq 0$ we have $-e_k \mathrm{HM}(p * x^{e_k - 1} * y^{a_k}) \neq -e_j \mathrm{HM}(p * x^{e_j - 1} * y^{a_j})$ for $1 \leq k \neq j \leq k_f$. And in case $a_k, a_j \neq 0$ we have $-a_k \mathrm{HM}(x^{e_k} * y^{a_k - 1} * p) \neq -a_j \mathrm{HM}(x^{e_j} * y^{a_j - 1} * p)$ for $1 \leq k \neq j \leq k_f$. Comparing the coefficients of the highest terms of the products (where $e_k \neq 0$ or $a_k \neq 0$), we see that we must have $\alpha_k = 0$ for $k = k_f, k_f - 1, \ldots, 1$ and α_0 arbitrary. That is $f = \alpha_1 x^0 y^0$, which shows that actually $f \in \mathbf{R}$ as claimed. □

Proposition 3.6.12 *Let $S = \mathbf{R}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over $\mathbf{R}$ in the variables $X_1, \ldots, X_n$. Let $X = \{X_1, \ldots, X_n\}$.*

Let $x, y \in X$ such that $x < y$ and $y * x = xy + p$ with $xy > p \in S$. Let $\mathbf{R}[x, y]_d = \{f \in \mathbf{R}[x, y] : \deg(f) \leq d\}$. If $p \neq 0$, $\mathrm{char}(\mathbf{R}) = q > 0$ and $0 \leq d < q$, then the following holds:

$$\mathrm{cen}(S) \cap \mathbf{R}[x, y]_d = \mathbf{R}.$$

Proof: In this case we have $e_k \leq d$ for $1 \leq k \leq k_f$ and so $e_k \neq 0$ in $\mathbf{R}$. As in the proof of the preceding proposition we can now conclude, that the system of k_f equations has rank $k - 1$ and therefore has only one solution such that $f \in \mathbf{R}$. □

Remark: In case $d \geq q = \mathrm{char}(\mathbf{R})$ it may happen that

$$\mathrm{cen}(S) \cap \mathbf{R}[x, y]_d \supsetneq \mathbf{R}.$$

Example 3.6.13 *Let $S = \mathbf{K}_2\{X, Y; Q\}$ be a solvable polynomial ring over a field $\mathbf{K}_2$ of characteristic 2 in the variables X, Y. Let $X < Y$ and $Y * X = XY + 1$ with $1 \in \mathbf{K}_2$.*

Let $f = Y^2 \in \mathbf{K}_2[X, Y]_2$, then clearly $f \in \mathrm{cen}_S(Y)$ and $f \in \mathrm{cen}_S(X)$ since $Y^2 * X = Y * (XY + 1) = (XY + 1)Y + Y1 = XY^2 + Y + Y = XY^2$.

This shows that $f \in \mathrm{cen}(S) \cap \mathbf{K}_2[X, Y]_2$ and $f \notin \mathbf{K}$.

Chapter 4

Ideals and Gröbner Bases

In this chapter we will discuss the main part of Gröbner bases theory for solvable polynomial rings.

First three sections treat abstract reduction relations, left reduction for solvable polynomial rings and some general properties of confluent left reduction relations. Then we introduce standard representations and apply them to left reduction relations and to the left ideal membership problem. Using standard representations we prove that the second Buchberger criterion for the detection of unnecessary S-polynomials holds for solvable polynomial rings. Then we define left Gröbner bases, give several characterizations of them and show that there exists a Buchberger algorithm to construct them. In the last sections we discuss right and two-sided ideals and Gröbner bases. We give conditions on the coefficient field under which the algorithmic construction of two-sided Gröbner bases is possible.

Throughout this chapter let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ denote a solvable polynomial ring over a skew field $\mathbf{K}$ with respect to a fixed but arbitrary admissible term order $<$. Q and Q' denote the commutator relations as defined in the axioms 3.2.1. T denotes the set of terms in the variables $X_1, \ldots, X_n$ and $\mathbf{K}^* = \mathbf{K} \setminus \{0\}$. In the algorithms we assume that $\mathbf{K}$ is computable and $<$ is decidable.

4.1 Reduction Relations

In this first section we summarize some important notations and definitions of reduction relations. In this section R may be any set, but we will later only use the definitions in case R is a ring.

Definition 4.1.1 *Let $\longrightarrow$ be a relation on R, (i.e. $\longrightarrow \subseteq R \times R$) then $\longrightarrow$ is called a* reduction relation *if it is a strictly anti-symmetric relation. That means, $(a,a) \notin \longrightarrow$ for all $a \in R$ and if for some $a, b \in R$ $(a,b) \in \longrightarrow$, then $(b,a) \notin \longrightarrow$. Furthermore an element $a \in R$ is called* irreducible *if for all $b \in R$ $(a,b) \notin \longrightarrow$.*

Definition 4.1.2 *Let $\longrightarrow$ be a reduction relation on R. Then $\longrightarrow$ is called* Noetherian *if there does not exist an infinite reduction sequence:*

$$a_1 \longrightarrow a_2 \longrightarrow a_3 \longrightarrow \ldots$$

for $a_i \in R$, $i = 1, 2, 3, \ldots$.

Definition 4.1.3 *Let $\longrightarrow$ be a reduction relation on R, $f, g, h \in R$.*

$\longleftarrow$ *denotes the inverse relation of $\longrightarrow$.*

$\longleftrightarrow$ *denotes the symmetric closure of $\longrightarrow$.*

$\longrightarrow^*$ *denotes the reflexive, transitive closure of $\longrightarrow$. If for some $n \in \mathbf{N}$ $f \longrightarrow^* g$ is equal to $f = f_1 \longrightarrow \ldots \longrightarrow f_n = g$ we write $f \longrightarrow^n g$.*

$\longleftrightarrow^*$ *denotes the reflexive, transitive closure of the symmetric closure of $\longrightarrow$. If for some $n \in \mathbf{N}$ $f \longleftrightarrow^* g$ is equal to $f \longleftrightarrow f_0 \longleftrightarrow \ldots \longleftrightarrow f_n = g$ we write $f \longleftrightarrow^n g$.*

$f \downarrow g$ *denotes that f and g reduce to a common element, that is there exists h with $f \longrightarrow^* h$ and $g \longrightarrow^* h$. In this case $f \longleftrightarrow^* g$.*

Reduction relations are in general not confluent; this means that two different reductions of the same element may lead to two different irreducible elements.

Definition 4.1.4 *Let $\longrightarrow$ be a reduction relation on R, $a, b, c, d \in R$. Then*

1. *$\longrightarrow$ is* confluent *if $a \longrightarrow^* c$ and $a \longrightarrow^* d$ implies $c \downarrow d$,*
2. *$\longrightarrow$ is* locally confluent *if $a \longrightarrow c$ and $a \longrightarrow d$ implies $c \downarrow d$,*
3. *$\longrightarrow$ has the* Church-Rosser property *if $a \longleftrightarrow^* b$ implies $a \downarrow b$.*
4. *$\longrightarrow$ has the* unique normal forms *if $a \longrightarrow^* b$, $a \longrightarrow^* c$ and b, c are irreducible implies $b = c$.*

Lemma 4.1.5 (Newman) *Let $\longrightarrow$ be a* Noetherian *reduction relation on R, then the properties 1, 2, 3 and 4 of definition 4.1.4 are equivalent.*

Proof: See [Bergman 1978], [Huet 1980]. □

4.2 Left Reduction

In this section we will define left reduction relations on a solvable polynomial ring R. In a later section we discuss also right reduction relations.

Definition 4.2.1 (Left Reduction) *Let $p \in R$, $t \in T$. Then the* left reduction $\longrightarrow_{t,p} \subseteq R \times R$ *is defined as follows:*

> *For $f, f' \in R$, $t \in T(f)$, $f \longrightarrow_{t,p} f'$ iff there exists $u \in T$ such that $t = u \cdot \mathrm{HT}(p) = \mathrm{HT}(u * p)$ and*
>
> $$f' = f - a_u * u * p,$$
>
> *where $a_u \in \mathbf{K}^*$ is the unique element of $\mathbf{K}^*$ such that $\mathrm{coeff}(t, f) = a_u * \mathrm{coeff}(t, u * p)$.*

By construction $t \notin T(f')$. If for certain f, t no such u exists, then t in $T(f)$ is called irreducible wrt. p.

This definition requires that

1. $\mathrm{HT}(p)$ divides t in the commutative sense and
2. the head term of $u * p$ is equal to t.

Now (1) is constructive by comparing exponents of powers of X_i in t and in $\mathrm{HT}(p)$ (which also determines u) and (2) holds by proposition 3.2.5.

For a completion procedure with respect to this reduction relation, the following lemma is required.

Lemma 4.2.2 *Let $p \in R$, $u \in T$, $a \in \mathbf{K}^*$ and let $t = \mathrm{HT}(u * p)$. Then $a * u * p \longrightarrow_{t,p} 0$.*

Proof: By proposition 3.2.5 we have $a * u * p = cup + h$ with $t = \mathrm{HT}(up) = u\mathrm{HT}(p)$. Let $a_u = a$ then $\mathrm{coeff}(t, a * u * p) = a_u * \mathrm{coeff}(t, u * p)$. So $cup + h - (a_u * u * p) = 0$ as claimed. □

Definition 4.2.3 *Reduction with respect to a polynomial $p \in R$ and with respect to sets of polynomials $P \subseteq R$ are defined as follows:*

$f \longrightarrow_p f'$ if $f \longrightarrow_{t,p} f'$ for some t in $T(f)$,

$f \longrightarrow_{t,P} f'$ if for some $p \in P$, $f \longrightarrow_{t,p} f'$,

$f \longrightarrow_P f'$ if for some $p \in P$, $f \longrightarrow_p f'$.

For sets $P, Q \subseteq R$ we define

$$P \longrightarrow Q \text{ if for some } f \in P,\ f' \in Q,\ P \setminus \{f\} = Q \setminus \{f'\} \text{ and } f \longrightarrow_{P\setminus\{f\}} f'.$$

We will also use the notations form 4.1.3 for the left reduction.

If f can not be reduced with respect to P we say f is irreducible with respect to P or f is in normal form with respect to P. P is irreducible or in normal form or *autoreduced*, if all $f \in P$ are irreducible with respect to $P \setminus \{f\}$. So if P is autoreduced and we have $P \longrightarrow^* Q$, then $P = Q$. Furthermore we generally assume that $0 \notin P$ for a reduction relation $\longrightarrow_P$ and that only 0 is reducible with respect to the empty set.

Lemma 4.2.4 *Let $f, f' \in R$, $P \subset R$, P finite then*

1. *$f \longrightarrow_P f'$ implies $f > f'$,*
2. *$\longrightarrow_P$ is a Noetherian reduction relation.*
3. *It exists f' with $f \longrightarrow_P^* f'$ and f' is irreducible with respect to P. f' is called a (not necessarily unique)* normal form *of f with respect to P.*

Proof: (1) Let $f \longrightarrow_P f'$, then $f \longrightarrow_{t,p} f'$ for some $t \in T$ and some $p \in P$. Then by definition 4.2.1 $t \notin T(f')$. Furthermore for all $s \in T(f)$ with $s > t$ we have $s \in T(f')$ and by the product lemma 3.2.5 all new terms in f' are $< t$. By definition of the quasi-order $<$ on R: $f > f'$.

(2) If $f \longrightarrow_P f'$, then by (1) $f > f'$ and since $<$ is a well-founded quasi-order on R, the claim follows.

(3) Let $f \longrightarrow_P^* f'$ be a maximal reduction sequence. Then by (2) this sequence is finite, say of length n: $f \longrightarrow_P f_1 \longrightarrow_P \ldots \longrightarrow_P f_n$ then f_n is irreducible mod P. □

The following two important lemmas deal with properties of polynomials under reductions.

Lemma 4.2.5 (Translation Lemma) *Let $f, g, h, f', g', h' \in R$ and let $P \subset R$. If $f = g + h$ and $h \longrightarrow_P^* h'$ then there exist f' and g' such that $f \longrightarrow_P^* f'$, $g \longrightarrow_P^* g'$ and $f' = g' + h'$.*

Proof: Let $h \longrightarrow_P^* h'$ be equal to $h \longrightarrow_P^k h'$ for some $k \in \mathbf{N}$. The proof is by induction on k. For $k = 0$ let $f' = f$ and $g' = g$.

For $k > 0$ let $h \longrightarrow_P^k h'$ be equal to $h \longrightarrow_P^{k-1} h'' \longrightarrow_{t,P} h'$. For some $t \in T(h'')$ and $p \in P$. By induction assumption there exist polynomials f'', g'' with $f \longrightarrow_P^{k-1} f''$, $g \longrightarrow_P^{k-1} g''$ such that $f'' = g'' + h''$.

Let $h' = h'' - c * u * p$ for some $u \in T$ and some $c \in \mathbf{K}^*$ with $t = \mathrm{HT}(u * p) = \mathrm{HT}(up)$ and $\mathrm{coeff}(t, h'') = c * \mathrm{coeff}(t, u * p)$. Let $c_1, c_2 \in \mathbf{K}$ such that $\mathrm{coeff}(t, f'') = c_1 * \mathrm{coeff}(t, u * p)$

and $\text{coeff}(t, g'') = c_2 * \text{coeff}(t, u * p)$ (possibly $c_1 = 0$ or $c_2 = 0$). Let $f' = f'' - c_1 * u * p$, $g' = g'' - c_2 * u * p$. This defines two reductions $f'' \longrightarrow^*_{t,P} f'$ and $g'' \longrightarrow^*_{t,P} g'$.

Since $f'' = g'' + h''$ we have $c_1 = c_2 + c$ and so $f' = g' + h'$. By construction and induction assumption $f \longrightarrow^{k-1}_P f'' \longrightarrow^*_{t,P} f'$ and $g \longrightarrow^{k-1}_P g'' \longrightarrow^*_{t,P} g'$, which proves the lemma. □

For the special case $h' = 0$ we have $f' = g'$, i.e. $f \downarrow_P g$:

Lemma 4.2.6 *Let $f, g \in R$ and let $P \subset R$. If $f - g \longrightarrow^*_P 0$ then $f \downarrow_P g$.*

4.3 Confluent Left Reduction

We summarize some useful properties of confluent (Noetherian) reduction relations.

Given a subset $G \subset R$ such that $\longrightarrow_G$ is confluent, we show, that there exists minimal subsets $G' \subset G$ such that $\longrightarrow_{G'}$ is confluent. Furthermore there exist autoreduced (or irreducible) subsets G, such that $\longrightarrow_G$ is confluent. Finally we treat reduction relations which are confluent on certain subsets $F(t)$ of R.

Lemma 4.3.1 *Let $G \subset R$ such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. Let $f, g \in R$ with $f \longleftrightarrow^*_G g$ and let g be irreducible wrt. G. Then $f \longrightarrow^*_G g$. In particular for $g = 0$ we have that $f \longleftrightarrow^*_G 0$ implies $f \longrightarrow^*_G 0$.*

Proof: Since $\longrightarrow_G$ is confluent, there exists $h \in R$ such that $f \longrightarrow^*_G h$ and $g \longrightarrow^*_G h$. But g is irreducible, so $g = h$ which proves the first claim of the lemma. Since 0 is irreducible the second claim is also true. □

Next we discuss minimal sets for confluent reduction relations.

Lemma 4.3.2 *Let $G \subset R$ such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. If there exist $f \in G$, $h \in R$, $G' = G \setminus \{f\}$, $t = \text{HT}(f)$ with $f \longrightarrow_{t,G'} h$, then also $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation and $G \longrightarrow^* G'$.*

Proof: Clearly $\longrightarrow_{G'}$ is a Noetherian reduction relation.

We show that $\longrightarrow_{G'}$ has unique normal forms; then by lemma 4.1.5 $\longrightarrow_{G'}$ is confluent. Let $g, g_1, g_2 \in R$ such that $g \longrightarrow^*_{G'} g_1$, $g \longrightarrow^*_{G'} g_2$ and g_1, g_2 are irreducible with respect to G'. By the confluence of $\longrightarrow_G$ there exists $q \in R$ such that $g_1 \longrightarrow^*_G q$ and $g_2 \longrightarrow^*_G q$. Now by definition of G', g_1 and g_2 are also irreducible with respect to G. So $g_1 = q = g_2$ which shows the confluence of $\longrightarrow_{G'}$. Since $f \longrightarrow_G 0$ we have $f \longrightarrow_G h \longrightarrow^*_G 0$. Then by definition of G' also $f \longrightarrow_{G'} h \longrightarrow^*_{G'} 0$ which proves $G \longrightarrow^*_{G'} G'$. □

Lemma 4.3.3 *Let $G \subset R$ be finite, such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. Let $G = G' \cup G''$ such that $G' \cap G'' = \emptyset$. If for any $f \in G''$, there exists $h \in R$, $t = \text{HT}(f)$ with $f \longrightarrow_{t,G'} h$, then also $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation and $G \longrightarrow^* G'$.*

Proof: We show by induction on the number of elements of G'', that G' is also a confluent Noetherian reduction relation. If $G'' = \emptyset$, then $G' = G$ and we are done. Let $f \in G''$, $G''' = G'' \setminus \{f\}$. By assumption there exist, $h \in R$, $t = \mathrm{HT}(f)$ such that $f \longrightarrow_{t,G'} h$. Now by lemma 4.3.2 $G' \cup G'''$ is still a confluent Noetherian reduction relation and by induction assumption on $G' \cup G'''$, G' is a confluent Noetherian reduction relation. □

An immediate consequence is:

Lemma 4.3.4 *Let $G \subset R$, G finite, such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. There exists $G' \subseteq G$, $|G'|$ minimal, such that $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation and $G \longrightarrow^* G'$.*

Proof: Let $G' \subseteq G$ with $|G'|$ minimal such that for all $f \in G \setminus G'$, there exists $h \in R$, $t = \mathrm{HT}(f)$ with $f \longrightarrow_{t,G'} h$. Then G' and $G'' = G \setminus G'$ satisfy the assumptions of lemma 4.3.3 and so $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation. □

The next lemma treats reduced polynomials and autoreduced sets.

Lemma 4.3.5 *Let $G \subset R$, G finite, such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. Let $g, h \in G$, $G'' = G \setminus \{g\}$, $h \neq g$ and $t \in T(g)$ such that*

$$g \longrightarrow_{t,h} g'.$$

If $g' = 0$ then let $G' = G''$ otherwise let $G' = G'' \cup \{g'\}$. Then $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation and $G \longrightarrow^* G'$.

Proof: The fact that $\longrightarrow_{G'}$ is a Noetherian reduction relation is clear.

We show that $\longrightarrow_{G'}$ has unique normal forms, then by lemma 4.1.5 $\longrightarrow_{G'}$ is confluent. Let $g, g_1, g_2 \in R$ such that $g \longrightarrow^*_{G'} g_1$, $g \longrightarrow^*_{G'} g_2$ and g_1, g_2 are irreducible with respect to G'. By the confluence of $\longrightarrow_G$ there exists $q \in R$ such that $g_1 \longrightarrow^*_G q$ and $g_2 \longrightarrow^*_G q$. Now g_1 and g_2 are also irreducible with respect to G, since otherwise g_1 and g_2 would also be reducible with respect to G'. So $g_1 = q = g_2$, which proves the lemma. □

Proposition 4.3.6 *Let $G \subset R$, G finite, such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. Then there exists a autoreduced set G' such that $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation and $G \longrightarrow^* G'$.*

Proof: By lemma 4.3.4 there exists a minimal set $G'' \subseteq G$ such that $G \longrightarrow^* G''$ and $\longrightarrow_{G''}$ is a confluent Noetherian reduction relation. Then by lemma 4.3.5 there exists a autoreduced set G' with $G'' \longrightarrow^* G'$ such that $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation. □

The uniqueness of such sets under the condition that G is also monic for left ideals generated by G is shown in lemma 5.1.2 in chapter 5.

Next we state a lemma on 'partially' confluent reduction relations.

Lemma 4.3.7 *Let $G \subset R$ such that $\longrightarrow_G$ is a confluent Noetherian reduction relation on $F(t) = \{h \in R \mid h < t\}$ for fixed $t \in T$. Let $h_1 \in F(t)$, $h, h_2 \in R$ with $h = h_1 + h_2$. If $h_1 \longrightarrow_G^* 0$ and $h_2 \longrightarrow_G^* 0$ then $h \longrightarrow_G^* 0$.*

Proof: Since $h_2 \longrightarrow_G^* 0$, by lemma 4.2.6 $h \downarrow_G h_1$. I. e. there exists $h_3 \in R$ such that $h \longrightarrow_G^* h_3$ and $h_1 \longrightarrow_G^* h_3$. By the confluence of $\longrightarrow_G$ on $F(t)$ and the fact that $h_1 \in F(t)$ there exists $h_4 \in R$ such that $h_3 \longrightarrow_G^* h_4$ and $0 \longrightarrow_G^* h_4$. So $h_4 = 0$ and consequently $h \longrightarrow_G^* 0$. □

4.4 Reductions and Ideal Membership

Let $\text{ideal}_l(P)$ denote the left ideal generated by $P \subseteq R$. It will be shown that reductions with respect to P do not lead outside of left ideals. And if the difference of two polynomials is in the ideal, then there exists back and forth reductions between these two polynomials.

Definition 4.4.1 *Let $I = \text{ideal}_l(P)$ be a left ideal in R, generated by a finite subset P of R. Then any $f \in I$ has a* left representation *(with respect to P):*

$$f = \sum_{p \in P} h_p * p = \sum_{i=1}^{k} c_i s_i * p_i,$$

where $h_p \in R$, $c_i \in \mathbf{K}^*$, $s_i \in T$ and $p_i \in P$ for $1 \leq i \leq k$.

Precisely we should write $c_i * s_i * p_i$ but by axiom 3.2.1(2) we have $c_i * s_i = c_i s_i$. Note, that the p_i are not necessarily distinct. The representation is obtained from the definition of elements in the left ideal by writing the left factor polynomials as sums of terms.

Lemma 4.4.2 *Let $f, g \in R$, $P \subset R$, P finite. If $f \longleftrightarrow_P^* g$ then $f - g \in \text{ideal}_l(P)$. In particular if $f \longrightarrow_P^* 0$ then $f \in \text{ideal}_l(P)$.*

Proof: Let $f \longleftrightarrow_P^* g$ be equal to $f \longleftrightarrow_P^k g$ for some $k \in \mathbf{N}$. The proof is by induction on k. For $k = 0$, $g = f$ and $f - g = 0 \in \text{ideal}_l(P)$.

For $k > 0$ let $f \longleftrightarrow_P^k g$ be equal to $f \longleftrightarrow_P^{k-1} f_{k-1} \longleftrightarrow_P f_k = g$. By induction assumption $f - f_{k-1} \in \text{ideal}_l(P)$. Now $f_{k-1} \longrightarrow_{t,p} g$ or $g \longrightarrow_{t,p} f_{k-1}$ for some $p \in P$. Thus $g = f_{k-1} - a * u * p$ or $f_{k-1} = g - a * u * p$ for some $a \in \mathbf{K}^*$ and some $t, u \in T$. In both cases $f_{k-1} - g = \pm a * u * p \in \text{ideal}_l(P)$. In combination with the induction assumption $f - g = (f - f_{k-1}) + (f_{k-1} - g) \in \text{ideal}_l(P)$ which proves the lemma. □

Lemma 4.4.3 *Let $P, Q \subset R$, P, Q finite, such that $P \longrightarrow^* Q$, then* $\text{ideal}_l(P) = \text{ideal}_l(Q)$.

Proof: Let $P \longrightarrow^* Q$ be equal to $P \longrightarrow^k Q$ for some $k \in \mathbf{N}$. The proof is by induction on k. For $k = 0$, $P = Q$ and $\mathrm{ideal}_l(P) = \mathrm{ideal}_l(Q)$.

For $k > 0$ let $P \longrightarrow^k Q$ be equal to $P \longrightarrow^{k-1} P' \longrightarrow Q$. By induction assumption $\mathrm{ideal}_l(P) = \mathrm{ideal}_l(P')$. Now from $P' \longrightarrow Q$ there exists $f \in P'$, $f' \in Q$, $P' \setminus \{f\} = Q \setminus \{f'\}$ such that $f \longrightarrow_{P' \setminus \{f\}} f'$. By this we have $f' = f - au * p$ for some $p \in P'$ and $p \in Q$. This shows that $f' \in \mathrm{ideal}_l(P')$ and also $f = f' + au * p \in \mathrm{ideal}_l(Q)$. So $\mathrm{ideal}_l(P') = \mathrm{ideal}_l(Q)$ which together with the induction assumption proves the lemma. □

Lemma 4.4.4 *Let $G \subset R$ such that $\longrightarrow_G$ is a confluent Noetherian reduction relation. If there exist $f \in G$, $h \in R$, $G' = G \setminus \{f\}$, $t = \mathrm{HT}(f)$ with $f \longrightarrow_{t,G'} h$. Then* $\mathrm{ideal}_l(G) = \mathrm{ideal}_l(G')$.

Proof: Let f, G, G' as in the assumptions of the lemma. Then $f \longrightarrow_G^* 0$ since $f \in G$, furthermore $\longrightarrow_{G'}$ is a confluent Noetherian reduction relation by 4.3.2. So we have also $f \longrightarrow_{G'}^* 0$, which shows $f \in \mathrm{ideal}_l(G')$ by lemma 4.4.2. This shows $\mathrm{ideal}_l(G) \subseteq \mathrm{ideal}_l(G')$, the reverse inclusion follows since $G' \subseteq G$. □

Lemma 4.4.5 *Let P be a finite subset of R. For all $f, g \in R$, if $f - g \in \mathrm{ideal}_l(P)$ then $f \longleftrightarrow_P^* g$.*

Proof: If $f - g \in \mathrm{ideal}_l(P)$ then by definition $f - g = \sum_{i=1}^{k} c_i s_i * p_i$, where $c_i \in \mathbf{K}^*$, $s_i \in T$ and $p_i \in P$ for $1 \leq i \leq k$.

We prove $f \longleftrightarrow_P^* g$ by induction on k. For $k = 0$, $f = g$ and the claim is trivial. For $k > 0$ let

$$f - g' = f - (g + \sum_{i=1}^{k-1} c_i s_i * p_i) = c_k s_k * p_k.$$

Since $\mathrm{HT}(s_k * p_k) = s_k * \mathrm{HT}(p_k) = s_k \mathrm{HT}(p_k)$ by lemma 4.2.2 $c_k * s_k * p_k \longrightarrow_P 0$ and by lemma 4.2.6 $f \downarrow_P g'$, that is $f \longleftrightarrow_P^* g'$. Now $g' - g = \sum_{i=1}^{k-1} c_i s_i * p_i$ and by induction assumption $g' \longleftrightarrow_P^* g$. Combining both results we get $f \longleftrightarrow_P^* g$. □

For the left reduction relation there are algorithms, which compute for any element $f \in R$ its left normal form and for any finite set $F \subset R$ a autoreduced set.

Lemma 4.4.6 *Let R be a solvable polynomial ring over a computable skew field $\mathbf{K}$ with respect to a decidable term order. Then for any finite $F \subset R$ and any $f \in R$ one can compute $g \in R$ such that*

1. *$f \longrightarrow_F^* g$ and $f - g \in \mathrm{ideal}_l(F)$.*
2. *g is left irreducible modulo F.*

Algorithm: $LNF(f, F)$
Input: $f \in R$ and $F = \{f_1, \ldots, f_k\} \subseteq R$.
Output: $g \in R$ satisfying the conditions (1) and (2) of the lemma.
begin $D \leftarrow \mathrm{HT}(F)$. $g \leftarrow f$.
  while $\exists s \in D$ with $s \mid t$ for some $t \in T(g)$ **do**
    Let $p \in F$ with $\mathrm{HT}(p) = s$. Let $u \in T$ with $t = su$.
    $c \leftarrow \mathrm{coeff}(t, u * p)$.
    $g \leftarrow g - c^{-1} \cdot u * p$.
    end.
  return(g).
end LNF.

Table 4.1: Algorithm: LNF

Proof: We give an algorithm which computes g in table 4.1.

Partial correctness follows from the definition of reduction.

Termination: Let $\{g_i\}_{i=0,1,\ldots}$ be the sequence of reduction polynomials with $g_0 = g$. Let $g_{i+1} = g_i - c_i^{-1} \cdot s_i * p_i$ be an immediate reduct of g_i. Then we have $g_{i+1} < g_i$. Since $<$ is a well-founded quasi-order on R the reduction sequence must be finite $\{g_i\}_{i=0,1,\ldots,k}$. □

Lemma 4.4.7 *Let R be a solvable polynomial ring over a computable skew field* **K** *with respect to a decidable term order. Then for any finite $F \subset R$ one can compute $G \subset R$ such that*

1. $\mathrm{ideal}_l(F) = \mathrm{ideal}_L(G)$,
2. *G is autoreduced and monic.*

Proof: We give an algorithm which computes G in table 4.2.

Partial correctness follows from the fact that $\mathrm{ideal}_l(F) = \mathrm{ideal}_l(G)$ is an invariant of the **while**-loop and irreducibility of G follows by the **while**-condition.

Termination: Assume that the algorithm does not terminate. Consider the elements of G during each iteration of the loop written as rows in a scheme, where the zeroes are also kept in the respective row. Then by the **while**-condition there exist a column in the scheme with an infinite sequence of polynomials $p \longrightarrow_{G_1} \ldots \longrightarrow_{G_n} p_n \longrightarrow_{G_{n+1}} \ldots$. But this contradicts the Noetherianity of the reduction relation and so proves termination. □

4.5 Standard Representations

In this section we define representations with the property the head terms of the representing polynomials do not exceed the head term of the represented polynomial. These

Algorithm: $LIRRSET(F)$
Input: $F = \{f_1, \ldots, f_k\} \subset R$.
Output: $G \subset R$ satisfying the conditions (1) and (2) of the lemma.
begin $G \leftarrow F$.
  while $\exists p \in G$ with p is reducible wrt. $G \setminus \{p\}$ **do**
    $G \leftarrow G \setminus \{p\}$.
    $p' \leftarrow \mathrm{LNF}(p, G)$.
    if $p' \neq 0$ **then**
      $p' \leftarrow \mathrm{HC}(p')^{-1} p'$.
      $G \leftarrow G \cup \{p'\}$. **end**.
    end.
  return(G).
end $LIRRSET$.

Table 4.2: Algorithm: LIRRSET

representations are called standard representations. The fact that 'normal' representations need not be standard has been one of the major difficulties in constructive ideal theory. We discuss under which conditions a standard representation can be obtained from a representation.

Definition 4.5.1 (Standard representation) *Let $P \subset R$, $0 \neq f \in \mathrm{ideal}_l(P)$. A representation*

$$f = \sum_{i=1}^{k} c_i s_i * p_i,$$

with $c_i \in \mathbf{K}^*$, $s_i \in T$, $p_i \in P$ for all $1 \leq i \leq k$ is called a standard representation with respect to P *if for all $1 \leq i \leq k$ the following condition is satisfied:*

$$\mathrm{HT}(s_i * p_i) \leq \mathrm{HT}(f).$$

For $t \in T$ the above representation is called a t-representation with respect to P *if for all $1 \leq i \leq k$ the following condition is satisfied:*

$$\mathrm{HT}(s_i * p_i) \leq t.$$

t-representations have been discussed by [Becker 1990] for commutative polynomial rings and power series rings.

Lemma 4.5.2 *Let P be a finite subset of R, let $f \in R$ and $b \in \mathbf{K}$, $u, t \in T$.*

1. *If f has a standard representation wrt. P, then also $bu * f$ has a standard representation wrt. P.*

2. *For $p \in P$, $f * p$ has a standard representation wrt. P.*

The same holds with 'standard representation' replaced by 't-representation'.

1. *If f has a t-representation wrt. P, then also $bu * f$ has a ut-representation wrt. P.*
2. *For $p \in P$ with $\mathrm{HT}(p) \leq t$, $f * p$ has a $\mathrm{HT}(f)t$-representation wrt. P.*

Proof: Let $f = \sum_{i=1}^{k} c_i s_i * p_i$ be a standard representation of f, with $c_i \in \mathbf{K}^*$, $s_i \in T$, $p_i \in P$ and $\mathrm{HT}(s_i * p_i) \leq \mathrm{HT}(f)$ for all $1 \leq i \leq k$. Then

$$bu * f = \sum_{i=1}^{k} bu * c_i s_i * p_i.$$

Now by the product proposition 3.2.5 there exist $d_i \in \mathbf{K}^*$ and $h_i \in R$ with $h_i < us_i$ and $bu * c_i s_i = d_i bc_i(us_i) + h_i$. Since $h_i \in R$ we have $h_i = \sum_{j=1}^{k_i} e_{ij} s_{ij}$. And we can multiply out. This shows that

$$bu * f = \sum_{i=1}^{k} (d_i bc_i(us_i) + \sum_{j=1}^{k_i} e_{ij} s_{ij}) * p_i = \sum_{i=1}^{k'} c'_i s'_i * p_i.$$

Since $s_i \mathrm{HT}(p_i) \leq \mathrm{HT}(f)$ we have $us_i \mathrm{HT}(p_i) \leq u\mathrm{HT}(f)$ and since $h_i < us_i$ also $s_{ij} < us_i$ and so $s'_i \mathrm{HT}(p'_i) \leq u\mathrm{HT}(f) = \mathrm{HT}(uf) = \mathrm{HT}(u * f)$. This shows that $bu * f$ has a standard representation wrt. P as claimed.

Now let $p \in P$ and let $f = \sum_{i=1}^{k} c_i s_i$ be a polynomial in R with $c_i \in \mathbf{K}^*$, $s_i \in T$. Let $s = \mathrm{HT}(f)$ then we have $s_i \leq s$ for $1 \leq i \leq k$. Then by the product proposition 3.2.5 $\mathrm{HT}(s_i * p) \leq \mathrm{HT}(s * p) = \mathrm{HT}(f * p)$ for $1 \leq i \leq k$. This shows, that

$$f * p = \sum_{i=1}^{k} c_i s_i * p$$

is a representation for $f * p$ which is a standard representation wrt. P. In the same way the claims for t-representations are proved. □

Lemma 4.5.3 *Let P be a finite subset of R and let $f \in R$. If $f \longrightarrow_P^* 0$, then f has a standard representation wrt. P.*

Proof: Let $f \longrightarrow_P^k 0$ for some $k \in \mathbf{N}$. We proceed by induction on k. For $k = 0$ we have $f = 0$ as standard representation.

For $k > 0$ let $f \longrightarrow_P g \longrightarrow_P^{k-1} 0$. Assume by induction assumption g has standard representation $g = \sum_{i=1}^{k} c_i s_i * p_i$, with $c_i \in \mathbf{K}^*$, $s_i \in T$, $p_i \in P$ for all $1 \leq i \leq k$. By definition of the reduction relation there exists $t \in T(f)$, $p \in P$ such that we have $f \longrightarrow_{t,P} g = f - cu * p$ with $t = \mathrm{HT}(u * p) = u * \mathrm{HT}(p) \leq \mathrm{HT}(f)$. So

$$f = cu * p + \sum_{i=1}^{k} c_i s_i * p_i$$

is a standard representation of f wrt. P. □

Lemma 4.5.4 *Let P be a finite subset of R, let* $\mathrm{ideal}_l(P)$ *be the left ideal generated by P and let $f \in \mathrm{ideal}_l(P)$. If all $0 \neq g \in \mathrm{ideal}_l(P)$ have a standard representation wrt. P then $f \longrightarrow_P^* 0$.*

Proof: If $f = 0$, then trivially $f \longrightarrow_P^* 0$. If $f \neq 0$ and $f \in \mathrm{ideal}_l(P)$, then f has a standard representation wrt. P: $f = \sum_{i=1}^{k} c_i s_i * p_i$, with $c_i \in \mathbf{K}^*$, $s_i \in T$, $p_i \in P$ for all $1 \leq i \leq k$. Let $J_t = \{j \ : \ 1 \leq j \leq n, \mathrm{HT}(s_i * p_i) = t\}$. We proceed by noetherian induction on $t = \mathrm{HT}(f)$.

Now $J_t \neq \emptyset$ since the representation is standard. Pick $l \in J_t$, and define a reduction $f \longrightarrow_{t,p_l} g$ by $g = f - cs_l * p_l$, where $0 \neq c \in \mathbf{K}$ such that $\mathrm{coeff}(t, f) = c\ \mathrm{coeff}(t, s_l * p_l)$. Now $g < f$, by construction $g \in \mathrm{ideal}_l(P)$ and so by induction assumption $g \longrightarrow_P^* 0$. Combining both reductions we obtain $f \longrightarrow_{t,P} g \longrightarrow_P^* 0$ as claimed. □

Proposition 4.5.5 *Let P be a finite subset of R, let* $\mathrm{ideal}_l(P)$ *be the left ideal generated by P. Then the following two conditions are equivalent:*

1. *For all $f \in \mathrm{ideal}_l(P)$, $f \longrightarrow_P^* 0$.*
2. *All $0 \neq f \in \mathrm{ideal}_l(P)$ have a standard representation wrt. P.*

Proof: $\Longrightarrow$ Let $0 \neq f \in \mathrm{ideal}_l(P)$, then by assumption $f \longrightarrow_P^* 0$ and by lemma 4.5.3 f has a standard representation wrt. P.

$\Longleftarrow$ Let $0 \neq f \in \mathrm{ideal}_l(P)$, by assumption all $0 \neq g \in \mathrm{ideal}_l(P)$ have a standard representation wrt. P. So by lemma 4.5.4 f is reducible to zero: $f \longrightarrow_P^* 0$. □

We will now show that all polynomials have standard representations wrt. P if a finite set of so called S-polynomials have a standard representation wrt. P. First the definition:

Definition 4.5.6 (Left S-Polynomial) *Let $f, g \in R$, $s, t, u, v, w \in T$, such that $s = \mathrm{HT}(f)$, $t = \mathrm{HT}(g)$, $w = \mathrm{lcm}(s, t)$, $us = w$ and $vt = w$. Furthermore let $a, b \in \mathbf{K}^*$ such that $a = \mathrm{coeff}(w, u * f)$ and $b = \mathrm{coeff}(w, v * g)$. Let $b', a' \in \mathbf{K}^*$ such that $b' = ba^{-1}$, $a' = 1$ so $b'a = a'b$, then*

$$\mathrm{LSP}(f, g) = b'u * f - a'v * g$$

is called the left S-polynomial *of f and g.*

Note, that by proposition 3.2.5 both a and b are $\neq 0$ and so $\mathrm{HT}(\mathrm{LSP}(f, g)) < w$. Note furthermore that $\mathrm{LSP}(g, f) = -\mathrm{LSP}(f, g)$ and $\mathrm{LSP}(f, g) \in \mathrm{ideal}_l(f, g)$ respectively $\mathrm{LSP}(f, g) \in \mathrm{ideal}_l(P)$ for any set P such that $f, g \in P$.

Lemma 4.5.7 *Let P be a finite subset of R, let* $\mathrm{ideal}_l(P)$ *be the left ideal generated by P. Furthermore let $H = \{\mathrm{LSP}(f, g) \ : \ f, g \in P, f \neq g\}$. Then the following assertions are equivalent:*

1. *all* $0 \neq f \in \mathrm{ideal}_l(P)$ *have a standard representation wrt.* P,
2. *all* $0 \neq h \in H$ *have a standard representation wrt.* P.

Proof: $\Longrightarrow$ Since for $0 \neq h \in H$ we have $h \in \mathrm{ideal}_l(P)$, so h has a standard representation wrt. P.

$\Longleftarrow$ Let $0 \neq f \in \mathrm{ideal}_l(P)$ we may assume that f has a representation wrt. P:

$$f = \sum_{i=1}^{k} c_i s_i * p_i,$$

with $c_i \in \mathbf{K}^*$, $s_i \in T$, $p_i \in P$ for all $1 \leq i \leq k$. Let $s = \mathrm{HT}(f)$ and let $t \in T$ with $t = \max_{i=0}^{k}\{\mathrm{HT}(s_i * p_i)\}$ where the maximum is taken with respect to the term order on T. Let $J_t = \{j \mid 1 \leq j \leq k, \mathrm{HT}(s_j * p_j) = t > s\}$.

We show by noetherian induction on t and on $|J_t|$, that the representation can be transformed to a standard representation. Case $t = s$, then $|J_t| = \emptyset$ and we have already a standard representation.

Case $t > s$, then since $t \notin T(f)$, we have $|J_t| \geq 2$. Assume first that $|J_t| = 2$ and assume by induction, that the claim holds for all t' with $t > t' \geq s$ and $J'_t = \emptyset$. Let $J_t = \{m, n\}$, $m \neq n$.

Then consider $c_m s_m * p_m + c_n s_n * p_n$ from the representation of f. Note that t does not occur in f so $0 = \mathrm{coeff}(t, f) = \mathrm{coeff}(t, c_m s_m * p_m) + \mathrm{coeff}(t, c_n s_n * p_n)$, which implies $c_m \mathrm{coeff}(t, s_m * p_m) = -c_n \mathrm{coeff}(t, s_n * p_n)$. Furthermore we have $\mathrm{HT}(s_j * p_j) = s_j \mathrm{HT}(p_j) = t$, $j = m, n$ by proposition 3.2.5. Let $w = \mathrm{lcm}(\mathrm{HT}(p_m), \mathrm{HT}(p_n))$, then $t = w'w$.

From the definition of the S-polynomial of p_m and p_n let $u, v \in T$ with $w = u\mathrm{HT}(p_m) = v\mathrm{HT}(p_n)$ and $b, a'' \in \mathbf{K}^*$, such that b $\mathrm{coeff}(w, u * p_m) = a''$ $\mathrm{coeff}(w, v * p_n)$. So write $\mathrm{LSP}(p_m, p_n) = bu * p_m - a''v * p_n = bu * p_m + av * p_n$. We have $w'u = s_m$ and $w'v = s_n$. By proposition 3.2.5 let $w' * bu = b'w'u + h_1$ with $0 \neq b' \in \mathbf{K}$ and $h_1 < w'u = s_m$ and $w' * av = a'w'v + h_2$ with $0 \neq a' \in \mathbf{K}$ and $h_2 < w'v = s_n$.

Let $b_1 = b'^{-1}$ and $a_1 = a'^{-1}$ and write $s_m = w'u = b_1 w' * bu - b_1 h_1$ and $s_n = w'v = a_1 w' * av - a_1 h_2$. So we can write

$$\begin{aligned} c_m s_m * p_m + c_n s_n * p_n &= c_m(b_1 w' * bu - b_1 h_1) * p_m + c_n(a_1 w' * av - a_1 h_2) * p_n \\ &= c_m(b_1 w' * bu) * p_m + c_n(a_1 w' * av) * p_n \\ &\quad -c_m(b_1 h_1) * p_m - c_n(a_1 h_2) * p_n. \end{aligned}$$

Here it is important that $c_m(b_1 w') = c_n(a_1 w')$ respectively $c_m b_1 = c_n a_1$ which follows from b $\mathrm{coeff}(w, u * p_m) = a$ $\mathrm{coeff}(w, v * p_n)$, c_m $\mathrm{coeff}(t, s_m * p_m) = -c_n$ $\mathrm{coeff}(t, s_n * p_n)$ and the definition of a_1 and b_1.

Furthermore by lemma 4.5.2 $-c_m(b_1 h_1) * p_m$ and $-c_n(a_1 h_2) * p_n$ both have standard representations wrt. P. By assumption of the lemma $\mathrm{LSP}(p_m, p_n)$ has a a standard representation wrt. P. Multiplication of this representation with $c_m b_1 w'$ still yields a standard

representation by lemma 4.5.2:

$$\begin{aligned}\mathrm{LSP}(p_m,p_n) &= \sum_{i=1}^{k_1} c_i s_i * p_i \\ (c_m b_1 w') * \mathrm{LSP}(p_m,p_n) &= \sum_{i=1}^{k_1} (c_m b_1 w') * c_i s_i * p_i = \sum_{i=1}^{k_2} c_i' s_i' * p_i\end{aligned}$$

Now using the standard representations of $-c_m(b_1h_1)*p_m$, $-c_n(a_1h_2)*p_n$ and $(c_mb_1w')*\mathrm{LSP}(p_m,p_n)$ write

$$\begin{aligned}f &= \sum_{i=1,i\neq m,i\neq n}^{k} c_i s_i * p_i + c_m s_m * p_m + c_n s_n * p_n \\ &= \sum_{i=1,i\neq m,i\neq n}^{k} c_i s_i * p_i + (c_m b_1 w') * \mathrm{LSP}(p_m,p_n) - c_m(b_1h_1)*p_m - c_n(a_1h_2)*p_n \\ &= \sum_{i=1,i\neq m,i\neq n}^{k} c_i s_i * p_i + \sum_{i=1}^{k_2} c_i' s_i' * p_m + \sum_{j=1}^{k_h} c_j s_j * p_n\end{aligned}$$

Since $\mathrm{HT}(s_i'*p_i) < t$ and $\mathrm{HT}(s_j*p_j) < t$ this is now a representation of f with $|J_t'| = \emptyset$. The representation is not necessarily a standard representation, but all what is needed here, is that the number of 'bad' terms decreases.

Case $t > s$, $|J_t| > 2$. Assume by induction, that the claim holds for all t' with $t > t' \geq s$ and all J_t' with $|J_t'| < |J_t|$. Let $m, n \in J_t$, $m \neq n$, $J_t' = J_t \setminus \{m,n\}$.

Again consider $c_m s_m * p_m + c_n s_n * p_n$ from the representation of f.

In this case we cannot directly conclude, that this sum can be represented using the S-polynomial of p_m and p_n. But we can represent one (say the first) summand using the S-polynomial.

By the same arguments as in the previous case we write $c_m s_m * p_m + c_n' s_n * p_n = (c_m b_1 w') * \mathrm{LSP}(p_m,p_n) + h_1 * p_m + h_2 * p_n$. Observe, that probably $c_n' \neq c_n$. But $\mathrm{coeff}(t, c_m s_m * p_m) = -\mathrm{coeff}(t, c_n' s_n * p_n)$ so using the standard representations of $(c_m b_1 w') * \mathrm{LSP}(p_m,p_n)$ and $h_1 * p_m + h_2 * p_n$ write

$$\begin{aligned}f &= \sum_{i=1,i\neq m,i\neq n}^{k} c_i s_i * p_i + c_m s_m * p_m + c_n s_n * p_n \\ &= \sum_{i=1,i\neq m,i\neq n}^{k} c_i s_i * p_i + ((c_m b_1 w') * \mathrm{LSP}(p_m,p_n) + h_1 * p_m + h_2 * p_n) \\ &\quad -c_n' s_n * p_n + c_n s_n * p_n \\ &= \sum_{i=1,i\neq m,i\neq n}^{k} c_i s_i * p_i + (c_n - c_n') s_n * p_n \\ &\quad + \sum_{i=1}^{k'} c_i' s_i' * p_i + \sum_{j=1}^{k_1} c_{j1} s_{j1} * p_m + \sum_{j=1}^{k_2} c_{j2} s_{j2} * p_n.\end{aligned}$$

For this representation (not necessarily standard) we have $|J'_t| \leq |J_t|-1$. Now by induction assumption we can find a standard representation for f which completes the proof. $\square$

Observe, that we actually do not need a standard representation of $\mathrm{LSP}(p_m, p_n)$ but only a v-representation for some $v < \mathrm{lcm}(\mathrm{HT}(p_m), \mathrm{HT}(p_n)) \leq t$ to improve the representation of f. This fact will be important in the next lemma, where we show, that a smaller set $H_b \subset H$ already suffices to proof the foregoing proposition. The criterion which characterizes the set H_b will be called (BBEC) for 'Buchberger's Euclidean Criterion' after Buchberger, who first invented the criterion ([Buchberger 1979]), and after Euclid, because the criterion avoids redundant computation as in Euclids algorithm in case of commutative polynomial rings in one variable.

Lemma 4.5.8 *Let P be a finite subset of R, let $\mathrm{ideal}_l(P)$ be the left ideal generated by P. Furthermore let $H = \{\mathrm{LSP}(f,g) \ : \ f,g \in P, f \neq g\}$ and let $H_b \subset H$ be such that the following conditions are fulfilled:*

> *if $\mathrm{LSP}(g_1,g_2) \in H$ with $\mathrm{LSP}(g_1,g_2) \notin H_b$ and $g_1, g_2 \in P$ then there exists $p \in P$ such that*
>
> $$\mathrm{HT}(p) \mid \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2)),$$
>
> *and $\mathrm{LSP}(g_1,p)$ and $\mathrm{LSP}(p,g_2) \in H_b$.* *(BBEC)*

Then the following assertions are equivalent:

1. *all $0 \neq f \in \mathrm{ideal}_l(P)$ have a standard representation wrt. P,*
2. *all $0 \neq h \in H_b$ have a standard representation wrt. P.*

Proof: $\Longrightarrow$ Since for $0 \neq h \in H_b$ we have $h \in \mathrm{ideal}_l(P)$, so h has a standard representation wrt. P.

$\Longleftarrow$ We may repeat the proof of the foregoing lemma 4.5.7. In case when a S-polynomial, of some $0 \neq p_m, p_n \in R$, is required which is not in H_b, but in H, we can find a t'-representation with $t' < t = \mathrm{lcm}(\mathrm{HT}(p_m), \mathrm{HT}(p_m))$ for it as described next. Using this t'-representation of $\mathrm{LSP}(p_m, p_n)$ instead of a standard representation of $\mathrm{LSP}(p_m, p_n)$ is then sufficient to improve the representation of f in the foregoing lemma 4.5.7.

The condition $\mathrm{HT}(p) \mid \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2))$ implies, that there exist $s_1, s_2 \in T$ such that

$$s_1 \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(p)) = t = s_2 \mathrm{lcm}(\mathrm{HT}(p), \mathrm{HT}(g_2)).$$

Let the 3 S-polynomials be

$$\begin{aligned} \mathrm{LSP}(g_1,g_2) &= b'_1 u_1 * g_1 - a'_1 v_1 * g_2 \\ \mathrm{LSP}(g_1,p) &= b'_2 u_2 * g_1 - a'_2 v_2 * p \\ \mathrm{LSP}(p,g_2) &= b'_3 u_3 * p - a'_3 v_3 * g_2. \end{aligned}$$

Where $0 \neq a_i, a_i', b_i, b_i' \in \mathbf{K}$, $u_i, v_i, w_i \in T$ $(i = 1, 2, 3)$ such that

$$\begin{aligned} t = w_1 &= \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(g_2)) = u_1\mathrm{HT}(g_1) = v_1\mathrm{HT}(g_2), \\ w_2 &= \mathrm{lcm}(\mathrm{HT}(g_1), \mathrm{HT}(p)) = u_2\mathrm{HT}(g_1) = v_2\mathrm{HT}(p), \\ w_3 &= \mathrm{lcm}(\mathrm{HT}(p), \mathrm{HT}(g_2)) = u_3\mathrm{HT}(p) = v_3\mathrm{HT}(g_2). \end{aligned}$$

Furthermore with $a_1 = \mathrm{coeff}(w_1, u_1 * g_1)$ and $b_1 = \mathrm{coeff}(w_1, v_1 * g_2)$, $a_2 = \mathrm{coeff}(w_2, u_2 * g_1)$ and $b_2 = \mathrm{coeff}(w_2, v_2 * p)$, $a_3 = \mathrm{coeff}(w_3, u_3 * p)$ and $b_3 = \mathrm{coeff}(w_3, v_3 * g_2)$; And with $b_i'a_i = a_i'b_i$, $i = 1, 2, 3$ by definition of the S-polynomials.

By the implications of the conditions on the head terms and the definitions of the S-polynomials let v_2, u_3 be such that we have $t = s_1v_2\mathrm{HT}(p) = s_2u_3\mathrm{HT}(p)$, which implies $s_1v_2 = s_2u_3$. Furthermore let u_2, v_3 be such that $s_1u_2 = u_1$ and $s_2v_3 = v_1$.

In order to setup the equation correctly we have to determine the following products:

$$\begin{aligned} s_1 * b_2' * u_2 &= (e_1b_2's_1 + q_1) * u_2 = e_1b_2'(e_5s_1u_2 + q_5) + q_1 * u_2 \\ &= e_1b_2'e_5(s_1u_2) + e_1b_2'q_5 + q_1 * u_2 \\ s_1 * a_2' * v_2 &= (e_2a_2's_1 + q_2) * v_2 = e_2a_2'(e_6s_1v_2 + q_6) + q_2 * v_2 \\ &= e_2a_2'e_6(s_1v_2) + e_2a_2'q_6 + q_2 * v_2 \\ s_2 * b_3' * u_3 &= (e_3b_3's_2 + q_3) * u_3 = e_3b_3'(e_7s_2u_3 + q_7) + q_3 * u_3 \\ &= e_3b_3'e_7(s_2u_3) + e_3b_3'q_7 + q_3 * u_3 \\ s_2 * a_3' * v_3 &= (e_4a_3's_2 + q_4) * v_3 = e_4a_3'(e_8s_2v_3 + q_8) + q_4 * v_3 \\ &= e_4a_3'e_8(s_2v_3) + e_4a_3'q_8 + q_4 * v_3 \end{aligned}$$

where by the product proposition 3.2.5 $0 \neq e_i \in \mathbf{K}$, $q_i \in R$ with $q_1, q_2 < s_1$, $q_3, q_4 < s_2$, $q_5 < u_2s_1$, $q_6 < v_2s_1$, $q_7 < u_3s_2$, $q_8 < v_3s_2$.

Let $0 \neq c_1, c_2, c_3, c_4, c_5 \in \mathbf{K}$ such that the following holds:

$$\begin{aligned} \mathrm{coeff}(t, c_1(e_2a_2'e_6)(s_1v_2) * p) &= \mathrm{coeff}(t, c_2(e_3b_3'e_7)(s_2u_3) * p) \\ &= \mathrm{coeff}(t, c_3b_1'(s_1u_2) * g_1), \end{aligned}$$

The existence follows from the Ore condition in $\mathbf{K}$. This implies by the definitions of $\mathrm{LSP}(p, g_2)$

$$\mathrm{coeff}(t, c_2(e_3b_3'e_7)(s_2u_3) * p) = \mathrm{coeff}(t, c_3a_1'(s_2v_3) * g_2).$$

which in turn implies by definition of $\mathrm{LSP}(g_1, g_2)$

$$\mathrm{coeff}(t, c_3b_1'(s_1u_2) * g_1) = \mathrm{coeff}(t, c_3a_1'(s_2v_3) * g_2),$$

Furthermore let $c_3b_1' = c_4(e_1b_2'e_5)$ and $c_3a_1' = c_5(e_4a_3'e_8)$.

The first equation establishes

$$0 = -c_1(e_2a_2'e_6)(s_1v_2) * p + c_2(e_3b_3'e_7)(s_2u_3) * p.$$

Then we can rewrite the S-polynomial of g_1 and g_2 as

$$\begin{aligned}
c_3\mathrm{LSP}(g_1,g_2) &= c_3b_1'u_1 * g_1 - c_3a_1'v_1 * g_2\\
&= c_4(e_1b_2'e_5)u_1 * g_1 - c_5(e_4a_3'e_8)v_1 * g_2\\
&= c_4(e_1b_2'e_5)(s_1u_2) * g_1 - c_5(e_4a_3'e_8)(s_2v_3) * g_2\\
&= c_4(e_1b_2'e_5)(s_1u_2) * g_1 - c_1(e_2a_2'e_6)(s_1v_2) * p\\
&\quad +c_2(e_3b_3'e_7)(s_2u_3) * p - c_5(e_4a_3'e_8)(s_2v_3) * g_2\\
&= c_4(s_1 * b_2' * u_2 - e_1b_2'q_5 - q_1 * u_2) * g_1\\
&\quad -c_1(s_1 * a_2' * v_2 - e_2a_2'q_6 - q_2 * v_2) * p\\
&\quad +c_2(s_2 * b_3' * u_3 - e_3b_3'q_7 - q_3 * u_3) * p\\
&\quad -c_5(s_2 * a_3' * v_3 - e_4a_3'q_8 - q_4 * v_3) * g_2\\
&= c_4(s_1 * b_2' * u_2) * g_1 - (e_1b_2'q_5 + q_1 * u_2) * g_1\\
&\quad -c_1(s_1 * a_2' * v_2) * p - (e_2a_2'q_6 + q_2 * v_2) * p\\
&\quad +c_2(s_2 * b_3' * u_3) * p - (e_3b_3'q_7 + q_3 * u_3) * p\\
&\quad -c_5(s_2 * a_3' * v_3) * g_2 - (e_4a_3'q_8 + q_4 * v_3) * g_2\\
&= c_4(s_1 * b_2' * u_2) * g_1 - c_1(s_1 * a_2' * v_2) * p\\
&\quad +c_2(s_2 * b_3' * u_3) * p - c_5(s_2 * a_3' * v_3) * g_2\\
&\quad -(e_1b_2'q_5 + q_1 * u_2) * g_1 - (e_2a_2'q_6 + q_2 * v_2) * p\\
&\quad -(e_3b_3'q_7 + q_3 * u_3) * p - (e_4a_3'q_8 + q_4 * v_3) * g_2\\
&= c_1s_1 * \mathrm{LSP}(g_1,p) + c_2s_2 * \mathrm{LSP}(p,g_2)\\
&\quad -(e_1b_2'q_5 + q_1 * u_2) * g_1 - (e_2a_2'q_6 + q_2 * v_2) * p\\
&\quad -(e_3b_3'q_7 + q_3 * u_3) * p - (e_4a_3'q_8 + q_4 * v_3) * g_2.
\end{aligned}$$

Now $\mathrm{LSP}(g_1,p)$ and $\mathrm{LSP}(p,g_2) \in H_b$, so by assumption they have standard representations in particular they have w_2' respectively w_3'-representations with $w_2' < w_2$ and $w_3' < w_3$. Then by lemma 4.5.2 $c_1s_1 * \mathrm{LSP}(g_1,p)$ and $c_2s_2 * \mathrm{LSP}(p,g_2)$ have standard representations with products $< t$.

Furthermore by lemma 4.5.2 all summands $(e_1b_2'q_5 + q_1 * u_2) * g_1 = h_1 * g_1$, $(e_2a_2'q_6 + q_2 * v_2) * p = h_2 * p$, $(e_3b_3'q_7 + q_3 * u_3) * p = h_3 * p$ and $(e_4a_3'q_8 + q_4 * v_3) * g_2 = h_4 * g_2$ have standard representations with products $< t$. This shows, that the sum of all this standard representations is a t'-representation of $\mathrm{LSP}(g_1,g_2)$ for some $t' < t$.

At this point we can continue as in the proof of the preceding lemma 4.5.7. □

Proposition 4.5.9 *Let P be a finite subset of R let* $\mathrm{ideal}_l(P)$ *be the left ideal generated by P. Then the following assertions are equivalent:*

1. *for all $f \in \mathrm{ideal}_l(P)$, $f \longrightarrow_P^* 0$,*
2. *for all $h \in H = \{\mathrm{LSP}(f,g) \ : \ f,g \in P, f \neq g\}$, $h \longrightarrow_P^* 0$.*
3. *for all $h \in H_b \subseteq H$, such that H_b satisfies the condition (BBEC) of lemma 4.5.8, $h \longrightarrow_P^* 0$.*

Proof: (1) $\Longrightarrow$ (2) and (3): Since for $h \in H_b$, $h \in H$ we have $h \in \text{ideal}_l(P)$ and by assumption $h \longrightarrow_P^* 0$.

(2) $\Longrightarrow$ (1): By assumption all $h \in H$, $h \longrightarrow_P^* 0$. By lemma 4.5.3 this implies that all $0 \neq h \in H$ have a standard representation. By lemma 4.5.7 this implies that all $0 \neq f \in \text{ideal}_l(P)$ have a standard representation wrt. P. So by lemma 4.5.4 f is reducible to zero: $f \longrightarrow_P^* 0$.

(3) $\Longrightarrow$ (1): By assumption all $h \in H_b$, $h \longrightarrow_P^* 0$. By lemma 4.5.3 this implies that all $0 \neq h \in H_b$ have a standard representation. By lemma 4.5.8 this implies that all $0 \neq f \in \text{ideal}_l(P)$ have a standard representation wrt. P. So by lemma 4.5.4 f is reducible to zero: $f \longrightarrow_P^* 0$. □

Using this proposition it is possible to reduce the test whether all polynomials in the left ideal are reducible wrt. P to the finite set H and furthermore to an even smaller set H_b. An algorithm which exploits this fact for the construction of ideal bases inducing confluent reduction relations will be discussed in a later section. But first we summarize the foregoing studies in the next section.

A final remark on further 'optimizations':

Claim 4.5.10 *In commutative polynomial rings the first of Buchberger's criteria states that if for two polynomials* $f, g \in G$

$\text{HT}(f)\text{HT}(g) = \text{lcm}(\text{HT}(f), \text{HT}(g))$ *then*
$\text{SP}(f, g)$ *has a standard representation wrt.* G. *(BBGC)*

This criterion will be called (BBGC) for 'Buchberger's Gaussian Criterion' after Buchberger, who first invented the criterion, and after Gauss, because the criterion avoids redundant computation as in Gauss algorithm in case of commutative linear polynomials.

This criterion is no more valid in the non-commutative case as the following counter-example shows:

Example 4.5.11 *Let* $R = \mathbf{Q}\{X, Y; Y * X = XY - 1\}$ *be the first Weyl algebra. Consider the following two polynomials* $p = X$, $q = Y$. *Then* $\text{HT}(p)\text{HT}(q) = \text{lcm}(\text{HT}(p), \text{HT}(q)) = XY$, *but* $\text{SP}(p, q) = X * Y - Y * X = XY - XY + 1 = 1$ *and* 1 *has no standard representation wrt.* $\{p, q\}$.

However as the proof in the commutative case shows, the criterion is a local criterion in the sense, that only the two involved polynomials need to be commutative. Moreover the criterion remains true if the coefficient ring is non-commutative, as long as it is a field. So the criterion is still valid for *commuting* polynomials, in particular for elements in the center it may be exploited. Although it would be too expensive to check each time if polynomials commute, it might be possible to determine such cases by an analysis of the commutator relations. This can be done as outlined in section 3.6.

4.6 Left Gröbner Bases

We are going to give characterizations of confluent reduction relations in a solvable polynomial ring by ideal membership tests, standard representations and S-polynomials.

Definition 4.6.1 *Let $G \subset R$ be a finite subset of R. If the left reduction relation $\longrightarrow_G$ satisfies one of the conditions of definition 4.1.4 then G is called a* left Gröbner base. *(Since $\longrightarrow_G$ is Noetherian, by lemma 4.1.5 $\longrightarrow_G$ satisfies all conditions of definition 4.1.4.)*

Theorem 4.6.2 *Let G be a finite subset of R, then the following assertions are equivalent.*

1. *G is a left Gröbner base.*
2. *For all $f, g \in R$, if $f - g \in \mathrm{ideal}_l(G)$ then $f \downarrow_G g$.*
3. *For all $f \in \mathrm{ideal}_l(G)$, $f \longrightarrow_G^* 0$.*
4. *For all $0 \neq f \in \mathrm{ideal}_l(G)$, $f \longrightarrow_G f'$.*
5. *For all $0 \neq f \in \mathrm{ideal}_l(G)$, there exists $g \in G$ such that $\mathrm{HT}(g) \mid \mathrm{HT}(f)$.*
6. *All $0 \neq f \in \mathrm{ideal}_l(G)$ have a standard representation wrt. G.*
7. *For all $h \in H = \{\mathrm{LSP}(f, g) \ : \ f, g \in G, f \neq g\}$, $h \longrightarrow_G^* 0$.*
8. *For all $h \in H_b \subseteq H$, such that H_b satisfies the condition (BBEC) of lemma 4.5.8, $h \longrightarrow_P^* 0$.*

Proof: (1) $\Longrightarrow$ (2): Let $f, g \in R$ such that $f - g \in \mathrm{ideal}_l(G)$. Then lemma 4.4.5: $f \longleftrightarrow_G^* g$. By (1) $\longrightarrow_G$ has the Church-Rosser property, so $f \downarrow_G g$.

(2) $\Longrightarrow$ (3): Specialise $g = 0$ in (2).

(3) $\Longrightarrow$ (1): We show that $\longrightarrow_G$ is confluent. Let $f, f_1, f_2 \in R$ such that $f \longrightarrow_G^* f_1$ and $f \longrightarrow_G^* f_2$, that is $f_1 \longleftrightarrow_G^* f_2$. By lemma 4.4.2 $f_1 - f_2 \in \mathrm{ideal}_l(G)$ and by (3) $f_1 - f_2 \longrightarrow_G^* 0$. From this by lemma 4.2.6 $f_1 \downarrow_G f_2$.

(3) $\Longrightarrow$ (4): By definition of $\longrightarrow_G^*$.

(4) $\Longrightarrow$ (3): Assume $0 \neq f \in \mathrm{ideal}_l(G)$ is minimal such that not $f \longrightarrow_G^* 0$. Now by (4) $f \longrightarrow_G f'$ with $f' \in \mathrm{ideal}_l(G)$ by lemma 4.4.2. However by definition of f: $f' \longrightarrow_G^* 0$ and so $f \longrightarrow_G^* 0$ a contradiction.

(5) $\Longrightarrow$ (4): By definition of left head term reduction.

(3) $\Longrightarrow$ (5): Assume $0 \neq f \in \mathrm{ideal}_l(G)$ and let $f \longrightarrow_G^k 0$ for some $k \in \mathbf{N}$. Let $1 \leq m \leq k$ minimal, and let $g \in G$ such that $f_m \longrightarrow_{t,g} f_{m+1}$ where $t = \mathrm{HT}(f)$. By definition of reduction this shows that $\mathrm{HT}(g) \mid \mathrm{HT}(f)$.

(3) $\Longleftrightarrow$ (6): follows from the equivalence of claims (1) and (2) in proposition 4.5.5.

(3) $\Longleftrightarrow$ (7): follows from the equivalence of claims (1) and (2) in proposition 4.5.9.

(3) $\Longleftrightarrow$ (8): follows from the equivalence of claims (1) and (3) in proposition 4.5.9. □

The proof of the following theorem presents the Buchberger algorithm for constructing Gröbner bases. The usage of the criterion (BBEC) is not shown, it is discussed in the implementation section.

Theorem 4.6.3 (Construction of left Gröbner bases) *Let R be a solvable polynomial ring over a computable skew field* **K** *with respect to a decidable term order. For any finite $F \subset R$ one can construct a left Gröbner base G of* $\mathrm{ideal}_l(F)$.

Proof: We give an algorithm which computes a left GB in table 4.3.

Algorithm: $LGB(F)$
Input: $F = \{f_1, \ldots, f_k\} \subseteq R$.
Output: A left Gröbner base G of $\mathrm{ideal}_l(F)$.
begin $G \leftarrow F$.
  $B \leftarrow \{(f,g) \ : \ f,g \in F, f \neq g\}$.
  while $B \neq \emptyset$ **do** Let $(f,g) \in B$.
    $B \leftarrow B \setminus \{(f,g)\}$.
    $h' \leftarrow \mathrm{LSP}(f,g)$.
    $h \leftarrow \mathrm{LNF}(h', G)$.
    if $h \neq 0$
      then $B \leftarrow B \cup \{(p,h) \ : \ p \in G\}$.
        $G \leftarrow G \cup \{h\}$
      end.
    end.
  return(G).
end LGB.

Table 4.3: Algorithm: LGB

Correctness follows from theorem 4.6.2(7), since upon termination $B = \emptyset$, which guaranties that all S-polynomials of polynomial pairs of G reduce to zero. Termination follows since a non-terminating run would produce an infinite sequence of polynomials where each new polynomial has an irreducible head term with respect to the earlier ones, which would contradict Dickson's lemma 3.1.1. □

4.7 Confluence and S-Polynomials

For completeness we give a direct proof of the properties of Gröbner bases using S-polynomials without using standard representations.

Proposition 4.7.1 *Let $G \subset R$ be a finite subset of R and let $H = \{\mathrm{LSP}(f,g) \ : \ f,g \in G, \mathrm{LSP}(f,g) \notin G\}$. Then G is a Gröbner base iff for all $f,g \in G$, $\mathrm{LSP}(f,g) \longrightarrow_G^* 0$.*

Proof: $\Longrightarrow$ Let $f,g,h,h' \in G$ and $h = \mathrm{LSP}(f,g)$. If $h = 0$ then the proposition is true.

If $h \neq 0$ let $h = b*u*f - a*v*g$, $a,b \in \mathbf{K}^*$, $u,v \in T$ as in the definition of $\mathrm{LSP}(f,g)$. Again by definition of $\mathrm{LSP}(f,g)$: $\mathrm{HT}(u*f) = u\mathrm{HT}(f) = t = v\mathrm{HT}(g) = \mathrm{HT}(v*g)$. So we can define two reductions $b*u*f \longrightarrow_{t,g} h = b*u*f - a*v*g = \mathrm{LSP}(f,g)$ and $b*u*f \longrightarrow_{t,f} h' = b*u*f - b*u*f = 0$. Since $\longrightarrow_G$ is confluent there exists h_1 such that $0 = h' \longrightarrow_G^* h_1$ and $\mathrm{LSP}(f,g) = h \longrightarrow_G^* h_1$. By this $0 = h_1$ and so $\mathrm{LSP}(f,g) \longrightarrow_G^* 0$.

$\Longleftarrow$ Let $G' = \{\mathrm{LSP}(p_i,p_j) \ : \ p_i,p_j \in G, \mathrm{LSP}(p_i,p_j) \notin G\}$ and let $G'' = G \cup G'$.

We show first that $\longrightarrow_{G''}$ is locally confluent. Let $f,f_1,f_2 \in R$, $p_1,p_2 \in G''$, $s,t, \in T(f)$, $u,v \in T$, such that $f \longrightarrow_{s,G''} f_1 = f - a*u*p_1$ and $f \longrightarrow_{t,G''} f_2 = f - b*v*p_2$. By Noetherian induction on the well-founded quasi-ordering $<_T$ assume that the reduction relation $\longrightarrow_{G''}$ is locally confluent on $F = \{h \in R \ : \ h <_T \min\{t,s\}\}$. By proposition 4.1.5 $\longrightarrow_{G''}$ is confluent on F and in particular for all $f \in \mathrm{ideal}_l(G'')$ with $\mathrm{HT}(f) < t$, $f \longrightarrow_{G''}^* 0$ holds. By lemma 4.2.6 it suffices to show $(f_1 - f_2) \longrightarrow_{G''}^* 0$, since then $f_1 \downarrow_{G''} f_2$ as desired. Let $f_1 - f_2 = f - a*u*p_1 - (f - b*v*p_2) = a*u*p_1 - b*v*p_2$.

Case $s \neq t$, say $s > t$: Then $s \in T(f_2) \setminus T(f_1)$ and so $s \in T(f_1 - f_2)$. Now $(f_1 - f_2) \longrightarrow_{s,G''} (f_1 - f_2) - a*u*p_1 = b*v*p_2$. By lemma 4.2.2 $v*p_2 \longrightarrow_{G''} v*p_2 - v*p_2 = 0$.

Case $s = t$: Since both p_1 and p_2 reduce the same term in f we have $\mathrm{HT}(u*p_1) = u\mathrm{HT}(p_1) = t = v\mathrm{HT}(p_2) = v*\mathrm{HT}(p_2)$. In particular t is a multiple of $\mathrm{lcm}(\mathrm{HT}(p_1),\mathrm{HT}(p_2))$. Let $t = w\ \mathrm{lcm}(\mathrm{HT}(p_1),\mathrm{HT}(p_2))$, $v = wv'$ and $u = wu'$. Then $\mathrm{LSP}(p_1,p_2) = a'*u'*p_1 - b'*v'*p_2$ for $0 \neq a',b' \in \mathbf{K}$. Furthermore $w*\mathrm{LSP}(p_1,p_2) = w*(a'*u'*p_1 - b'*v'*p_2) = (w*a'*u')*p_1 - (w*b'*v')*p_2 = (a''wu' + h_1)*p_1 - (b''wv' + h_2)*p_2 = a''wu'*p_1 - b''wv'*p_2 + h_1*p_1 - h_2*p_2 = au*p_1 - bv*p_2 + h_1*p_1 - h_2*p_2$. Where $h_1 < u$ and $h_2 < v$ by proposition 3.2.5. By this

$$f_1 - f_2 = a*u*p_1 - b*v*p_2 = w*\mathrm{LSP}(p_1,p_2) - h_1*p_1 + h_2*p_2.$$

Now by lemma 4.2.2 $w*\mathrm{LSP}(p_1,p_2) \longrightarrow_{t,G''} 0$. For the second and third sumand $h_1*p_1 < t$, $h_2*p_2 < t$ and so by induction assumption $h_1*p_1 \longrightarrow_{G''} 0$ and $h_2*p_2 \longrightarrow_{G''} 0$. By twofold application of lemma 4.3.7 $w*\mathrm{LSP}(p_1,p_2) - h_1*p_1 + h_2*p_2 \longrightarrow_{G''} 0$.

Both cases show that $\longrightarrow_{G''}$ is locally confluent and so G'' is a Gröbner base. By assumption of the proposition $\mathrm{LSP}(p_i,p_j) \longrightarrow_G^* 0$. so there exists $h \in R$ such that $\mathrm{LSP}(p_i,p_j) \longrightarrow_G h$. This shows that G, G', G'' satisfy the assumptions of lemma 4.3.3 which finally proves that G is a Gröbner base. □

In commutative polynomial rings, the following lemma can be proven without knowing that $\longrightarrow_P^*$ is confluent on 'smaller polynomials'. In case of solvable polynomial rings the proof seems not to hold. However $f*p \in \mathrm{ideal}_l(P)$, and if P is a Gröbner base, then $f*p \longrightarrow_P^* 0$ by theorem 4.6.2(3).

Lemma 4.7.2 *Let $P \subset R$ be a Gröbner base. For all $f \in R$, $p \in P$ we have $f*p \longrightarrow_P^* 0$.*

4.8 Right Reduction

In this section we introduce right reductions and discuss their relation to left reductions. For the right reduction we face the following problem: to reduce e.g. the polynomial bX_i we must find $a \in \mathbf{K}$ such that $bX_i = c_{ai}aX_i$ where $X_i * a = c_{ai}aX_i + p_{ij}$ by axiom 3.2.1. In other words, for any $b \in \mathbf{K}$ we must find $a \in \mathbf{K}$ such that $b = c_{ai}a$. This requires that the endomorphisms $\alpha_i : \mathbf{K} \longrightarrow \mathbf{K}$, $a \mapsto c_{ai}a$ must be *surjective*. Since we have already shown that each of this endomorphisms is injective in case $\mathbf{K}$ is a domain, we require α_i to be bijective and hence to be an automorphism.

> So from now on we will make the global assumption that the α_i $(1 \leq i \leq n)$ are surjective (hence automorphisms) whenever we consider right ideals and right reductions.

Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ denote a solvable polynomial ring.

Definition 4.8.1 (Right Reduction) *Let $p \in R$, $t \in T$. Then the* right reduction $\longrightarrow_{r,t,p} \subseteq R \times R$ *is defined as follows:*

> *For $f, f' \in R$, $t \in T(f)$, $f \longrightarrow_{r,t,p} f'$ iff there exists $u \in T$ such that $t = u \cdot \mathrm{HT}(p) = \mathrm{HT}(p * u)$ and*
>
> $$f' = f - p * a_u u,$$
>
> *where $a_u \in \mathbf{K}^*$ is the unique element of $\mathbf{K}^*$ such that $\mathrm{coeff}(t, f) = \mathrm{coeff}(t, p * a_u u)$.*

By construction $t \notin T(f')$. If for certain f, t no such u exists, then t in $T(f)$ is called irreducible wrt. p. *$\longrightarrow_{r,p}$ and $\longrightarrow_{r,P}$ for a subset $P \subseteq R$ are defined like the respective definitions for left reductions.*

This definition requires that

1. $\mathrm{HT}(p)$ divides t in the commutative sense and
2. the head term of $p * u$ is equal to t,
3. furthermore a_u must be determined in a way that the coefficient of t in f is equal to the coefficient of t in $p * a_u u$.

Now (1) is constructive by comparing exponents of powers of X_i in t and in $\mathrm{HT}(p)$ (which also determines u) and (2) holds by proposition 3.2.5. Furthermore (3) can be satisfied, since all endomorphisms $\alpha_i : \mathbf{K} \longrightarrow \mathbf{K}$ with $a \mapsto c_{ai}a$ are by assumption surjective. Note that (3) may be hard to satisfy algorithmicaly and only under further restrictions on the automorphisms α_i, e.g. the condition that $\alpha_i = \mathrm{id}_{\mathbf{K}}$.

Lemma 4.8.2 *Let $p \in R$, $u \in T$, $a \in \mathbf{K}^*$ and let $t = \mathrm{HT}(p * u)$. Then $p * au \longrightarrow_{r,t,p} 0$.*

Proof: By proposition 3.2.5 we have $p * au = cup + h$ with $t = \mathrm{HT}(up) = u\mathrm{HT}(p)$. Let $a_u = a$ then $\mathrm{coeff}(t, p * au) = \mathrm{coeff}(t, p * a_u u)$. So $cup + h - (p * a_u u) = 0$ as claimed. □

Lemma 4.8.3 *Let $f, p \in R$, $t \in T(f)$. Then f is left reducible by p erasing t iff f is right reducible by p erasing t.*

Proof: Under these conditions, we know that $t = \mathrm{HT}(s * \mathrm{HT}(p)) = s\mathrm{HT}(p)$ for $s \in T$ and that $\mathrm{coeff}(t, s * p) \neq 0 \Longleftrightarrow \mathrm{coeff}(t, p * s) \neq 0$. And the coefficients can be determined such that $\mathrm{coeff}(t, f) = \mathrm{coeff}(t, a_s s * p) = \mathrm{coeff}(t, p * a'_s s)$. □

Lemma 4.8.4 (Right Translation Lemma) *Let $f, g, h, f', g', h' \in R$, $P \subset R$ (finite). If $f = g + h$ and $h \longrightarrow^*_{r,P} h'$ then there exist f' and g' such that $f \longrightarrow^*_{r,P} f'$, $g \longrightarrow^*_{r,P} g'$ and $f' = g' + h'$.*

Proof: As in the left case. □

Lemma 4.8.5 *Let $f, g \in R$, $P \subset R$ (finite). If $f - g \longrightarrow^*_{r,P} 0$ then $f \downarrow_{r,P} g$.*

4.9 Right Representations

Recall that $\mathrm{ideal}_r(P)$ denotes the right ideal generated by $P \subseteq R$.

Definition 4.9.1 *Let $I = \mathrm{ideal}_r(P)$ be a right ideal in R, generated by a finite subset $P = \{p_1, \ldots, p_k\}$ of R. Then any $f \in I$ has a* right representation *(with respect to P):*

$$f = \sum_{p \in P} p * h_p = \sum_{i=1}^{k} p_i * c_i s_i,$$

where $h_p \in R$, $c_i \in \mathbf{K}^*$, $s_i \in T$ and $p_i \in P$ for $1 \leq i \leq k$.

Again note, that the p_i need not be distinct.

Lemma 4.9.2 *Let P be a finite subset of R, $f \in R$ with $f \in \mathrm{ideal}_r(P)$. Then f has a representation of the form*

$$f = \sum_{i=1}^{k} p_i * s_i * c_i,$$

where $c_i \in \mathbf{K}^*$, $s_i \in T$ and $p_i \in P$ for $1 \leq i \leq k$.

Proof: Since $f \in \mathrm{ideal}_r(P)$, f has a representation $f = \sum_{i=1}^{k} p_i * b_i s_i$ with $b_i \in \mathbf{K}^*$, $s_i \in T$ and $p_i \in P$ for $1 \leq i \leq k$.

The proof is by Noetherian induction on $v = \max\{\mathrm{HT}(p_i * s_i) \ : \ 1 \leq i \leq k\}$ where $p_i * b_i s_i$ are not jet of the desired form, and $J = \{i \ : \ \mathrm{HT}(p_i * s_i) = v, 1 \leq i \leq k\}$.

Assume first $|J| = 1$ and assume without loss of generality $k = 1$ with $v = \mathrm{HT}(p_1 * s_1) = \mathrm{HT}(p_1)$, that is $s_1 = 1$. Then let $c_1 = b_1$ and $f = p_1 * s_1 * c_1$ is the desired representation.

Now assume that $|J| > 1$ and assume without loss of generality $k = 1$ with $v = \mathrm{HT}(p_1 * s_1)$. By proposition 3.2.5 and surjectivity of the endomorphisms $\mathbf{K} \longrightarrow \mathbf{K}$ $a \mapsto c_{ai}a$ there exists $c_1 \in \mathbf{K}^*$ with $s_1 * c_1 = b_1 s_1 + h_1$ with $b_1 \neq 0$ $h_1 <_t s_1$, $h_1 \in R$.

Now $p_1 * h_1 <_T \mathrm{HT}(p_1 * s_1)$ and $p_1 * h_1 = f' \in \mathrm{ideal}_r(P)$, so by induction assumption f' has a representation $f' = \sum_{i=1}^{k'} p'_i * s'_i * c'_i$, where $c'_i \in \mathbf{K}^*$, $s'_i \in T$ and $p'_i \in P$ for $1 \leq i \leq k'$.

Then $b_1 s_1 = s_1 * c_1 - \sum_{i=1}^{k'} p'_i * s'_i * c'_i$ is a representation of $b_1 s_1$ in the desired form. Furthermore for $f' = \sum_{i=2}^{k} p_i * b_i s_i$ we have $|J'| < |J|$ and by induction assumption we may assume that f' has a representation $f' = \sum_{i=1}^{k''} p''_i * s''_i * c''_i$. Combining the two representations we obtain $f = p_1 * s_1 * c_1 - \sum_{i=1}^{k'} p'_i * s'_i * c'_i + \sum_{i=1}^{k''} p''_i * s''_i * c''_i$ as claimed. □

The relation between right reductions and membership in right ideals is contained in the following lemma.

Lemma 4.9.3 *Let $f, g \in R$, $P \subset R$, P finite. Then $f \longleftrightarrow^*_{r,P} g$ if and only if $f - g \in \mathrm{ideal}_r(P)$.*

Proof: As for the left cases 4.4.2, 4.4.5. □

As for left reduction there is an algorithm, which computes for any element $f \in R$ its right normal form.

Lemma 4.9.4 *For any finite $F \subset R$ and any $f \in R$ one can compute $g \in R$ such that*

1. *$f \longrightarrow^*_{r,F} g$ and $f - g \in \mathrm{ideal}_r(F)$.*
2. *g is irreducible modulo F.*

Proof: We give an algorithm which computes g in table 4.4.

Partial correctness follows from the definition of reduction and lemma 4.8.3. Termination follows from the well-foundedness of the $<$ quasi-order on R as in the case of left normal form. □

Algorithm: $RNF(f, F)$
Input: $f \in R$ and $F = \{f_1, \ldots, f_k\} \subseteq R$.
Output: $g \in R$ satisfying the conditions (1) and (2) of the lemma.
begin $D \leftarrow \mathrm{HT}(F)$. $g \leftarrow f$.
  while $\exists s \in D$ with $s \mid t$ for some $t \in T(g)$ **do**
    Let $p \in F$ with $\mathrm{HT}(p) = s$. Let $u \in T$ with $t = su$.
    Determine $c \in \mathbf{K}^*$, such that $\mathrm{coeff}(t, g) = \mathrm{coeff}(t, p * (cu))$.
    $g \leftarrow g - p * (cu)$.
    end.
  return(g).
end RNF.

Table 4.4: Algorithm: RNF

4.10 Right Gröbner Bases

Incorporating the definitions of the right reduction right standard representations and right S-polynomials (RSP) we may obtain the right analogons of the left Gröbner bases. For completeness we state the theorem, but we omit the proofs.

Definition 4.10.1 *Let $G \subset R$ be a finite subset of R. If the right reduction relation $\longrightarrow_{r,G}$ satisfies one of the conditions of definition 4.1.4 then G is called a* right Gröbner base. *(Since $\longrightarrow_{r,G}$ is Noetherian, by lemma 4.1.5 $\longrightarrow_{r,G}$ satisfies all conditions of definition 4.1.4.)*

Definition 4.10.2 (Right S-Polynomial) *Let $f, g \in R$, $s, t, u, v, w \in T$, such that $s = \mathrm{HT}(f)$, $t = \mathrm{HT}(g)$, $w = \mathrm{lcm}(s, t)$, $us = w$ and $vt = w$. Furthermore let $a, b \in \mathbf{K}^*$ such that $1 = \mathrm{coeff}(w, f * au)$ and $1 = \mathrm{coeff}(w, g * bv)$. Then*

$$\mathrm{RSP}(f, g) = f * au - g * bv$$

is called the right S-polynomial *of f and g.*

Note, that by proposition 3.2.5 both a and b are $\neq 0$ and so $\mathrm{HT}(\mathrm{RSP}(f, g)) < w$. Note furthermore that $\mathrm{RSP}(g, f) = -\mathrm{RSP}(f, g)$ and $\mathrm{RSP}(f, g) \in \mathrm{ideal}_r(f, g)$ respectively $\mathrm{RSP}(f, g) \in \mathrm{ideal}_r(P)$ for any set P such that $f, g \in P$.

Theorem 4.10.3 *Let G be a finite subset of R, then the following assertions are equivalent.*

1. *G is a right Gröbner base.*
2. *For all $f, g \in R$, if $f - g \in \mathrm{ideal}_r(G)$ then $f \downarrow_{r,G} g$.*

3. *For all* $f \in \text{ideal}_r(G)$, $f \longrightarrow^*_{r,G} 0$.
4. *For all* $0 \neq f \in \text{ideal}_r(G)$, $f \longrightarrow_{r,G} f'$.
5. *For all* $0 \neq f \in \text{ideal}_r(G)$, *there exists* $g \in G$ *such that* $\text{HT}(g) \mid \text{HT}(f)$.
6. *All* $0 \neq f \in \text{ideal}_r(G)$ *have a right standard representation wrt.* G.
7. *For all* $h \in H$ *with* $H = \{\text{RSP}(f,g) \mid f, g \in G, f \neq g\}$, $h \longrightarrow^*_{r,G} 0$.
8. *For all* $h \in H_b \subseteq H$, *such that* H_b *satisfies the condition (BBEC) (with respect to right S-polynomials) of lemma 4.5.8,* $h \longrightarrow^*_{r,G} 0$.

If the right ideal is contained in the left ideal, then we have the following proposition:

Proposition 4.10.4 *Let* G *be a left Gröbner base such that* $\text{ideal}_r(G) \subseteq \text{ideal}_l(G)$. *Then* G *is also a right Gröbner base.*

Proof: Let $f \in \text{ideal}_r(G)$. Since G is a left Gröbner base, every $f \in \text{ideal}_r(G) \subseteq \text{ideal}_l(G)$ is left reducible modulo G. Then f is also right reducible modulo G by proposition 4.8.3. This shows by theorem 4.10.3(4) that G is a right Gröbner base. □

4.11 Two-sided Gröbner Bases

Recall that $\text{ideal}_t(P)$ denotes the two-sided ideal generated by $P \subseteq R$. And that $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ denotes a solvable polynomial ring.

Definition 4.11.1 *Let* $I = \text{ideal}_t(P)$ *be a right ideal in* R, *generated by a finite subset* $P = \{p_1, \ldots, p_k\}$ *of* R. *Then any* $f \in I$ *has a* representation *(with respect to* P*):*

$$f = \sum_{p \in P} h_p * p * g_p = \sum_{i=1}^{k} c_i s_i * p_i * c_i' s_i',$$

where $h_p, g_p \in R$, $c_i, c_i' \in \mathbf{K}^*$, $s_i, s_i' \in T$ *and* $p_i \in P$ *for* $1 \leq i \leq k$.

Proposition 4.11.2 *Let* P *be a subset of* R. *Then the following are equivalent:*

1. $\text{ideal}_r(P) \subseteq \text{ideal}_l(P)$,
2. $\text{ideal}_l(P) = \text{ideal}_t(P)$,
3. *For all* $c \in \mathbf{K}$, $s \in T$, $p \in P$, $p * cs \in \text{ideal}_l(P)$,
4. *For all* $c \in \mathbf{K}$, $1 \leq i \leq n$, $p \in P$, $p * c \in \text{ideal}_l(P)$ *and* $p * X_i \in \text{ideal}_l(P)$.

Proof: (1) $\Longrightarrow$ (4) follows since for all $f \in P \subseteq \mathrm{ideal}_l(P)$ $f * c \in \mathrm{ideal}_r(P) \subseteq \mathrm{ideal}_l(P)$ and $f * X_i \in \mathrm{ideal}_r(P) \subseteq \mathrm{ideal}_l(P)$.

(4) $\Longrightarrow$ (3) follows by induction on the structure of s. Let $cs = c$ then $p * cs = p * c$ and by assumption $p * c \in \mathrm{ideal}_l(P)$. Let $s = X_1^{e_1} \cdot \ldots \cdot X_j^{e_j}$ with $1 \leq j \leq n$ minimal with $e_j \geq 1$. Then $p * cs = p * cX_1^{e_1} \cdot \ldots \cdot X_j^{e_j - 1} \cdot X_j$ and $p * cs = p * cX_1^{e_1} \cdot \ldots \cdot X_j^{e_j - 1} * X_j$. By induction assumption $f = p * cX_1^{e_1} \cdot \ldots \cdot X_j^{e_j - 1} \in \mathrm{ideal}_l(P)$. So f has a left representation wrt. P: $f = \sum_{i=1}^{k} c_i s_i * p_i$. Now $f * 1X_j = \sum_{i=1}^{k} c_i s_i * p_i * X_j$ and by assumption $p_i * X_j \in \mathrm{ideal}_l(P)$. This shows $p * cs = f * X_j \in \mathrm{ideal}_l(P)$ as claimed.

(3) $\Longrightarrow$ (2): clearly $\mathrm{ideal}_l(P) \subseteq \mathrm{ideal}_t(P)$. To prove the inverse inclusion let $f \in \mathrm{ideal}_t(P)$, Then f has a representation in the form $f = \sum_{i=1}^{k} c_i s_i * p_i * c_i' s_i'$. So from $p_i * c_i' s_i' \in \mathrm{ideal}_l(P)$ it follows that $c_i s_i * p_i * c_i' s_i' \in \mathrm{ideal}_l(P)$ and consequently $f \in \mathrm{ideal}_l(P)$.

(2) $\Longrightarrow$ (1) follows, since $\mathrm{ideal}_r(P) \subseteq \mathrm{ideal}_t(P) = \mathrm{ideal}_r(P)$. □

Note, that claim (4) is not a finite set of conditions if $\mathbf{K}$ is an infinite field, since c runs through all elements of $\mathbf{K}$ in $p * c$.

However if $\mathbf{K}$ is finitely generated over its center and the center of $\mathbf{K}$ lies in the centralizer of the variables of R, then the conditions (4) of proposition 4.11.2 are equivalent a (finite) set of conditions.

Lemma 4.11.3 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring. Assume furthermore, that*

1. *$\mathbf{K}$ is finitely generated by $C = \{c_1, \ldots, c_k\}$ over its center:*

$$\mathbf{K} = \{ \sum_{1=1,\ldots,k} \lambda_i c_i \ : \ \lambda_i \in \mathrm{cen}(\mathbf{K}), c_i \in \mathbf{K}, k < \infty \}.$$

2. *and $\mathrm{cen}(\mathbf{K}) \subseteq \mathrm{cen}_R(X_1, \ldots, X_n)$.*

Then the following conditions are equivalent:

1. *For all $c \in \mathbf{K}$, $1 \leq i \leq n$, $p \in P$, $p * c \in \mathrm{ideal}_l(P)$ and $p * X_i \in \mathrm{ideal}_l(P)$.*
2. *For all $c \in C$, $1 \leq i \leq n$, $p \in P$, $p * c \in \mathrm{ideal}_l(P)$ and $p * X_i \in \mathrm{ideal}_l(P)$.*

Conditions (1) are the conditions (4) of proposition 4.11.2.

Proof: (1) $\Longrightarrow$ (2) follows, since $C \subseteq \mathbf{K}$.

(2) $\Longrightarrow$ (1): We have to show $p * c \in \mathrm{ideal}_l(P)$ for all $c \in \mathbf{K}$. Since $\mathbf{K}$ is finitely generated over is center, we have $c = \sum_{1=1,\ldots,k} \lambda_i c_i$ with $\lambda_i \in \mathrm{cen}(\mathbf{K})$, $c_i \in C$ for $1 \leq i \leq k$.

Furthermore by $\mathrm{cen}(\mathbf{K}) \subseteq \mathrm{cen}_R(X_1, \ldots, X_n)$ we have

$$\begin{aligned} p * c &= p * (\sum_{1=1,\ldots,k} \lambda_i c_i) \\ &= \sum_{1=1,\ldots,k} p * (\lambda_i c_i) \\ &= \sum_{1=1,\ldots,k} \lambda_i (p * c_i). \end{aligned}$$

Now by assumption of (2) all $p * c_i \in \mathrm{ideal}_l(P)$ for $1 \leq i \leq k$, so also the sum is in the left ideal. This shows that $p * c \in \mathrm{ideal}_l(P)$ as claimed. □

We remark, that if the variables commute with the coefficients and the coefficients commute among themselves the set of conditions (4) of proposition 4.11.2 is also equivalent a (finite) set of conditions.

Lemma 4.11.4 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring. Assume furthermore, that*

> $\mathbf{K}$ *is commutative and* $\mathbf{K} \subseteq \mathrm{cen}_R(X_1, \ldots, X_n)$.

Then the following conditions are equivalent:

1. *For all $c \in \mathbf{K}$, $1 \leq i \leq n$, $p \in P$, $p * c \in \mathrm{ideal}_l(P)$ and $p * X_i \in \mathrm{ideal}_l(P)$.*
2. *For all $1 \leq i \leq n$, $p \in P$, $p * X_i \in \mathrm{ideal}_l(P)$.*

Condition (1) is the condition (4) of proposition 4.11.2.

Proof: By assumption $p * c = cp$, so clearly $p * c \in \mathrm{ideal}_l(P)$ if $cp \in \mathrm{ideal}_l(P)$. □

Lemma 4.11.5 *Let G be a left Gröbner base in R, then* $\mathrm{ideal}_l(G) = \mathrm{ideal}_t(G)$ *implies* $\mathrm{ideal}_r(G) = \mathrm{ideal}_t(G)$.

Proof: Clearly $\mathrm{ideal}_r(G) \subseteq \mathrm{ideal}_t(G)$. Then assume for a contradiction that $A = \mathrm{ideal}_t(G) \setminus \mathrm{ideal}_r(G)$ is non-empty. Let $f \in A$ be minimal with respect to the quasiordering $<$ on R. By assumption $f \in \mathrm{ideal}_l(G)$ and by theorem 4.6.2(6) f has a left standard representation $f = \sum_{i=1}^{k} c_i s_i * p_i$ with $c_i \in \mathbf{K}^*$, $s_i \in T$, $p_i \in G$ for $1 \leq i \leq k$. Now observe that by the product lemma 3.2.5 $t = \mathrm{HT}(c_i s_i * p_i) = \mathrm{HT}(p_i * c_i s_i)$. So by the automorphism assumption (for α_k) for right ideals there exists $0 \neq d_i \in \mathbf{K}$ with $\mathrm{HC}(c_i s_i * p_i) = \mathrm{HC}(p_i * d_i c_i s_i)$. Let $f_i' = c_i s_i * p_i - p_i * d_i c_i s_i$, then $\mathrm{HT}(f_i') < t \leq \mathrm{HT}(f)$. Since $p_i \in G$ we have $f_i' \in \mathrm{ideal}_t(G)$ and by assumption $f_i' \in \mathrm{ideal}_l(G)$. Furthermore by minimality of f we have $f_i' \in \mathrm{ideal}_r(G)$. This implies $c_i s_i * p_i = f_i' + p_i * d_i c_i s_i \in \mathrm{ideal}_r(G)$. So $f \in \mathrm{ideal}_r(G)$, which contradicts the choice of f and so proves the lemma. □

Recall, that $\longrightarrow$ denotes left reduction and that $\longrightarrow_r$ right reduction.

Theorem 4.11.6 *Let G be a finite subset of R. Then the following assertions are equivalent:*

1. *G is a left Gröbner base and* $\mathrm{ideal}_l(G) = \mathrm{ideal}_r(G)$,
2. *G is a left Gröbner base and* $\mathrm{ideal}_l(G) = \mathrm{ideal}_t(G)$,
3. *For all $f, g \in R$ with $f - g \in \mathrm{ideal}_t(G)$: $f \downarrow g$ modulo G.*
4. *For all $f \in R$ with $f \in \mathrm{ideal}_t(G)$: $f \longrightarrow_G^* 0$,*
5. *For all $0 \neq f \in R$ with $f \in \mathrm{ideal}_t(G)$ f is left reducible modulo G,*
6. *G is a left Gröbner base and for all $0 \neq c \in \mathbf{K}$, $1 \leq i \leq n$, $p \in G$: $p * cX_i \longrightarrow_G^* 0$,*
7. *For all $0 \neq f \in R$ with $f \in \mathrm{ideal}_t(G)$ there exists $g \in G$ such that $\mathrm{HT}(g) \mid \mathrm{HT}(f)$.*
8. *G is a right Gröbner base and* $\mathrm{ideal}_r(G) = \mathrm{ideal}_l(G)$,
9. *G is a right Gröbner base and* $\mathrm{ideal}_r(G) = \mathrm{ideal}_t(G)$,
10. *For all $f, g \in R$ with $f - g \in \mathrm{ideal}_t(G)$: $f \downarrow_r g$ modulo G.*
11. *For all $f \in R$ with $f \in \mathrm{ideal}_t(G)$: $f \longrightarrow_{r,G}^* 0$,*
12. *For all $0 \neq f \in R$ with $f \in \mathrm{ideal}_t(G)$ f is right reducible modulo G,*
13. *G is a right Gröbner base and for all $0 \neq c \in \mathbf{K}$, $1 \leq i \leq n$, $p \in G$: $cX_i * p \longrightarrow_{r,G}^* 0$,*

Proof: The equivalence between (1) and (2) follows from the foregoing proposition 4.11.5.

The equivalence between (2), (3), (4), (5) and (7) follows from theorem 4.6.2.

The equivalence between (2) and (6) follows from the proposition 4.11.2.

(8), (9), (10), (11), (12) and (13) are the right hand analogues of (1) – (6) and are equivalent by the same reasoning.

Finally (5) and (12) are equivalent by lemma 4.8.3. □

Definition 4.11.7 *A finite subset G of R is a* two-sided Gröbner base*, if it satisfies the equivalent conditions of theorem 4.11.6.*

Note again, that the conditions (6) and (13) are not finite if $\mathbf{K}$ is not finite. So in order to obtain an algorithm which computes a two-sided Gröbner base we have to restrict ourself to solvable polynomial rings $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$, where $\mathbf{K}$ is finitely generated over its center and the center of $\mathbf{K}$ is contained in the centralizer of the variables of R. Or we have to impose the restriction, that the coefficients commute with the variables.

The proof of the following theorem presents the modified Buchberger algorithm for constructing two-sided Gröbner bases.

Theorem 4.11.8 (Construction of two-sided Gröbner bases)
Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ *be a solvable polynomial ring over a computable field* $\mathbf{K}$ *and with respect to a decidable term order. Such that*

$\mathbf{K}$ *is finitely generated over its center and* $\mathrm{cen}(\mathbf{K}) \subseteq \mathrm{cen}_R(X_1, \ldots, X_n)$,

Then for any finite $F \subset R$ *one can construct a two-sided Gröbner base* G *of* $\mathrm{ideal}_t(F)$.

Proof: We give an algorithm which computes a two-sided GB in table 4.5. Let $\mathbf{K}$ be generated by $C = \{c_1, \ldots, c_k\}$ over its center.

Correctness follows e.g. from theorem 4.11.6(6) together with lemma 4.11.3 in case of condition (1) or with lemma 4.11.4 in case of condition (2). Termination follows from Dickson's lemma 3.1.1. □

Algorithm: $TSGB(F)$
Input: $F = \{f_1, \ldots, f_k\} \subseteq R$, where R satisfies conditions (1,2) above.
Output: A two-sided Gröbner base G of $\text{ideal}_t(F)$.
begin $G \leftarrow F$.
$B \leftarrow \{(f, g) \ : \ f, g \in F, f \neq g\}$.
$M \leftarrow \{f * c_j X_i \ : \ f \in F, \ 1 \leq i \leq n, \ 1 \leq j \leq k, \}$.
while $M \neq \emptyset$ **do** Let $h \in M$.
$M \leftarrow M \setminus \{h\}$.
$p \leftarrow \text{LNF}(h, G)$.
if $p \neq 0$
then $B \leftarrow B \cup \{(f', p) \ : \ f' \in G\}$.
$G \leftarrow G \cup \{p\}$ **end**.
end.
while $B \neq \emptyset$ **do** Let $(f, g) \in B$.
$B \leftarrow B \setminus \{(f, g)\}$.
$h \leftarrow \text{LSP}(f, g)$.
$p \leftarrow \text{LNF}(h, G)$.
if $p \neq 0$
then $B \leftarrow B \cup \{(f, p) \ : \ f \in G\}$.
$G \leftarrow G \cup \{p\}$. $i \leftarrow 0$.
while $i < n$ **do** $i \leftarrow i + 1$.
$j \leftarrow 0$.
while $j < k$ **do** $j \leftarrow j + 1$.
$q \leftarrow \text{LNF}(p * c_j X_i, G)$.
if $q \neq 0$
then $B \leftarrow B \cup \{(f, q) \ : \ f \in G\}$.
$G \leftarrow G \cup \{q\}$ **end**.
end.
end.
end.
end.
return(G).
end $TSGB$.

Table 4.5: Algorithm: TSGB

Chapter 5

Applications

In this chapter we discuss the 'classical' applications of Gröbner base theory, as there are elimination ideals, residue class rings, generators for syzygy modules, ideal intersection, homogeneous ideals and partial Gröbner bases. Most applications are straight forward to develop, only homogeneous ideals need some more attention, since the $*$-product does not respect homogeneity of the polynomials. Fortunately in one of the most interesting applications, namely modules over solvable polynomial rings, the homogenous methods can be used.

Finally we treat bases for subalgebras of solvable polynomial rings. We show that the tag variable method is not applicable for subalgebra base construction, since the tag variables must satisfy certain commutator relations, which in general do not define a solvable polynomial ring. As in the commutative case the bases constructed by completion procedures may no more be finite. Even worse, we could only show, that there exists a semi-decision procedure for the solution of the subalgebra membership problem.

5.1 Reduced Gröbner Bases

In this section let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring with respect to an admissible, $*$-compatible term order $<$ over a field $\mathbf{K}$.

Definition 5.1.1 *Let $P \subset R$. Recall, that P is called* monic *if for each $p \in P$,* $\mathrm{HC}(p) = 1$. *P is called* reduced left (right, two-sided) Gröbner base *if P is an autoreduced monic left (right, two-sided) Gröbner base.*

The existence of autoreduced Gröbner bases, generating a prescribed ideal, follows from 4.3.6. Dividing each polynomial by its head coefficient shows, that there exists also reduced Gröbner bases. The following lemma states that reduced Gröbner bases for a given ideal are unique relative to a given term order.

Lemma 5.1.2 *Let P, Q be a finite subsets of R such that both P and Q are reduced left Gröbner bases. If* $\mathrm{ideal}_l(P) = \mathrm{ideal}_l(Q)$ *then $P = Q$. The same holds for right and two-sided Gröbner bases.*

Proof: Let $P \triangle Q = (P \setminus Q) \cup (Q \setminus P)$. Assume for a contradiction, that $P \triangle Q \neq \emptyset$, and let $0 \neq f \in P \triangle Q$ with minimal head term, e.g. $f \in P \setminus Q$. Since both P and Q are reduced left Gröbner bases and $f \in \mathrm{ideal}_l(P) = \mathrm{ideal}_l(Q)$ we have $f \longrightarrow_Q^* 0$. So there exists $g \in Q$, (so $g \neq f$), with $\mathrm{HT}(g) \mid \mathrm{HT}(f)$. Since $g \neq f$ we see $g \in Q \setminus P$. By minimality of f we must have $\mathrm{HT}(f) = \mathrm{HT}(g)$ since otherwise $g \in P \triangle Q$ with $\mathrm{HT}(g) < \mathrm{HT}(f)$.

If $\mathrm{HT}(g) = \mathrm{HT}(f)$, then also $\mathrm{HC}(g) = 1 = \mathrm{HC}(f)$ and since $f - g \in \mathrm{ideal}_l(P)$ we have $f - g \longrightarrow_P^* 0$. This either shows $f = g$ which implies $f \in Q$ again a contradiction, or $f \neq g$; then there exists $s = \mathrm{HT}(f - g) \in T(f) \cup T(g)$ with $s < \mathrm{HT}(f) = \mathrm{HT}(g)$. But then there exists $q \in P$ with $\mathrm{HT}(q) \mid s$, which shows that f or g are reducible with respect to $q \in P \setminus \{f, g\}$. Again a contradiction to the irreducibility of P.

For right Gröbner bases the claim follows similarly and for two-sided Gröbner bases G recall that the two-sided ideal generated by G is equal to the left ideal generated by G. □

5.2 Ring and Field Extensions

A useful property to note is the stability of Gröbner bases under coefficient field extensions. By lemma 3.3.7 we can also consider extensions of solvable polynomial rings by new variables and ask how Gröbner bases behave in such extensions.

Lemma 5.2.1 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over a field $\mathbf{K}$. Let $\mathbf{L}$ be an extension field of $\mathbf{K}$ and let $R' = \mathbf{L}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring with commutator relations Q over the field $\mathbf{L}$.*

If G is a left (right) Gröbner base in R with respect to a $*$-compatible admissible term order $<$ then G is also a left (right) Gröbner base in R' with respect to $<$. If $\mathbf{L}$ is moreover commutative, then if G is a two-sided Gröbner base in R with respect to a $*$-compatible admissible term order $<$ then G is also a two-sided Gröbner base in R' with respect to $<$.

Proof: G is a left Gröbner base in R' if all S-polynomials of elements of G are left reducible to 0 wrt. G. Let $h = \mathrm{LSP}(f, g)$ for some $f \neq g \in G$ then $h \in R \subseteq R'$ and $h \longrightarrow_G^* 0$ in R and so also in R'. A similar arguments holds for right S-polynomials and right reduction. Furthermore for $c \in \mathbf{K} \subseteq \mathbf{L}$ and $1 \leq i \leq n$ we have $g * cX_i \longrightarrow_G^* 0$, either by construction in R or since $\mathbf{L}$ is commutative and by assumption the elements of $\mathbf{L} \setminus \mathbf{K}$ commute with the variables. So $g * cX_i \longrightarrow_G^* 0$ also in R'. □

Lemma 5.2.2 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$ with respect to a $*$-compatible admissible term order $<$. Let $Y_1, \ldots, Y_m$ be new variables.*

Let $R_1 = \mathbf{K}\{X_1, \ldots, X_n, Y_1, \ldots, Y_m; Q_1, Q_1'\}$ be an extension solvable polynomial ring over the field $\mathbf{K}$ with respect to a $*$-compatible admissible term order $<'$ extending $<$.

Let G be a left Gröbner base in R with respect to $<$. Then G is also a left Gröbner base in R_1 with respect to $<'$. If the $Y_1, \ldots, Y_m$ commute with the elements of $\mathbf{K}$ then also for a right (two-sided) Gröbner base G in R with respect to $<$ G is also a right (two-sided) Gröbner base in R_1 with respect to $<'$.

Proof: G is a left Gröbner base in R_1 if all S-polynomials of elements of G are left reducible to 0 wrt. G. Let $h = \mathrm{LSP}(f, g)$ for some $f \neq g \in G$ then $h \in R \subseteq R_1$ and $h \longrightarrow_G^* 0$ in R and so also in R_1. A similar arguments holds for right S-polynomials and right reduction. Furthermore under the stated restriction on the variables for Y_j, $1 \leq j \leq m$ and $0 \neq c \in K$ we have $g * Y_j * c = (g * c) * Y_j \longrightarrow_G^* 0$, in R_1 by applying the reduction in R. □

5.3 Elimination Ideals

In this section let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring.

Definition 5.3.1 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring with respect to a $*$-compatible admissible pure lexicographic ordering $<$. Let $0 \leq m \leq n$ and define*

$$R_m = \mathbf{K}\{X_1, \ldots, X_m; Q_m, Q_m'\}$$

with $R_m = R \cap \mathbf{K}[X_1, \ldots, X_m]$, $Q_m = Q \cap \mathbf{K}[X_1, \ldots, X_m]$ and $Q_m' = Q' \cap \mathbf{K}[X_1, \ldots, X_m]$. Then R_m is a solvable subring of R, since by definition of Q_m, Q_m' and p_{ij}, $p_{ai} \in R_m$ for $a \in \mathbf{K}$, $1 \leq i < j \leq m$ and by the product lemma 3.2.5, R_m is closed under $*$ multiplication, where the p_{ij}, p_{ai} are from the commutator relations Q, respectively Q'. R_m is called the m-th elimination ring.

In particular $R_0 = \mathbf{K}$ and $R_n = R$.

Lemma 5.3.2 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring with respect to a $*$-compatible admissible pure lexicographic term ordering $<$. Let $0 \leq m < n$ and let $R_m = \mathbf{K}\{X_1, \ldots, X_m; Q_m, Q_m'\}$ be an elimination ring.*

Let G be a (reduced) left Gröbner base in R, $G_m = G \cap R_m$. Then G_m is a (reduced) left Gröbner base in R_m and

$$\mathrm{ideal}_l(G) \cap R_m = \mathrm{ideal}_l(G_m),$$

where the ideal on the right hand side is taken in R_m. The claim also holds for right or two-sided ideals and (reduced right or reduced two-sided) Gröbner bases.

Proof: First we show that G_m is a (reduced) left Gröbner base in R_m. Let $f \in R_m \cap \text{ideal}_l(G)$ then $f \longrightarrow_{t,g} f'$ for some $t \in T(f)$ and some $g \in G$. Then $\text{HT}(g) \mid t$ and by the pure lexicographical order this implies $g \leq \text{HT}(g) \leq t \in R_m$ and so $g \in R_m$. So $f \longrightarrow_{t,g} f'$ for some $g \in G_m$, which shows the claim by the characterization theorem for Gröbner bases.

Next for $f \in \text{ideal}_l(G) \cap R_m$ we have $f \longrightarrow_G^* 0$ and since G_m is a left Gröbner base also $f \longrightarrow_{G_m}^* 0$. This shows $\text{ideal}_l(G) \cap R_m \subseteq \text{ideal}_l(G_m)$. The inverse inclusion follows since $G_m \subseteq G \cap R_m$ and consequently in R_m: $\text{ideal}_l(G_m) \subseteq \text{ideal}_l(G \cap R_m) \subseteq \text{ideal}_l(G) \cap R_m$. A similar argumentation establishes the claim for the right and two-sided case. □

5.4 Residue Class Rings

Let R be a ring and let I be a left (right, two-sided) ideal, then R/I denotes the left (right) R-module of the set of cosets of I together with the left (right) scalar multiplication and addition of cosets defined as usual, respectively in the two-sided case the residue class ring of R modulo the ideal I. In this section let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring.

Lemma 5.4.1 *Let G be a (reduced) left (right, two-sided) Gröbner base in R. Let*

$$B = \{s \in T \ : \ \text{HT}(g) \not| s \text{ for all } g \in G\}.$$

Let $[s]$ denote the coset (residue class) of $s \in T$ modulo $\text{ideal}_{l,r,t}(G)$ *respectively. Then*

1. *$[B] = \{[s] \ : \ s \in B\}$ is a $\mathbf{K}$-basis of the (left, right) vector space $R/\text{ideal}_{l,r,t}(G)$ respectively.*
2. *The (left, right) vector space $R/\text{ideal}_{l,r,t}(G)$ is finite dimensional iff for every $1 \leq i \leq n$ there exists $g_i \in G$ such that $\text{HT}(g_i) \in T(X_i)$.*

Proof: We show the proof for left ideals, for right and two-sided ideals a similar proof can be found.

(1) We show first that $[B]$ is left linearly independent. Assume for a contradiction, that for some pairwise different elements $[s_i]$ there exist non-zero $a_i \in K$ such that

$$\sum_{i=1}^{k} a_i [s_i] = [0].$$

$1 \leq k \leq |B|$. Then we have $f = \sum_{i=1}^{k} a_i s_i \in \text{ideal}_l(G)$. Thus f is reducible wrt. G and so some s_i is divisible by a head term of some polynomial of G. But this contradicts the choice of s_i as irreducible wrt. G.

Next we show that $[B]$ spans the left vector space $R/\text{ideal}_l(G)$. Therefore let $f \in R$ be arbitrary. Let $f' \in \mathbf{R}$ be an irreducible left reduct of f: $f \longrightarrow_G^* f'$. Let $f' =$

$\sum_{i=1}^{k} a_i s_i$, then each s_i is irreducible wrt. G. This shows each $s_i \in B$ and so $[f] = [f'] = \sum_{i=1}^{k} a_i [s_i]$. Since $R \longrightarrow R/\mathrm{ideal}_l(G)$ is surjective, we have shown, that every element $[f']$ of $R/\mathrm{ideal}_l(G)$ has a representation as linear combination wrt. $[B]$.

(2) If the condition on the head terms of the polynomials in G is fulfilled, then the total degree of each $s_i \in B$ is bounded. Since there are only finitely many terms $s_i \in T$ with bounded total degree, the number of elements of B is bounded, whence B is finite.

Conversely if for some $1 \leq i \leq n$ no $g \in G$ exists with $\mathrm{HT}(g) \in T(X_i)$, then $T(X_i) \subseteq B$. Since $T(X_i)$ is infinite, this implies that B is infinite too. □

Lemma 5.4.2 *Let $I = \mathrm{ideal}_{l,r,t}(F)$ be a left (right, two-sided) ideal in R generated by F. Then the (left, right) vector space $R/\mathrm{ideal}_{l,r,t}(F)$ respectively is finite dimensional iff for every $1 \leq i \leq n$ there exists $0 \neq f_i \in \mathrm{ideal}_{l,r,t}(F)$ respectively such that $f_i \in \mathrm{ideal}_{l,r,t}(F) \cap \mathbf{K}[X_i]$.*

Proof: We show the proof for left ideals, for right and two-sided ideals a similar proof can be found. Let B be a basis of $R/\mathrm{ideal}_l(F)$. If for some $1 \leq i \leq n$ no $0 \neq f \in \mathrm{ideal}_l(F)$ exists with $f \in \mathrm{ideal}_l(F) \cap \mathbf{K}[X_i]$, then $T(X_i) \subseteq B$. Since $T(X_i)$ is infinite, this implies that B is infinite too.

Conversely if for every $1 \leq i \leq n$, there exists $0 \neq f_i \in \mathrm{ideal}_l(F)$ such that $f_i \in \mathrm{ideal}_l(F) \cap \mathbf{K}[X_i]$ then the total degree of each $s_i \in B$ is bounded. Since there are only finitely many terms $s_i \in T$ with bounded total degree, the number of elements of B is bounded, whence B is finite. □

In chapter 6 we present an algorithm, which for a given left Gröbner base computes the univariate polynomials in the left ideal of minimal degree, provided the conditions of the lemmas are fulfilled. Here we state the existence of such an algorithm.

Lemma 5.4.3 *Let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a computable field $\mathbf{K}$ and with respect to a decidable term order. For two-sided ideals assume furthermore that*

$$\mathbf{K} \text{ is finitely generated over its center and } \mathrm{cen}(\mathbf{K}) \subseteq \mathrm{cen}_R(X_1, \ldots, X_n),$$

Let $I = \mathrm{ideal}_{l,r,t}(F)$ be a left (right, two-sided) ideal in R generated by F. Then there exists an algorithm which decides if the (left, right) vector space $R/\mathrm{ideal}_{l,r,t}(F)$ respectively is finite dimensional and if so computes for every $1 \leq i \leq n$ polynomials $0 \neq f_i \in \mathrm{ideal}_{l,r,t}(F)$ respectively such that $f_i \in \mathrm{ideal}_{l,r,t}(F) \cap \mathbf{K}[X_i]$ respectively. Moreover the algorithm determines the unique monic polynomial of minimal degree with these properties.

Proof: Let G be a left (right, two-sided) Gröbner base of $\mathrm{ideal}_{l,r,t}(F)$ respectively. Then by lemma 5.4.1 the (left, right) vector space $R/\mathrm{ideal}_{l,r,t}(F)$ respectively is finite dimensional iff for every $1 \leq i \leq n$ there exists $g_i \in G$ such that $\mathrm{HT}(g_i) \in T(X_i)$. Clearly this condition can be checked by an algorithm.

Let $[B]$ be a $\mathbf{K}$-basis of the (left, right) vector space $R/\mathrm{ideal}_{l,r,t}(G)$ respectively. Since the vector space dimension is finite, the powers $[X_i^k]$, $k \in \mathbf{N}$, must be linearly dependent. Now every $[X_i^k]$ can be represented as left (right) linear combination of the basis elements in $[B]$ using the left (right) normal form algorithm. So for $k = 0, \ldots$ a sequence of basis elements for

$$\{\ [X_i^0], [X_i^1], \ldots, [X_i^k]\ \}$$

can be computed and checked for linear dependence. Then the first linear dependence

$$0 = a_0[X_i^0] + a_1[X_i^1] \ldots + a_k[X_i^k].$$

with $a_i \in \mathbf{K}$, $a_k \neq 0$ determines a polynomial

$$f = a_0 X_i^0 + a_1 X_i^1 + \ldots + a_k X_i^k \in \mathrm{ideal}_l(F) \cap \mathbf{K}[X_i]$$

That the degree of a polynomial so constructed is minimal is clear and if we divide f by $0 \neq a_k$ then it is monic and consequently unique. $\square$

5.5 Syzygies

In this section let $R = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring with respect to a $*$-compatible admissible term order $>$.

Definition 5.5.1 *Let S be a ring. $P = \{p_1, \ldots, p_m\}$ be a finite subset of S. Let*

$$M_P = \{(h_1, \ldots, h_m) \in S^m \ :\ h_1 p_1 + \ldots + h_m p_m = 0\}.$$

M_P is called left module of syzygies for P. *The elements of M_P are called left* syzygies of P. *Right syzygies and two-sided syzygies are similarly defined as ${}_PM = \{(h_1, \ldots, h_m) \in S^m \ :\ p_1 h_1 + \ldots + p_m h_m = 0\}$ and $M_P M = \{(h_1, h_1', \ldots, h_m, h_m') \in S^{2m} \ :\ h_1 p_1 h_1' + \ldots + h_m p_m h_m' = 0\}$ respectively.*

Definition 5.5.2 *Let R be a solvable polynomial ring with respect to a $*$-compatible admissible term order. $P = \{p_1, \ldots, p_m\}$ be a monic left Gröbner base in R. For $1 \leq i < j \leq m$ let*

$$f_{ij} = \mathrm{LSP}(p_i, p_j) = a_{ij} u_{ij} * p_i - b_{ij} v_{ij} * p_j$$

be the left S-polynomials of all distinct pairs of elements of P; with $0 \neq a_{ij}, b_{ij} \in \mathbf{K}$, $u_{ij}, v_{ij} \in T$ and $\mathrm{HT}(f_{ij}) < \mathrm{HT}(u_{ij} * p_i) = u_{ij}\mathrm{HT}(p_i) = v_{ij}\mathrm{HT}(p_j) = \mathrm{HT}(v_{ij} * p_j)$.

Since $f_{ij} \in \mathrm{ideal}_l(P)$ and P is a Gröbner base we have $f_{ij} \longrightarrow_P^* 0$. This reduction determines a (standard) representation of f_{ij} from which terms belonging to the same p_i can be combined to a polynomial q_{ijk}:

$$f_{ij} = \sum_{k=1}^{m} q_{ijk} * p_k$$

with $q_{ijk} \in R$ *and* $\mathrm{HT}(q_{ijk} * p_k) = \mathrm{HT}(q_{ijk}p_k) \leq \mathrm{HT}(f_{ij})$. *Subtracting both representations of* f_{ij} *we obtain a syzygy of* P. *More precisely let* $b_{ij} = (r_{ij1}, \ldots, r_{ijm}) \in R^m$ *with*

$$r_{ijk} = \begin{cases} q_{ijk} & k \neq i, j \\ q_{ijk} - a_{ij}u_{ij} & k = i \\ q_{ijk} + b_{ij}v_{ij} & k = j \end{cases}$$

then $B = \{b_{ij} \ : \ 1 \leq i < j \leq m\}$ *is a set of left syzygies of* P.

Using right S-polynomials and right reduction we obtain a corresponding definition of certain right syzygies.

Theorem 5.5.3 *Let* R *be a solvable polynomial ring with respect to a* $*$*-compatible admissible term order. Let* G *be a monic left (right) Gröbner base in* R *and let* B *be the set of left (right) syzygies as defined in 5.5.2. Then* B *generates* M_G *(*$_GM$*) as a left (right)* R*-module.*

Proof: We discuss only the left version, the right version is obtained using the respective right representations. First we show $B \subseteq M_G$ as already claimed in the definition of B. Let $G = \{g_1, \ldots, g_m\}$ and let $b_{ij} \in B$ then

$$\begin{aligned} \sum_{k=1}^{m} r_{ijk} * g_k &= \sum_{k=1, k\neq i, k\neq j}^{m} q_{ijk} * g_k + (q_{iji} - a_{ij}u_{ij}) * g_i + (q_{ijj} + b_{ij}v_{ij}) * g_j \\ &= \sum_{k=1}^{m} q_{ijk} * g_k + (-a_{ij}u_{ij}) * g_i + (+b_{ij}v_{ij}) * g_j \\ &= f_{ij} + (-a_{ij}u_{ij}) * g_i + (+b_{ij}v_{ij}) * g_j \\ &= f_{ij} - \mathrm{LSP}(g_i, g_j) \\ &= 0 \end{aligned}$$

This shows $b_{ij} \in M_G$.

Next we show that B generates M_G. Therefore assume for a contradiction, that B does not generate M_G. Then there exists $h \in M_G$ such that $h \neq \sum_{1\leq i<j\leq m} p_{ij} * b_{ij}$ for all $p_{ij} \in R$. Let such a $h = (h_1, \ldots, h_m)$ be minimal in respect, that $t = \max\{\mathrm{HT}(h_k * g_k) \ : \ 1 \leq k \leq m\}$ is minimal (wrt. $<_T$) and $|J_t|$ with $J_t = \{k : \mathrm{HT}(h_k * g_k) = t\}$ is minimal.

Now $\sum_{k=1}^{m} h_k * g_k = 0$ and so $\sum_{k\in J_t} \mathrm{HM}(h_k * g_k) = \sum_{k\in J_t} \mathrm{HC}(h_k * g_k)t = 0$, which shows $J_t = \emptyset$ or $|J_t| \geq 2$. If $J_t = \emptyset$ then we are done, so assume $J_t \neq \emptyset$. Let $e, l \in J_t$ such that $t = \mathrm{HT}(h_e * g_e) = \mathrm{HT}(h_e)\mathrm{HT}(g_e) = \mathrm{HT}(h_l)\mathrm{HT}(g_l) = \mathrm{HT}(h_l * g_l)$. This shows $\mathrm{lcm}(\mathrm{HT}(g_e), \mathrm{HT}(g_l))w' = t$ for some $w' \in T$. Let $\mathrm{LSP}(g_e, g_l) = au * g_e - bv * g_l$.

Let $0 \neq c \in \mathbf{K}$ such that

$$\mathrm{coeff}(t, h_e * g_e) \ = \ c * \mathrm{coeff}(t, w' * au * g_e). \tag{5.1}$$

Let $b' = c * w' * b_{el}$ (by componentwise multiplication), then $b' \in M_G$ since $b_{el} \in M_G$. Then also $h' = (h'_1, \ldots, h'_m) = h - b' \in M_G$.

Let $J'_t = \{k : \mathrm{HT}(h'_k * g_k) = t\}$, then we claim that $|J'_t| < |J_t|$:

Case $k \neq e, l$: then $\mathrm{HT}(h'_k * g_k) = \mathrm{HT}(h_k * g_k - c * w' * b_{elk} * g_k) \leq \max\{\mathrm{HT}(h_k * g_k), \mathrm{HT}(c * w' * b_{elk} * g_k)\} = t$. Moreover $\{k \neq e, l : \mathrm{HT}(h'_k * g_k) = t\} = \{k \neq e, l : \mathrm{HT}(h_k * g_k) = t\}$ by the product lemma 3.2.5.

Case $k = l$: then $\mathrm{HT}(h'_l * g_l) = \mathrm{HT}(h_l * g_l - c * w' * b_{ell} * g_l) \leq \max\{\mathrm{HT}(h_l * g_l), \mathrm{HT}(c * w' * b_{ell} * g_l)\} = t$.

Case $k = e$: then $\mathrm{HT}(h'_e * g_e) = \mathrm{HT}(h_e * g_e - c * w' * b_{ele} * g_e) < t$ since by construction (5.1) $t = \mathrm{HT}(h_e * g_e) = \mathrm{HT}(c * w' * b_{ele} * g_e)$ and the coefficients of t cancel in the difference.

Now by minimality of h this shows that h' has a representation as linear combination by elements of B. But then $h = h' + b'$ has a representation as linear combination by elements of B, a contradiction. □

We are now going to prove a 'transformation' lemma for syzygies with respect to different ideal bases. The proposition was reported by [Zacharias 1978] for commutative polynomial rings and was also stated in [Apel, Lassner 1988] for enveloping algebras.

Proposition 5.5.4 *Let I be a left ideal in an unitary ring R and let $F, G \subset R$, $F = \{f_1, \ldots, f_m\}$, $G = \{g_1, \ldots, g_l\}$ such that $I = \mathrm{ideal}_l(F) = \mathrm{ideal}_l(G)$. Let $Y = (p_{ij})$ with $p_{ij} \in R$ for $1 \leq i \leq m$, $1 \leq j \leq l$ and $X = (q_{ij})$ with $q_{ij} \in R$ for $1 \leq i \leq m$, $1 \leq j \leq l$ be the transformation matrices between the F and G:*

$$\begin{aligned} f_i &= \sum_{j=1,\ldots,l} p_{ij} * g_j \quad 1 \leq i \leq m \\ g_j &= \sum_{i=1,\ldots,m} q_{ij} * f_i \quad 1 \leq j \leq l \end{aligned}$$

If we consider the F and G also as vectors and denote matrix transposition by ^{t}, we can write more compactly: $G^t = XF^t$ and $F^t = YG^t$. Let I_m denote the $m \times m$ unit matrix. Let B_G be a generator of M_G, then B_F (in block matrix representation) defined by

$$B_F = \begin{pmatrix} I_m - YX \\ B_G X \end{pmatrix}$$

is a generator of M_F. If we adopt the convention to write the multiplicants of the summands of the entries of a product matrix in the right ideal and right representation case in the reverse order, we also obtain

$${}_F B = \begin{pmatrix} I_m - YX \\ {}_G BX \end{pmatrix}.$$

Note that for a left Gröbner base G, Y can be computed during the construction of G and X can be computed by reduction of the $f_i \in F$ wrt. G.

Proof: We show first, that the rows of B_F are syzygies:

$$B_F F^t = \begin{pmatrix} I_m - YX \\ B_G X \end{pmatrix} F^t = \begin{pmatrix} I_m F^t - YXF^t \\ B_G X F^t \end{pmatrix} = \begin{pmatrix} F^t - YG^t \\ B_G G^t \end{pmatrix} = \begin{pmatrix} F^t - F^t \\ 0 \end{pmatrix} = 0.$$

Now we show, that the rows of B_F generate M_F: Let $h \in M_F$, that is $hF^t = 0$. Since $F^t = YG^t$, we have $hYG^t = 0$ which implies that $hY \in M_G$. Now B_G is a generator for M_G and so hY is a linear combination of the B_G. So there exist $a = (a_1, \ldots, a_k) \in R^k$, $k = |B_G|$ such that

$$hY = aB_G.$$

By back transformation with X we have $hYX = aB_G X$ and adding $0 = hI_m - hI_m$ on the left hand side gives $h(I_m - I_m + YX) = aB_G X$. So

$$h = h(I_m - YX) + aB_G X = a' \begin{pmatrix} I_m - YX \\ B_G X \end{pmatrix} = a' B_F$$

with $a' = (h_1, \ldots, h_m, a_1, \ldots, a_k) \in R^{m+k}$. The right case is handled similarly. □

Theorem 5.5.5 *Let R be a solvable polynomial ring with respect to a $*$-compatible admissible term order. Let $G = \{g_1, \ldots, g_m\}$ be a subset of R such that* $\mathrm{ideal}_l(G) = \mathrm{ideal}_t(G)$. *(By theorem 4.11.6 this condition is in particular fulfilled if G is a two-sided Gröbner base.) Let $M_G M$ be the set of two-sided syzygies and let $w_t = (h_1, h'_1, \ldots, h_m, h'_m) \in S^{2m}$. By proposition 4.11.2 we have* $\mathrm{ideal}_l(G) = \mathrm{ideal}_t(G)$ *if and only if* $\mathrm{ideal}_r(G) \subseteq \mathrm{ideal}_l(G)$. *So for $1 \leq i \leq m$ we have $g_i * h'_i \in \mathrm{ideal}_l(G)$ and consequently there exist $f_{ij} \in S$, for $1 \leq i, j \leq m$ such that $g_i * h'_i = \sum_{j=1}^m f_{ij} * g_j$. Let $\bar{h}_j = \sum_{i=1}^m h_i * f_{ij}$ for $1 \leq j \leq m$ and let $w_l = (\bar{h}_1, \ldots, \bar{h}_m) \in S^m$. Then*

$$w_t \in M_G M \iff w_l \in M_G.$$

Proof: Let $G = \{g_1, \ldots, g_m\}$ and let $w_t = (h_1, h'_1, \ldots, h_m, h'_m) \in M_G M$. For $1 \leq i \leq m$, $g_i * h'_i \in \mathrm{ideal}_l(G)$. So let $f_{ij} \in S$, for $1 \leq i, j \leq m$ such that $g_i * h'_i = \sum_{j=1}^m f_{ij} * g_j$. Let $\bar{h}_j = \sum_{i=1}^m h_i * f_{ij}$ for $1 \leq j \leq m$ and let $w_l = (\bar{h}_1, \ldots, \bar{h}_m) \in S^m$. Then the following equivalences hold

$$\begin{aligned} \sum_{i=1}^m h_i * g_i * h'_i = 0 &\iff \sum_{i=1}^m h_i * (\sum_{j=1}^m f_{ij} * g_j) = 0 \\ &\iff \sum_{i=1}^m \sum_{j=1}^m h_i * f_{ij} * g_j = 0 \\ &\iff \sum_{j=1}^m (\sum_{i=1}^m h_i * f_{ij}) * g_j = 0 \\ &\iff \sum_{j=1}^m \bar{h}_j * g_j = 0. \end{aligned}$$

This shows $w_l = (\bar{h}_1, \ldots, \bar{h}_m) \in M_G$ if and only if $w_t \in M_G M$. □

Gröbner bases for B_G

Let $I = \text{ideal}_l(G)$, $G = \{g_1, \ldots, g_k\}$ and let B_G be a generator of the module of syzygies M_G.

One may ask, if given $h \in R^k$, is $h \in M_G$?.

The easy solution is to compute $b = h_1 * g_1 + \ldots + h_k * g_k$ and to check if $b = 0$. An answer including more information would be to *represent h as a linear combination of the B_G*. To solve this problem we should have a reduction relation and a Gröbner base $GB(B_G)$ for the module of syzygies, such that

$$h \in M_G \iff h \longrightarrow^*_{GB(B_G)} 0.$$

Then examining the reduction steps would provide the representation of h as linear combination of the $GB(B_G)$ and hence of B_G. This problem is discussed in the subsection on partial Gröbner bases in the next section.

5.5.1 Ideal Intersection

In this subsection we are going to reformulate the ideal intersection problem as syzygy problem. We remark that the 'tag variable' method to determine the ideal intersection known for commutative polynomial rings does also apply here, since tag variables are only substituted by 0 and 1 respectively (and $0, 1 \in \text{cen}(R)$). So we do not have to setup commutator relations for the new variables in such a way, that the resulting polynomial ring might be no solvable polynomial ring.

The main fact, using syzygies, is contained in the following lemma.

Lemma 5.5.6 *Let S be a solvable polynomial ring. Let $F_1 = \{f_1, \ldots, f_r\} \subset S$, $F_2 = \{g_1, \ldots, g_s\} \subset S$ and let $F = F_1 \cup F_2$. Then*

$$\text{ideal}_l(F_1) \cap \text{ideal}_l(F_2) = \text{ideal}_l(P)$$

where $P = \{p_1, \ldots, p_k\} \subset S$ with $p_j = \sum_{i=1}^{r} h_{ij} f_{ij}$ for $1 \leq j \leq k = |B_F|$ and $(h_{1j}, \ldots, h_{rj}, h'_{1j}, \ldots, h'_{sj}) \in B_F$. The same holds for right ideals and right syzygies.

Proof: Let $I = \text{ideal}_l(F_1) \cap \text{ideal}_l(F_2)$. Furthermore let M_F be the module of syzygies of F and B_F be a set of generators for the module of syzygies of F. Then the following equations hold. $I = \text{ideal}_l(F_1) \cap \text{ideal}_l(F_2) = \{p \in S \ : \ p \in \text{ideal}_l(F_1) \text{ and } p \in \text{ideal}_l(F_2)\}$

$$\begin{aligned} &= \{p \in S \ : \ p = \sum_{i=1}^{r} h_i * f_i \text{ and } p = \sum_{i=1}^{s} h'_i * g_i, \quad h_i, h'_i \in S\} \\ &= \{p \in S \ : \ p = \sum_{i=1}^{r} h_i * f_i \text{ and } 0 = \sum_{i=1}^{r} h_i * f_i - \sum_{i=1}^{s} h'_i * g_i, \quad h_i, h'_i \in S\} \end{aligned}$$

$$
\begin{aligned}
&= \{p \in S \ : \ p = \sum_{i=1}^{r} h_i * f_i \text{ for } (h_1, \ldots, h_r, h'_1, \ldots, h'_s) \in M_F, \quad h_i, h'_i \in S\} \\
&= \{p \in S \ : \ p = \sum_{j=1}^{k} h''_j * p_j \text{ where } p_j = \sum_{i=1}^{r} h_{ij} f_i \text{ for} \\
&\quad (h_{1j}, \ldots, h_{rj}, h'_{1j}, \ldots, h'_{sj}) \in B_F, \quad h_{ij}, h'_{ij}, h''_i \in S\}.
\end{aligned}
$$

The last equality holds, since M_F is generated by B_F as left S-module:

$$(h_1, \ldots, h_r, h'_1, \ldots, h'_s) = \sum_{j=1}^{k} w_j * (h_{1j}, \ldots, h_{rj}, h'_{1j}, \ldots, h'_{sj})$$

in the notations as above and $w_j \in S$. So we have $p = \sum_{i=1}^{r} h_i * f_i = \sum_{i=1}^{r} (\sum_{j=1}^{k} w_j * h_{ij}) * f_i$ $= \sum_{j=1}^{k} w_j * (\sum_{i=1}^{r} h_{ij} * f_i) = \sum_{j=1}^{k} w_j * p_j$ as claimed. The right ideal case is proven similarly. □

Left common multiples

A special case of the ideal intersection problem is the question of the existence of left common multiples for two elements. That means, given $a, b \in S$ (solvable polynomial ring), do there exist $b', a' \in S$ such that

$$b'a = a'b \qquad (*)$$

It is known (cf. 8.2.3) that this problem is always positively solvable in a Noetherian domain. If the ideal membership problem is solvable in such a ring, then the proof of this fact can be adapted to obtain an algorithm for the computation of such left common multiples.

An other method to determine left common multiples is to consider the equation $(*)$ as an ideal intersection problem

$$Sa \cap Sb = \emptyset \quad ?$$

or directly as a syzygy problem

$$b'a - a'b = 0.$$

The last way is persued and discussed e.g. in [Apel, Lassner 1988].

5.5.2 Ideal Quotient

In this subsection we are going to define ideal left quotients and show how ideal quotients can be computed using syzygy methods.

Definition 5.5.7 *Let S be a ring. Let $I \subseteq S$ be a left (right) ideal, and let $J \subseteq S$ be a subset of S. Then the set*

$$I :_l J \ = \ \{h \in S \ : \ hg \in I \text{ for all } g \in J\}$$

is called the left ideal quotient of I by J. *The right ideal quotient of I by J is defined similarly and is denoted by $I :_r J$.*

$I :_l J$ is a left ideal of S, since for $h_1 g \in I$, $h_2 g \in I$ and $f \in S$ also $(h_1 - h_2)g \in I$ and $f h_1 g \in I$ (because I is a left ideal) for all $g \in J$. If I is a left ideal generated by a finite subset $F = \{f_1, \ldots, f_k\}$ of S, i.e. $I = \text{ideal}_l(F)$, then $\text{ideal}_l(F) :_l J = \{h \in S : \text{ exists } h_1, \ldots, h_k \in S, \text{ with } hg = h_1 * f_1 + \ldots + h_k * f_k \text{ for all } g \in J\}$. Respectively for right ideals (with F as before, $I = \text{ideal}_r(F)$) we have $\text{ideal}_r(F) :_r J = \{h \in S : \text{ exist } h_1, \ldots, h_k \in S, \text{ with } gh = f_1 * h_1 + \ldots + f_k * h_k \text{ for all } g \in J\}$.

If G is a subset of S and I is a left (right) ideal in S, then

$$I :_l G = \bigcap_{g \in G} I :_l \{g\}, \quad \text{respectively} \quad I :_r G = \bigcap_{g \in G} I :_r \{g\}.$$

This identity holds, since e.g. for left ideals $hg \in I$ for all $g \in G$ if and only if $h \in I :_l \{g\}$ for all $g \in G$. In particular for finite $G = \{g_1, \ldots, g_k\}$ we have $I :_{l,r} G = \bigcap_{i=1,\ldots,k} I :_{l,r} \{g_i\}$.

Having reduced the problem of determination of ideal quotients to $I :_{l,r} \{g\}$ (which we will simply denote by $I :_{l,r} g$) we now solve this problem using syzygies for solvable polynomial rings S.

Lemma 5.5.8 *Let S be a solvable polynomial ring. Let $I = \text{ideal}_l(F)$ be a left ideal in S generated by a finite set $F = \{f_1, \ldots, f_k\} \subseteq S$ and let $g \in S$. Let $F' = \{g, f_1, \ldots, f_k\}$ and let $B_{F'}$ be a generating set for the module of left syzygies of F'. If we let*

$$H = \{h \in S : \text{ exists } h_1, \ldots, h_k \in S, \text{ with } (h, h_1, \ldots, h_k) \in B_{F'}\},$$

then $\text{ideal}_l(H) = \text{ideal}_l(F) :_l g$. *A similar result holds for right ideals and right syzygies.*

Proof: "$\subseteq$" For $h \in H$ there exists $(h, h_1, \ldots, h_k) \in B_{F'}$, which by definition of $B_{F'}$ implies $hg + h_1 f_1 + \ldots + h_k f_k = 0$, which implies $hg = -h_1 f_1 - \ldots - h_k f_k$. So $hg \in \text{ideal}_l(F)$ and consequently $h \in \text{ideal}_l(F) :_l g$.

"$\supseteq$" For $h \in \text{ideal}_l(F) :_l g$ we get $h_1, \ldots, h_k \in S$ with $hg - h_1 f_1 - \ldots - h_k f_k = 0$ following the above way backwards. This shows that $(h, h_1, \ldots, h_k) \in M_{F'}$, the module of left syzygies of F'. Since $M_{F'}$ is generated by $B_{F'}$, i.e. every element of $M_{F'}$ is a linear combination of elements of $B_{F'}$. So we see that there exist in particular for the first component polynomials $g_1, \ldots, g_m \in S$ such that $h = g_1 h'_1 + \ldots + g_m h'_m$ with $h'_1, \ldots, h'_m \in S$ from the first component of elements from $B_{F'}$. This shows that $h'_1, \ldots, h'_m \in H$ and so $h \in \text{ideal}_l(H)$, which completes the proof. □

Since we have seen, that for solvable polynomial rings S (under the usual computability conditions) there exists an algorithm to compute a basis for the module of syzygies B_F for any finite F in S and since we can compute ideal intersections in S, we see that there is also an algorithm to compute left (right) ideal quotients for any finite set of elements of S.

5.6 Homogeneous Ideals

In this section we consider partial left (right, two-sided) Gröbner bases over solvable polynomial rings. Partial Gröbner bases are Gröbner bases, where S-polynomial reduction to zero is restricted to some degree interval. We first recall some definitions and properties about graded structures. Then we discuss partial reductions and partial Gröbner bases. The presentation is adapted from [Becker, Weispfenning 1992].

As usual let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, with respect to an admissible $*$-compatible ordering, over a field $\mathbf{K}$.

5.6.1 Gradings and Homogeneity

Definition 5.6.1 *By a* grading γ *of a polynomial ring* $\mathbf{K}[X_1, \ldots, X_n]$ *with set of terms* T *we mean a monoid homomorphism*

$$\gamma : (T, 1, \cdot) \longrightarrow (\mathbf{N}, 0, +).$$

This means that γ *is a mapping from* T *to* $\mathbf{N}$ *such that* $\gamma(1) = 0$ *and* $\gamma(s \cdot t) = \gamma(s) + \gamma(t)$ *for* $s, t \in T$. *For polynomials* $0 \neq f \in \mathbf{K}[X_1, \ldots, X_n]$ *we define the* γ*-degree of* f, *which will also be denoted by* $\gamma(f)$, *as*

$$\gamma(f) = \max\{\gamma(t) \ : \ t \in T(f)\}.$$

For solvable polynomial rings $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ *we define the* γ*-degree of* $0 \neq f \in S$ *by the* γ*-degree of* f *as element of* $\mathbf{K}[X_1, \ldots, X_n]$.

Let $S = \mathbf{K}[X_1, \ldots, X_n]$ be a polynomial ring over $\mathbf{K}$ in n variables with terms T. A grading γ on T with *weights* $a_1, \ldots, a_n \in \mathbf{N}$ can be defined as

$$\gamma(t) = \gamma(X_1^{\nu_1} \ldots X_n^{\nu_n}) = a_1\nu_1 + \ldots + a_n\nu_n,$$

where $t = X_1^{\nu_1} \ldots X_n^{\nu_n} \in T$. Moreover since γ is a homomorphism between $(T, 1, \cdot)$ and $(\mathbf{N}, 0, +)$ any grading on T arises from a linear form. In fact let $\gamma(X_i) = a_i \in \mathbf{N}$ for $1 \leq i \leq n$ then we have

$$\gamma(X_1^{\nu_1} \ldots X_n^{\nu_n}) = \gamma(X_1)\nu_1 + \ldots + \gamma(X_n)\nu_n = a_1\nu_1 + \ldots + a_n\nu_n.$$

This also shows that $s \mid t$ implies $\gamma(s) \leq \gamma(t)$ for all $s, t \in T$.

Since a solvable polynomial ring over a domain is a domain by the product lemma 3.2.5 we have:

$$\gamma(fg) = \gamma(f * g) = \gamma(f) + \gamma(g)$$

for all $0 \neq f, g \in S$. By definition of the degrees of polynomials it holds also that $\gamma(f + g) \leq \max\{\gamma(f), \gamma(g)\}$ for all $0 \neq f, g \in S$.

We call an element f of S *homogeneous of degree* d if for all $t \in T(f)$ we have $\gamma(t) = d$ and we call it *homogeneous* if for all $t, s \in T(f)$ we have $\gamma(t) = \gamma(s)$. So every polynomial f of S can be represented as a (finite) sum of its homogeneous components:

$$f = \sum_{i \in \mathbf{N}} f_i,$$

where each f_i is homogeneous of degree i. An left (right, two-sided) ideal I in S is called *homogeneous* if it is generated by homogeneous elements. One can prove, that I is homogeneous, *iff* with each $f \in I$ it contains every homogeneous component of f. Homogeneous ideals are denoted by $\text{ideal}_l^h(F)$.

A representation or standard representation of a polynomial $f \in S$ with respect to a set of homogeneous polynomials P defines a *homogeneous representation* or *homogeneous standard representation* of f with respect to P.

Note that contrary to commutative polynomial rings homogeneity is in general not preserved under the $*$-product in solvable polynomial rings.

Example 5.6.2 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over $\mathbf{K}$ in n variables with commutator relations Q and Q'. The polynomials X_j and X_i are homogeneous, but their product $X_j * X_i = c_{ij}X_iX_j + p_{ij} \in Q$ is not homogeneous if $p_{ij} \neq 0$ and $\gamma(p_{ij}) \neq \gamma(c_{ij}X_iX_j)$. Also the polynomials a and X_i are homogeneous, but $X_i * a = c_{ai}aX_i + p_{ai} \in Q'$ is not homogeneous if $p_{ai} \neq 0$ and $\gamma(p_{ai}) \neq \gamma(c_{ai}aX_i)$.*

This suggests the following definition:

Definition 5.6.3 *Let $S = (S, *, \leq)$ be solvable polynomial ring with $*$-product and term order $\leq$, then a grading γ on S is called* homogeneity compatible with $*$ *if for all $0 \neq f, g \in S$*

> *f and g homogeneous implies that $f * g$ is homogeneous.*

Example 5.6.4 *Let $S = \mathbf{K}\{X_1, \ldots, X_n, Y_1, \ldots, Y_m; Q, Q\}$ be a solvable polynomial ring over a field $\mathbf{K}$, such that the variables Y_j commute with each other and with all X_i for $1 \leq j \leq m$ and $1 \leq i \leq n$ and the commutator relations between the X's do not contain any Y's. Then we define $\gamma(X_i) = 0$ for $1 \leq i \leq n$, $\gamma(a) = 0$ for $0 \neq a \in \mathbf{K}$ and $\gamma(Y_j) = 1$ for $1 \leq j \leq m$. Then clearly $\gamma(f * g) = 0 = \gamma(f) + \gamma(g)$ for all $0 \neq f, g \in S$ which do not contain any Y's. Let $x_1y_1, x_2y_2 \in T(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ be terms with $x_1, x_2 \in T(X_1, \ldots, X_n)$ and $y_1, y_2 \in T(Y_1, \ldots, Y_m)$. Then we have $(x_1y_1) * (x_2y_2) = (x_1 * x_2)(y_1y_2)$ and for the degrees we have $\gamma((x_1y_1) * (x_2y_2)) = \gamma((x_1 * x_2)(y_1y_2)) = \gamma(x_1 * x_2) + \gamma(y_1y_2) = 0 + \gamma(y_1y_2) = \gamma(y_1) + \gamma(y_2) = \gamma(x_1y_1) + \gamma(x_2y_2)$. So the degrees of polynomials $0 \neq p, q \in S$ and the degree of their product $p * q$ depends only on the degrees of the commuting variables. This shows that if p and q are homogeneous, then their product $p * q$ is homogeneous.*

We conclude this subsection with some remarks about the relation between a grading and a term order.

Let S be (solvable) polynomial ring with term order $\leq$, then a grading γ on S is called *compatible with* $\leq$ if for all $s, t \in T$

$$\gamma(s) \leq \gamma(t) \quad \Longrightarrow \quad s \leq t.$$

Let S be (solvable) polynomial ring with term order $\leq$, and let γ be a grading on S. Then there exists a term order $\leq'$ on S such that γ is compatible with $\leq'$. To see this, define the term order $\leq'$ on T as follows:

$$s \leq' t \iff \begin{cases} \gamma(s) < \gamma(t), & \text{or} \\ \gamma(s) = \gamma(t) & \text{and } s \leq t, \end{cases}$$

where $s, t \in T$. But note that $\leq'$ may not be $*$-compatible.

5.6.2 Partial Gröbner Bases

We are new prepared to state the main results of partial Gröbner bases. Throughout this subsection let $S = (S, *, \leq)$ be solvable polynomial ring with $*$-product and $*$-compatible admissible term order $\leq$ and a grading γ on S which is homogeneity compatible with $*$ and compatible with $<$. We state the claims only for left ideals and left reduction, but using the previous subsection and the results from chapter 4 on right and two-sided ideals and right reductions it can be seen, that the claims also hold in the right and two-sided cases with the respective modifications.

Lemma 5.6.5 *Let S be solvable polynomial ring with a $*$-compatible admissible term order $\leq$ and a grading γ which is homogeneity compatible with $*$ and compatible with $\leq$. Let $\{0\} \neq P \subseteq S$ (finite), let $d \in \mathbf{N}$ and let $0 \neq f, g, p \in S$ with $\gamma(f) = d$.*

1. *If p is homogeneous and $f \longrightarrow_p g$ then $\gamma(p), \gamma(g) \leq d$. If moreover f is homogeneous, then g is homogeneous with $\gamma(g) = d$.*
2. *If all elements of P are homogeneous and $f \longrightarrow_P^* g$ then $\gamma(g) \leq d$ and $\gamma(p) \leq d$ for all $p \in P$ which occur in the reduction. If moreover f is homogeneous, then g is homogeneous with $\gamma(g) = d$.*
3. *If all elements of P are homogeneous and f has a standard representation wrt. P then $\gamma(p) \leq d$ for all $p \in P$ which occur in the standard representation of f.*

Proof: 1) By definition of the left reduction and the properties of the homogeneity respecting grading γ. 2) The claims on P follow by induction on the length of a reduction sequence. 3) Follows, since in the standard representation $f = \sum_i s_i p_i$ we have $\gamma(s_i * p_i) \leq \gamma(f)$ because $\mathrm{HT}(s_i * p_i) \leq \mathrm{HT}(f)$. $\square$

Especially for S-polynomials we note:

Lemma 5.6.6 *Let S be solvable polynomial ring with a $*$-compatible admissible term order $\leq$ and a grading γ which is homogeneity compatible with $*$ and compatible with $<$. Let $0 \neq f, g \in S$ be homogeneous and let $\mathrm{LSP}(f,g) \neq 0$. Then $\mathrm{LSP}(f,g)$ is homogeneous and*

$$\gamma(\mathrm{LSP}(f,g)) = \gamma(\mathrm{lcm}(\mathrm{HT}(f), \mathrm{HT}(g))).$$

Definition 5.6.7 *Let $F \subset S$ be a subset of a solvable polynomial ring with a $*$-compatible admissible term order $\leq$ and a grading γ which is homogeneity compatible with $*$ and compatible with $<$. For $d, e \in \mathbf{N}$ define*

$$F(d,e) = \{f \in F \ : \ d \leq \gamma(f) < e\}$$

*and $F(d,\infty) = \{f \in F \ : \ d \leq \gamma(f) \ \}$. For finite $F \subseteq S$ let the d-*restriction *of the reduction relation be defined as*

$$\longrightarrow_{d,F} \quad = \quad \longrightarrow_F \ \cap \ S(0,d)^2.$$

We are now going to give characterizations of confluent homogeneous reduction relations in a solvable polynomial ring by ideal membership tests, standard representations and S-polynomials.

Definition 5.6.8 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, with respect to an admissible $*$-compatible ordering, over a field $\mathbf{K}$ and with a grading γ on S which is homogeneity compatible with $*$ and compatible with $<$. Let $G \subset S$ be a finite subset of homogeneous polynomials of S and let $d \in \mathbf{N}$. If the left reduction relation $\longrightarrow_{d,G}$ satisfies one of the conditions of definition 4.1.4 then G is called a* left d-Gröbner base. *(Since $\longrightarrow_{d,G}$ is Noetherian, by lemma 4.1.5 $\longrightarrow_{d,G}$ satisfies all conditions of definition 4.1.4.)*

Theorem 5.6.9 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, with respect to an admissible $*$-compatible ordering, over a field $\mathbf{K}$ and with a grading γ on S which is homogeneity compatible with $*$ and compatible with $<$. Let $G \subset S$ be a finite subset of homogeneous polynomials of S and let $d \in \mathbf{N}$. Then the following assertions are equivalent.*

1. *G is a left d-Gröbner base.*
2. *For all $f, g \in S(0,d)$, if $f - g \in \mathrm{ideal}_l(G)(0,d)$ then $f \downarrow_{d,G} g$.*
3. *For all $f \in \mathrm{ideal}_l(G)(0,d)$, $f \longrightarrow^*_{d,G} 0$.*
4. *For all $0 \neq f \in \mathrm{ideal}_l(G)(0,d)$, $f \longrightarrow_{d,G} f'$.*
5. *For all $0 \neq f \in \mathrm{ideal}_l(G)(0,d)$, there exists $g \in G$ such that $\mathrm{HT}(g) \mid \mathrm{HT}(f)$.*
6. *All $f \in \mathrm{ideal}_l(G)(0,d)$ have a homogeneous standard representation wrt. G.*

7. *For all* $h \in H(0,d) = \{\mathrm{LSP}(f,g) \ : \ f,g \in G, f \neq g\}(0,d)$, $h \longrightarrow_{d,G}^* 0$.

8. *For all* $h \in H_b \subseteq H(0,d)$, *such that* H_b *satisfies the condition (BBEC) of lemma 4.5.8 for* $\longrightarrow_{d,G}$ *reduction,* $h \longrightarrow_{d,G}^* 0$.

Proof: (1) $\Longrightarrow$ (2): Let $f,g \in S$ such that $f - g \in \mathrm{ideal}_l(G)(0,d)$. Then lemma 4.4.5 together with lemma 5.6.5(2): $f \longleftrightarrow_{d,G}^* g$. By (1) $\longrightarrow_{d,G}$ has the Church-Rosser property, so $f \downarrow_{d,G} g$.

(2) $\Longrightarrow$ (3): Specialise $g = 0$ in (2).

(3) $\Longrightarrow$ (1): We show that $\longrightarrow_{d,G}$ is confluent. Let $f, f_1, f_2 \in S$ such that $f \longrightarrow_{d,G}^* f_1$ and $f \longrightarrow_{d,G}^* f_2$, that is $f_1 \longleftrightarrow_{d,G}^* f_2$. By lemma 4.4.2 together with lemma 5.6.5(2) $f_1 - f_2 \in \mathrm{ideal}_l(G)(0,d)$ and by (3) $f_1 - f_2 \longrightarrow_{d,G}^* 0$. From this by lemma 4.2.6 together with lemma 5.6.5(2) $f_1 \downarrow_{d,G} f_2$.

(3) $\Longrightarrow$ (4): By definition of $\longrightarrow_{d,G}^*$.

(4) $\Longrightarrow$ (3): Assume $0 \neq f \in \mathrm{ideal}_l(G)(0,d)$ is minimal such that not $f \longrightarrow_{d,G}^* 0$. Now by (4) $f \longrightarrow_{d,G} f'$ with $f' \in \mathrm{ideal}_l(G)(0,d)$ by lemma 4.4.2 together with lemma 5.6.5(2). However by definition of f: $f' \longrightarrow_{d,G}^* 0$ and so $f \longrightarrow_{d,G}^* 0$ a contradiction.

(5) $\Longrightarrow$ (4): By definition of left head term reduction.

(3) $\Longrightarrow$ (5): Assume $0 \neq f \in \mathrm{ideal}_l(G)(0,d)$ and let $f \longrightarrow_{d,G}^k 0$ for some $k \in \mathbf{N}$. Let $1 \leq m \leq k$ minimal, and let $g \in G$ such that $f_m \longrightarrow_{d,t,g} f_{m+1}$ where $t = \mathrm{HT}(f)$. By definition of reduction this shows that $\mathrm{HT}(g) \mid \mathrm{HT}(f)$.

(3) $\Longleftrightarrow$ (6): follows from the equivalence of claims (1) and (2) in proposition 4.5.5 together with lemma 5.6.5(2,3).

(3) $\Longleftrightarrow$ (7): follows from the equivalence of claims (1) and (2) in proposition 4.5.9 together with lemma 5.6.5(2,3).

(3) $\Longleftrightarrow$ (8): follows from the equivalence of claims (1) and (3) in proposition 4.5.9 together with lemma 5.6.5(2,3). □

The proof of the following theorem presents the Buchberger algorithm for constructing d-Gröbner bases.

Theorem 5.6.10 (Construction of left d-Gröbner bases)
Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ *be a solvable polynomial ring, with respect to an admissible* $*$*-compatible ordering, over a field* $\mathbf{K}$ *and with a grading* γ *on* S, *with given computable weights, which is homogeneity compatible with* $*$ *and compatible with* $<$. *For any finite* $F \subset S$ *of homogeneous polynomials one can construct a left (right)* d*-Gröbner base* G *of* $\mathrm{ideal}_l(F)(0,d)$ *(*$\mathrm{ideal}_r(F)(0,d)$*).*

Proof: We give an algorithm which computes a left *d-GB* in table 5.1. If we replace the left normalform algorithm LNF by the right normalform algorithm RNF we obtain the algorithm $RHGB$ for the computation of a right d-Gröbner base.

Correctness follows from theorem 5.6.9(7), since upon termination all S-polynomials in $S(0,d)$ reduce to zero. Termination follows from Dickson's lemma 3.1.1. □

Algorithm: $LHGB(F, d)$
Input: $F = \{f_1, \ldots, f_k\} \subseteq S$ with each f_i homogeneous, $d \in \mathbf{N}$.
Output: A left d-Gröbner base G of $\text{ideal}_l(F)(0, d)$.
begin $G \leftarrow F$.
$B \leftarrow \{(f, g) \ : \ f, g \in F, f \neq g\}$.
while $B \neq \emptyset$ **do** Let $(f, g) \in B$.
$B \leftarrow B \setminus \{(f, g)\}$.
if $0 \leq \gamma(\text{lcm}(\text{HT}(f), \text{HT}(g))) < d$
then $h' \leftarrow \text{LSP}(f, g)$.
$h \leftarrow \text{LNF}(h', G)$.
if $h \neq 0$
then $B \leftarrow B \cup \{(p, h) \ : \ p \in G\}$.
$G \leftarrow G \cup \{h\}$ **end**.
end.
return(G).
end $LHGB$.

Table 5.1: Algorithm: LHGB

5.7 Modules over Solvable Polynomial Rings

In this section we consider free left (right, bi) modules over solvable polynomial rings. Again we remark, that the results of this section also hold for right and bi-modules over solvable polynomial rings with the respective modifications.

Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring, with respect to an admissible $*$-compatible ordering, over a field $\mathbf{K}$. Let $M = S^m$ be a free left S-module with canonical basis $u_1, \ldots, u_m$. First we need to introduce some notation about generating sets of submodules.

Definition 5.7.1 *Let M be a R-module. We say a left (right, two-sided) sub module is* generated by a set N, $N \subseteq M$ *if it is of the form:*

$$\text{module}_l(N) = \{ \sum_{i \in \Lambda} r_i a_i \ : \ r_i \in R, a_i \in N, \Lambda \textit{ finite } \},$$

respectively $\text{module}_r(N) = \{ \sum_{i \in \Lambda} a_i r_i \ : \ r_i \in R, a_i \in N, \Lambda \textit{ finite } \}$, $\text{module}_t(N) = \{ \sum_{i \in \Lambda} r_i a_i s_i \ : \ r_i, s_i \in R, a_i \in N, \Lambda \textit{ finite } \}$. *If $N = \{a_1, \ldots, a_n\} \subseteq M$ is finite, then we write also* $\text{module}_{l,r,t}(a_1, \ldots, a_n)$ *for* $\text{module}_{l,r,t}(N)$.

We can ask the same questions as for polynomial rings: Let $N = \text{module}_l(a_1, \ldots, a_k)$ be a left submodule of M generated by $a_1, \ldots, a_k$,

given $a \in M$, is $a \in N$?
given a finite generating set of a submodule N, is there a canonical basis for N ?

The questions are answered using the method of partial Gröbner bases form section 5.6. To apply these we need some preparations.

In the commutative case, where $S = \mathbf{K}[X_1, \ldots, X_n]$, we can embed the free module $M = S^m = \text{module}(u_1, \ldots, u_m)$ into a polynomial ring with m additional variables:

$$\begin{aligned} S^m &\hookrightarrow S[Y_1, \ldots, Y_m] = \mathbf{K}[X_1, \ldots, X_n, Y_1, \ldots, Y_m] = S_{nm} \\ u_i &\mapsto Y_i \quad 1 \leq i \leq m. \end{aligned}$$

With the restriction of the multiplication in S_{nm} to polynomials from S with polynomials from S_{nm}. Moreover there are several ways to order the variables, e.g. $X_i < Y_j$, $Y_j < X_i$ or according to some 'weights'. This way has been persued e.g. by [Möller, Mora 1986]. There is also a way proposed by [Armbruster, Kredel 1986] where the embedding into an extended polynomial ring is not required.

In the non-commutative case we can also embed a solvable polynomial ring $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ into an extended solvable polynomial ring

$$S_{nm} = \mathbf{K}\{X_1, \ldots, X_n, Y_1, \ldots, Y_m; Q_{nm}, Q'_{nm}\}.$$

In this case we have to specify commutator relations between the X_i and the Y_j: the $Y's$ commute with each other and with all $X's$ and with all coefficients. By lemma 3.3.7 this ensures that S_{nm} is really a solvable polynomial ring.

Furthermore we must define a grading γ on S_{nm} such that γ is homogeneity compatible with respect to $*$. As suggested by example 5.6.4 we do this by defining $\gamma(X_i) = 0$ for $1 \leq i \leq n$, $\gamma(a) = 0$ for $0 \neq a \in \mathbf{K}$ and $\gamma(Y_j) = 1$ for $1 \leq j \leq m$. Then clearly $\gamma(f * g) = 0 = \gamma(f) + \gamma(g)$ for all $0 \neq f, g \in S$. Also for homogeneous elements $0 \neq u, v \in S_{nm}$, $u * v$ is homogeneous, since all $Y's$ commute with the $X's$ and with each other. So we have proved

Lemma 5.7.2 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$ with commutator relations Q, Q' and a $*$-compatible term order $<$. Then there exists an extended solvable polynomial ring*

$$S_{nm} = \mathbf{K}\{X_1, \ldots, X_n, Y_1, \ldots, Y_m; Q_{nm}, Q'_{nm}\}$$

and a grading γ, which is homogeneity compatible with respect to $*$, such that the free left module S^m can be embedded into S_{nm}

$$\begin{aligned} S^m &\hookrightarrow S_{nm} \\ fu_i &\mapsto fY_i \quad f \in S,\ 1 \leq i \leq m. \end{aligned}$$

More precisely we have

$$\begin{array}{rcl} S^m & \cong & \{g \in S_{nm} \ : \ \gamma(g) = 1\} \cup \{0\} \\ \sum\limits_{1 \leq i \leq m} f_i u_i & \mapsto & \sum\limits_{1 \leq i \leq m} f_i Y_i, \end{array}$$

with $\gamma(f_i) = 0$ *for* $f_i \in S$ *and* $\gamma(Y_j) = 1$ *for* $1 \leq i \leq m$.

As usual we will identify S^m with its image in S_{nm}. Now all results of partial reductions are available for free left modules over solvable polynomial rings.

In particular for finite subsets N of S^m there exists a *left submodule Gröbner base* G of module$_l(N)$, since by theorem 5.6.9 for homogeneous left ideals there exists a left partial 1-Gröbner base for N in S_{nm}.

Furthermore we can find bases for the modules of syzygies for a left submodule of S^m, since we can apply a partial version of the algorithm which generates the left module of *syzygies* for a solvable polynomial ring.

Combining all this methods, we can also find *resolutions* (free resolutions if they exist, or resolutions up to a given bound) for left modules over solvable polynomial rings by iterating the computation of modules of syzygies.

5.8 Subalgebra Bases

In this section we consider subalgebras of solvable polynomial rings. Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring, where *the coefficients commute with the variables*, with respect to an admissible $*$-compatible ordering, over a *commutative* field $\mathbf{K}$.

As with Gröbner bases in the case of ideals in S we look for canonical bases F for subalgebras R of S. That means bases, such that for a suitable reduction relation $f \in R$ if and only if $f \longrightarrow_F^* 0$.

In the commutative case there are three approaches:

1. the tag variable method of [Shannon, Sweedler 1988],
2. the term rewriting method of [Kapur, Madlener 1989] and
3. the standard representation method of [Robbiano, Sweedler 1988].

The tag variable method can be used to determine subalgebra membership by ordinary reduction (wrt. Gröbner Bases) of suitable ideals. This method can not be carried over to solvable polynomial rings since it requires, that the ordering of the tag variables can be changed deliberately. This in turn requires that the tag variables commute with the

other variables, which is not the case. More precisely an examination of the respective proofs show that for tag variables $t_1, \ldots, t_m$ a homomorphism ϕ:

$$\begin{array}{rcll} \mathbf{K}[X_1, \ldots, X_n, t_1, \ldots, t_m] & \longrightarrow & \mathbf{K}[X_1, \ldots, X_n] & \\ t_i & \mapsto & f_i & 1 \leq i \leq m \end{array}$$

is required, where $f_1, \ldots, f_m$ denote the generators of the subalgebra. Now ϕ is a homomorphism between *solvable polynomial rings* if and only if the t_i and the f_i satisfy the same commutator relations. So

$$X_j * t_i = t_i X_j + X_j * f_i - f_i * X_j \qquad (*)$$

must hold. This in general does not define commutator relations for the t_i which satisfy axioms 3.2.1(3). This follows since the term order must be choosen such that $t_i < X_j$, in turn this requires that we have $X_j * f_i - f_i * X_j < X_j$, which is obviously not guaranteed for arbitrary polynomials f_i.

However the tag variable method can still be applied to determine subalgebra bases for the center of a solvable polynomial ring, provided a set of generators for the center is given. Or it can be applied if the commutator relations $(*)$ for the newly introduced variables can be satisfied for a particular set of generators.

The latter two methods have the disadvantage, that the constructed subalgebra bases may not be finite. More precisely the existence of a finite (canonical) subalgebra base depends on the term order, and there are subalgebras which do not have finite (canonical) subalgebra bases with respect to any term order. However this methods can (to a certain extend) be carried over to solvable polynomial rings. Unfortunately the completion procedure for the construction of subalgebra bases is only finite for fixed degree bounds. It provides therefore not a decision procedure for subalgebra membership as in certain commutative cases. It provides only a semi-decision procedure, in the sense, that if some polynomial is an element of a subalgebra, then a subalgebra base can be constructed, such that this polynomial reduces to zero wrt. this base.

The methods 2 and 3 rely both on the possibility to find algorithmically positive solutions of linear diophantine equations. There are several works on this topic, but we include only one reference to [Clausen, Fortenbacher 1989] which should be generally available; for further references see also the above cited articles.

To proceed we need first some definitions, then we discuss a suitable reduction relation, standard representations and finally the subalgebra base construction.

Definition 5.8.1 *Let $F \subset S$, with $F = \{f_i\}_{i \in \Lambda}$. Let $f = f_{j_1} * f_{j_2} * \ldots * f_{j_k}$ be a word with $j_i \in \Lambda$ for $1 \leq i \leq k$. Let $J_f = \{j_i\}_{1 \leq i \leq k}$ (J_f is called an indexed set), then we define*

$$\prod_J^* F = F_J^* = \prod_{J_f}^* F = f_{j_1} * f_{j_2} * \ldots * f_{j_k}.$$

For $l \in \Lambda$ let $e_l = e_l(J_f) = |\{i \ : \ l = j_i, j_i \in J_f\}|$. Then let $\ell = |J_f|$ and let $E = E(J_f) = (e_1(J_f), \ldots, e_\ell(J_f))$ and define for the commutative product of the f_j

$$F^E = \prod F^E = \prod F^{E(J_f)} = \prod F^{E(J)} = f_1^{e_1} \cdot \ldots \cdot f_\ell^{e_\ell}.$$

As usual the empty products are defined to be 1, $F^*_\emptyset = F^\emptyset = 1$.

$\prod^*_J F$ and F^E will be our preferred notation.

Definition 5.8.2 *Let $F \subseteq S$ be a subset of S. We denote the* **K**-subalgebra of S generated by F *by*

$$\text{subalg}(F) = \mathbf{K}\langle F\rangle = \{ \sum_{i\in\Lambda'} a_i \overset{*}{\prod_{J_i}} F \ : \ a_i \in \mathbf{K}, \Lambda', J_i \text{ finite } \}.$$

We denote subalg(F) *also by* **K**-subalg(F) *if we want to indicate the dependence on the field* **K**.

In other words we have $\mathbf{K} \subseteq \text{subalg}(F)$ and if $f, g \in \text{subalg}(F)$ then $f - g$ and $f * g \in \text{subalg}(F)$.

Lemma 5.8.3 *Let F be a finite subset of S, let J be an indexed set and let $E = E(J)$. Then there exists $0 \neq c \in \mathbf{K}$ and $h \in S$ such that*

$$\overset{*}{\prod_J} F = c \prod F^E + h,$$

with $h < \text{HT}(\prod F^E)$. In particular $\text{HT}(\prod^*_J F) = \text{HT}(\prod F^E)$.

Proof: By induction on $|J|$ using the product lemma 3.2.5. □

5.8.1 Subalgebra Reduction

Recall that reduction of a term t from a polynomial f means, that a suitable multiple of some other polynomial is subtracted from f, such that the term t disappears in the difference. In case of subalgebra reduction we have the difficulty that we must represent such a term as the head term of a product of some polynomials from the subalgebra. The determination of such suitable polynomials can be done by solving systems of linear diophantine equations generated by the required relations between the exponents of the head terms of the involved polynomials. We define now a suitable reduction relation in subalgebras and discuss the decidability and computability of such a reduction relation.

Definition 5.8.4 (Subalgebra Reduction) *S be a solvable polynomial ring, let $F = \{f_i\}_{i\in\Lambda}$ be a subset of S and let $t \in T$. Then $\longrightarrow_{t,F} \subseteq \ S \times S$ denotes a* subalgebra reduction relation *if*

for $f, f' \in S$, $t \in T(f)$ with $f \longrightarrow_{t,F} f'$, there exists

1. *a finite subset $F_t \subseteq F$ with $F_t = \{f_j \ : \ 1 \leq j \leq l\}$, $l \geq 0$, and*
2. *an indexed set $J_t = \{j_i \ : \ 1 \leq j_i \leq l, i \in \Lambda\}$, such that $t = \mathrm{HT}(\prod^*_{J_t} F_t)$,*
3. *and $0 \neq a \in \mathbf{K}$ such that $\mathrm{coeff}(t, f) = a \ \mathrm{coeff}(t, \prod^*_{J_t} F_t)$*

and

$$f' = f - a \prod_{J_t}^{*} F_t.$$

By the product lemma 3.2.5 and the construction $t \notin T(f')$. If for certain f, t no such F_t exists, then t in $T(f)$ is called irreducible. *F_t is called a reduction set for t. We furthermore define*

$f \longrightarrow_F g$ if for some $t \in T$: $f \longrightarrow_{t,F} g$.

Since $a * \prod^*_{J_t} F_t \in \mathrm{subalg}(F)$ we see that $f - f' \in \mathrm{subalg}(F)$. Note furthermore that $J_t = \emptyset$ is allowed, so elements of the ground field $\mathbf{K}$ can always be reduced to zero.

Furthermore note, that *any permutation* $\pi \in \mathcal{S}_\ell$ of

$$f_{\pi(i_1)} * \ldots * f_{\pi(i_\ell)}$$

of the polynomials in the word $f_{i_1} * \ldots * f_{i_\ell}$ with $\ell = |J_t|$ could be taken for the subalgebra reduction. ($\mathcal{S}_\ell$ the group of permutations of a set of ℓ elements.)

Instead of the definition '$f \longrightarrow_{t,F} g$ if for some $t \in T$: $f \longrightarrow_{t,F} g$' it would be sufficient for our purposes, to add the restriction *such that for no $t' \in T$ with $t' > t$ $f \longrightarrow_{t',F} g$*. In other words a term t would be selected for reduction only if no t' with bigger head term could be taken. But matters will not be much more complicated, so we stay with the first definition.

The other concepts like irreducibility and the reflexive and transitive closure of the subalgebra reduction relation are defined as for (abstract) reduction relations (cf. 4.1.1). Also autoreduced bases are defined as in the ideal case.

Lemma 5.8.5 *Let S be a solvable polynomial ring, let $F = \{f_1, \ldots, f_m\}$ be a finite subset of S and let $t \in T$. Then there exists an algorithm which determines if t is subalgebra reducible with respect to F.*

Proof: Let S have n variables $X_1, \ldots, X_n$ and let $t = X_1^{e_{t1}} \ldots X_n^{e_{tn}}$. Furthermore let the set of head terms of F be $\{t_i = X_1^{e_{i1}} \ldots X_n^{e_{in}} \ : \ t_i = \mathrm{HT}(f_i), \ 1 \leq i \leq m \ \}$.

Then by definition 5.8.4 t is subalgebra reducible with respect to F if there exists natural numbers $d_1, \ldots, d_m$, such that $t = \prod_{i=1,\ldots,m} t_i^{d_i}$. Comparing exponents of equal variables this condition leads to a set of n linear diophantine equations for the d_i:

$$\sum_{i=1,\ldots,m} e_{ij} d_i = e_{tj}, \quad 1 \leq j \leq n.$$

Together with the conditions $0 \leq d_i \leq e,\ 1 \leq i \leq m$ where $e = \max\{e_{tj} \ : \ 1 \leq j \leq n\}$.

Now using an algorithm which can solve the problem of positive solutions of linear diophantine equations (see e.g. [Clausen, Fortenbacher 1989]) we can solve the subalgebra reduction problem. □

Note, that the problem for finding the d_i's $(1 \leq i \leq n)$ in the conditions in the above proof, is a special instance of the so called 'knapsack problem'. Both the 'linear diophantine equations' and the 'knapsack' problems are known to be NP-complete. For a survey on NP-complete problems see e.g. [Garey, Johnson 1978].

Lemma 5.8.6 *Let S be a solvable polynomial ring with a $*$-compatible admissible term order $<$. Then for every subset $F \subseteq S$ the reduction relation $\longrightarrow_F$ is Noetherian.*

Proof: First by definition of the reduction relation $f \longrightarrow_{t,F} g$ this says, that $g = f - a\prod_{J_t}^* F_t$ for some $0 \neq a \in \mathbf{K}$ and a reduction set F_t. Furthermore $t = \mathrm{HT}(\prod_{J_t}^* F_t)$ by the product lemma 3.2.5, so any new term in g is smaller than t in the quasi-order induced by the term order $<$. This implies that $f > g$ and then the claim follows by the well-ordering of $>$. □

Lemma 5.8.7 *Let $F \subset S$. Then for any finite subset $F' = \{f_1, \ldots, f_k\}$ of F and any finite indexed set J there exists a subalgebra reduction*

$$\prod_J^* F' \longrightarrow_{t,F} 0$$

where $t \in T$ is the head term of $\prod_J^* F'$. Moreover if F is finite, such a reduction can be found in a finite number of steps.

Proof: By proposition 3.2.5 we have $p = \prod_J^* F' = cF'^E + h = cq + h$ with $t = \mathrm{HT}(\prod_J^* F') = \mathrm{HT}(F'^E)$. This shows, that there exists a subset F_t of F and a indexed set J_t (namely $F_t = F'$ and $J_t = J$) such that t is reducible. Then with $a = 1$ we have $\mathrm{coeff}(t, p) = a * \mathrm{coeff}(t, p)$ and so $cq + h - (a * p) = 0$ as claimed.

To construct such F_t and J_t we may examine all subsets of the finite set F to determine first all finitely many possible solutions of $t = \mathrm{HT}(F'^E)$ by an algorithm for the solution of linear diophantine equations. Then we may check all J' such that $E = E(J')$ if subalgebra reduction to **zero** is possible. □

The following two important lemmas deal with properties of sums of polynomials under reductions.

Lemma 5.8.8 *Let $f, g, h, f', g', h' \in S$, $F \subset S$. If $f = g + h$ and $h \longrightarrow_F^* h'$ then there exist f' and g' such that $f \longrightarrow_F^* f'$, $g \longrightarrow_F^* g'$ and $f' = g' + h'$.*

Proof: The proof is similar to the proof of lemma 4.2.5. Let $h \longrightarrow_F^* h'$ be equal to $h \longrightarrow_F^k h'$ for some $k \in \mathbf{N}$. The proof is by induction on k. For $k = 0$ let $f' = f$ and $g' = g$.

For $k > 0$ let $h \longrightarrow_F^k h'$ be equal to $h \longrightarrow_F^{k-1} h'' \longrightarrow_{t,F} h'$. For some $t \in T(h'')$ and reduction set F_t. By induction assumption there exist polynomials f'', g'' with $f \longrightarrow_F^{k-1} f''$, $g \longrightarrow_F^{k-1} g''$ such that $f'' = g'' + h''$. Let $h' = h'' - c * p$ for $p = \prod_{J_t}^* F_t$ and some $c \in \mathbf{K}$ with $t = \mathrm{HT}(p)$ and $\mathrm{coeff}(t, h'') = c * \mathrm{coeff}(t, p)$. Let $c_1, c_2 \in \mathbf{K}$ such that $\mathrm{coeff}(t, f'') = c_1 * \mathrm{coeff}(t, p)$ and $\mathrm{coeff}(t, g'') = c_2 * \mathrm{coeff}(t, p)$ (possibly $c_1 = 0$ or $c_2 = 0$). Let $f' = f'' - c_1 * p$, $g' = g'' - c_2 * p$. This defines two reductions: $f'' \longrightarrow_{t,F} f'$ and $g'' \longrightarrow_{t,F} g'$. Since $f'' = g'' + h''$ we have $c_1 = c_2 + c$ and so $f' = g' + h'$. By construction and induction assumption $f \longrightarrow_F^{k-1} f'' \longrightarrow_{t,F} f'$ and $g \longrightarrow_F^{k-1} g'' \longrightarrow_{t,F} g'$, which proves the lemma. □

For the special case $h' = 0$ we have $f' = g'$, i. e. $f \downarrow_F g$:

Lemma 5.8.9 *Let $f, g \in S$, $F \subset S$. If $f - g \longrightarrow_F^* 0$ then $f \downarrow_F g$.*

5.8.2 Reductions and Subalgebra Membership

In this subsection we will show, that reductions do not lead outside a subalgebra and give algorithms for subalgebra reduction.

Lemma 5.8.10 *Let $f, g \in S$, $F \subset S$. If $f \longleftrightarrow_F^* g$ then $f - g \in \mathrm{subalg}(F)$.*

Proof: Let $f \longleftrightarrow_F^* g$ be equal to $f \longleftrightarrow_F^k g$ for some $k \in \mathbf{N}$. The proof is by induction on k. For $k = 0$, $g = f$ and $f - g = 0 \in \mathrm{subalg}(F)$.

For $k > 0$ let $f \longleftrightarrow_F^k g$ be equal to $f \longleftrightarrow_F^{k-1} f_{k-1} \longleftrightarrow_F f_k = g$. By induction assumption $f - f_{k-1} \in \mathrm{subalg}(F)$. Now $f_{k-1} \longrightarrow_{t,F} g$ or $g \longrightarrow_{t,F} f_{k-1}$ for some reduction set F_t. Thus $g = f_{k-1} - a * p$ or $f_{k-1} = g - a * p$ for some $a \in \mathbf{K}$ and some $t \in T$, $p = \prod_{J_t}^* F_t$. In both cases $f_{k-1} - g = \pm a * p \in \mathrm{subalg}(F)$. In combination with the induction assumption $f - g = (f - f_{k-1}) + (f_{k-1} - g) \in \mathrm{subalg}(F)$ which proves the lemma. □

Lemma 5.8.11 *Let F be a subset of S. For all $f, g \in S$, if $f - g \in \mathrm{subalg}(F)$ then there exists a subalgebra reduction $f \longleftrightarrow_F^* g$.*

Proof: If $f - g \in \mathrm{subalg}(F)$ then by definition $f - g = \sum_{i=1}^k c_i * \prod_{J_i}^* F_i$, where $c_i \in \mathbf{K}$ and $F_i \subseteq F$ for $1 \leq i \leq k$.

We prove $f \longleftrightarrow_F^* g$ by induction on k. For $k = 0$, $f = g$ and the claim is trivial. For $k > 0$ let

$$f - g' = f - (g + \sum_{i=1}^{k-1} c_i * \prod_{J_i}^* F_i) = c_k * \prod_{J_k}^* F_k.$$

By lemma 5.8.7 there exists a subalgebra reduction $c_k * \prod^*_{J_k} F_k \longrightarrow_F 0$ and by lemma 5.8.9 $f \downarrow_F g'$, that is $f \longleftrightarrow^*_F g'$. Now $g' - g = \sum_{i=1}^{k-1} c_i * \prod^*_{J_i} F_i$ and by induction assumption $g' \longleftrightarrow^*_F g$. Combining both results we get $f \longleftrightarrow^*_F g$. □

Next we give an algorithm which computes a subalgebra normal form.

Lemma 5.8.12 *Let S be a solvable polynomial ring over a computable field and with decidable term order. For any finite $F \subset S$ and any $f \in S$ one can compute $g \in S$ such that*

1. *$f \longrightarrow^*_F g$ and $f - g \in \mathrm{subalg}(F)$.*
2. *g is subalgebra irreducible modulo F.*

Proof: We give an algorithm which computes g in table 5.2.

Algorithm: $SRNF(f, F)$
Input: $f \in S$ and $F = \{f_1, \ldots, f_k\} \subseteq S$.
Output: $g \in S$ satisfying the conditions (1) and (2) of the lemma.
begin $g \leftarrow f$.
  while exists F_t, J_t for some $t \in T(g)$ **do**
    $h \leftarrow \prod^*_{J_t} F_t$.
    $c \leftarrow \mathrm{coeff}(t, h)$.
    $g \leftarrow g - c^{-1} \cdot h$.
    end.
  return(g).
end $SRNF$.

Table 5.2: Algorithm: SRNF

F_t denotes a reduction set of t and J_t denotes an indexed set such that $t = \mathrm{HT}(h) = \prod^*_{J_t} \mathrm{HT}(F)$. Partial correctness then follows from the definition of reduction.

Termination: Let $\{g_i\}_{i=0,1,\ldots}$ be the sequence of reduction vectors with $g_0 = f$. Let $g_{i+1} = g_i - a_i^{-1} \cdot h_i$ be an immediate reduct of g_i. Then we have $g_{i+1} < g_i$. Since $<$ is a well-founded quasi-order on S the reduction sequence must be finite $\{g_i\}_{i=0,1,\ldots,k}$. □

Note that the lemma is also true if F is an infinite set of polynomials such that for each $t \in T$ there are only finitely many polynomials in F with head term equal to t. This holds, since there are only finitely many divisors of a term t and consequently we need only consider the finite set of polynomials with these divisors as head terms. However this would require an algorithm which determines such a finite set of polynomials in a finite number of steps. See [Robbiano, Sweedler 1988] for further discussion of reductions by infinite sets. If there are infinitely many polynomials with the same head term, then the lemma does not hold.

As in the case of polynomial ideals, there is an algorithm to compute an autoreduced and monic subalgebra base, where the concepts are defined as in the ideal case.

Lemma 5.8.13 *Let S be a solvable polynomial ring over a computable field and with decidable term order. For any finite $F \subset S$ one can compute $G \subset S$ such that*

1. $\mathrm{subalg}(F) = \mathrm{subalg}(G)$,
2. *G is autoreduced and monic.*

Proof: As in the ideal case. □ The algorithm will be called $SRIRRSET$.

5.8.3 Standard Representations

Definition 5.8.14 *Let $F \subset S$, $f \in \mathrm{subalg}(F)$. A representation*

$$f = \sum_{i=1}^{k} c_i \prod_{J_i}^{*} F_i,$$

with $c_i \in \mathbf{K}$, $F_i \subseteq F$ (finite), for all $1 \leq i \leq k$ is called a standard representation with respect to F *if for all $1 \leq i \leq k$ the following condition is satisfied:*

$$\mathrm{HT}(\prod_{J_i}^{*} F_i) \leq \mathrm{HT}(f).$$

The next lemma shows, that standard representations are preserved under multiplication.

Lemma 5.8.15 *Let F be a subset of S, let $f \in F$ and $g = \prod_{J_g}^{*} F \in S$. If f has a standard representation wrt. F, then $g * f$ and $f * g$ have a standard representation wrt. F.*

Proof: We show only the case $g * f$. Let $f = \sum_{i=1}^{k} c_i \prod_{J_i}^{*} F_i$ be a standard representation of f, with $c_i \in \mathbf{K}$, $F_i \subseteq F$ and $\mathrm{HT}(\prod_{J_i}^{*} F_i) \leq \mathrm{HT}(f)$ for all $1 \leq i \leq k$. Then

$$g * f = \sum_{i=1}^{k} g * c_i \prod_{J_i}^{*} F_i.$$

Now the coefficients commute with the variables, so $g * c_i = c_i g$. This shows that

$$g * f = \sum_{i=1}^{k} c_i g * \prod_{J_i}^{*} F_i = \sum_{i=1}^{k} c_i \prod_{J_g}^{*} F * \prod_{J_i}^{*} F_i = \sum_{i=1}^{k} c_i \prod_{J_i'}^{*} F_i'.$$

Since $\prod_{J_g}^{*} F \leq \mathrm{HT}(g)$ and $\prod_{J_i}^{*} F_i \leq \mathrm{HT}(f)$ we have $\prod_{J_i'}^{*} F_i' \leq \mathrm{HT}(gf)$. This shows that $g * f$ has a standard representation wrt. F as claimed. The case $f * g$ is proved similarly. □

Lemma 5.8.16 *Let F be a subset of S and let $f \in S$. If $f \longrightarrow_F^* 0$, then f has a standard representation wrt. F.*

Proof: Let $f \longrightarrow_F^k 0$ for some $k \in \mathbf{N}$. We proceed by induction on k. For $k = 0$ we have $f = 0$ as standard representation.

For $k > 0$ let $f \longrightarrow_F g \longrightarrow_F^{k-1} 0$. Assume by induction assumption g has standard representation $g = \sum_{i=1}^{k} c_i \prod_{J_i}^* F_i$, with $c_i \in \mathbf{K}$, $F_i \subset F$, for all $1 \leq i \leq k$. By definition of the reduction relation there exists $t \in T(f)$ such that we have $f \longrightarrow_{t,F} g = f - c \prod_{J_t}^* F_t$ with $t = \mathrm{HT}(\prod_{J_t}^* F_t)$. So $t \leq \mathrm{HT}(f)$ and

$$f = c \prod_{J_t}^{*} F_t + \sum_{i=1}^{k} c_i \prod_{J_i}^{*} F_i$$

is a standard representation of f wrt. F. □

Lemma 5.8.17 *Let F be a subset of S, let* $\mathrm{subalg}(F)$ *be the subalgebra generated by F and let $f \in \mathrm{subalg}(F)$. If all $g \in \mathrm{subalg}(F)$ have a standard representation wrt. F then $f \longrightarrow_F^* 0$.*

Proof: Since $f \in \mathrm{subalg}(F)$, f has a standard representation wrt. F: $f = \sum_{i=1}^{k} c_i \prod_{J_i}^* F_i$, with $c_i \in \mathbf{K}$, $F_i \subseteq F$ for all $1 \leq i \leq k$. Let $I_t = I_t(f) = \{i \ : \ 1 \leq i \leq k, \mathrm{HT}(\prod_{J_i}^* F_i) = t\}$. We proceed by noetherian induction on $t = \mathrm{HT}(f)$ and $|I_t|$. Case $f = 0$, then trivially $f \longrightarrow_F^* 0$.

Case $f \neq 0$, $t = \mathrm{HT}(f)$. Now $I_t \neq \emptyset$ since the representation is standard. Pick $l \in I_t$, and define a reduction $f \longrightarrow_{t,F} g$ by $g = f - c \prod_{J_l}^* F_l$, where $0 \neq c \in \mathbf{K}$ such that $\mathrm{coeff}(t, f) = c \ \mathrm{coeff}(t, \prod_{J_l}^* F_l)$. Now $\mathrm{HT}(g) < \mathrm{HT}(f)$ or $|I_t(g)| < |I_t(f)|$, by construction $g \in \mathrm{subalg}(F)$ and so by induction assumption $g \longrightarrow_F^* 0$. Combining both reductions we obtain $f \longrightarrow_{t,F} g \longrightarrow_F^* 0$ as claimed. □

Proposition 5.8.18 *Let F be a subset of S, let* $\mathrm{subalg}(F)$ *be the subalgebra generated by F. Then the following two conditions are equivalent:*

1. *For all $f \in \mathrm{subalg}(F)$, $f \longrightarrow_F^* 0$.*
2. *All $f \in \mathrm{subalg}(F)$ have a standard representation wrt. F.*

Proof: $\Longrightarrow$ Let $f \in \mathrm{subalg}(F)$, then by assumption $f \longrightarrow_F^* 0$ and by lemma 5.8.16 f has a standard representation wrt. F.

$\Longleftarrow$ Let $f \in \mathrm{subalg}(F)$, by assumption all $g \in \mathrm{subalg}(F)$ have a standard representation wrt. F. So by lemma 5.8.17 f is reducible to zero: $f \longrightarrow_F^* 0$. □

5.8.4 Superposition Polynomials

In analogy to S-polynomials in ideal theory we define now superposition polynomials.

Definition 5.8.19 *Let F be a subset of a solvable polynomial ring S. The* superposition polynomials *are defined as*

$$\begin{aligned}\text{SUP-POL}(F) \;=\; \{\; p_1 - cp_2 \;:\; p_1, p_2 \in S,\; p_1 = \prod_{J_1}^{*} F_1, p_2 = \prod_{J_2}^{*} F_2, F_1 \subset F, F_2 \subset F,\\ \text{HT}(p_1) = \text{HT}(p_2),\; \text{HC}(p_1) = c\text{HC}(p_2), 0 \neq c \in \mathbf{K},\; \}.\end{aligned}$$

The superposition indexes *are defined as*

$$\text{SUP-IDX}(F) \;=\; \{\; (J_1, J_2) \;:\; p_1 - cp_2 \in \text{SUP-POL}(F),\; p_1 = \prod_{J_1}^{*} F_1, p_2 = \prod_{J_2}^{*} F_2 \;\}.$$

The superposition exponents *are defined as*

$$\begin{aligned}\text{SUP-EXP}(F) \;=\; \{\; (e_1, e_2) \;:\; p_1 - cp_2 \in \text{SUP-POL}(F),\; p_1 = \prod_{J_1}^{*} F_1, p_2 = \prod_{J_2}^{*} F_2,\\ e_1 = E(J_1), e_2 = E(J_2) \;\}.\end{aligned}$$

We will continue to call the elements of SUP-POL(F) S-polynomials.

Note that by construction SUP-POL(F) $\subseteq$ subalg(F). Furthermore for $p = p_1 - cp_2 \in$ SUP-POL(F) we have by construction $\text{HT}(p) < \text{HT}(p_1) = \text{HT}(p_2)$.

Lemma 5.8.20 *Let F be a subset of S, let* subalg(F) *be the subalgebra generated by F. Furthermore let $H =$* SUP-POL(F). *Then the following assertions are equivalent:*

1. *all $f \in$* subalg(F) *have a standard representation wrt. F,*
2. *all $h \in H$ have a standard representation wrt. F.*

Proof: $\Longrightarrow$ Since for $h \in H$ we have $h \in$ subalg(F), so h has a standard representation wrt. F.

$\Longleftarrow$ Let $f \in$ subalg(F) we may assume that f has a representation wrt. F:

$$f = \sum_{i=1}^{k} c_i \prod_{J_i}^{*} F_i,$$

with $c_i \in \mathbf{K}$, $F_i \subset F$ for all $1 \leq i \leq k$. Let $s = \text{HT}(f)$ and let $t \in T$ with $t = \max\{\text{HT}(\prod_{J_i}^{*} F_i) \;:\; 1 \leq i \leq k\;\}$, where the maximum is taken with respect to the term order on T. Let $I_t = \{\; i \;:\; 1 \leq i \leq k, \text{HT}(\prod_{J_i}^{*} F_i) = t > s \;\}$. We show by noetherian

induction on t and on $|I_t|$, that the representation can be transformed to a standard representation. Case $t = s$, then $|I_t| = \emptyset$ and we have already a standard representation.

Case $t > s$, then since $t \notin T(f)$, we have $|I_t| \geq 2$. Assume by induction, that the claim holds for all t' with $t > t' \geq s$ and I'_t with $|I'_t| < |I_t|$. Let $m, n \in I_t$, $m \neq n$, $I'_t = I_t \setminus \{m\}$. Then consider $c_m \prod^*_{J_m} F_m + c_n \prod^*_{J_n} F_n$ from the representation of f. Note that we have $\mathrm{HT}(\prod^*_{J_m} F_m) = \mathrm{HT}(\prod^*_{J_n} F_n) = t$. So by definition of the elements of $H = \text{SUP-POL}(F)$, there exists $0 \neq c \in \mathbf{K}$ such that $h = \prod^*_{J_m} F_m - c \prod^*_{J_n} F_n \in H$. So we can write

$$c_m \overset{*}{\prod_{J_m}} F_m + c_n \overset{*}{\prod_{J_n}} F_n = c_m(\overset{*}{\prod_{J_m}} F_m - c \overset{*}{\prod_{J_n}} F_n) + (c_n - cc_m) \overset{*}{\prod_{J_n}} F_n.$$

Now by assumption h has a standard representation wrt. F, say $h = \sum_{i'=1}^{k'} c_i \prod^*_{J'_i} F'_i$. So we can rewrite f as

$$\begin{aligned} f &= c_m \overset{*}{\prod_{J_m}} F_m + c_n \overset{*}{\prod_{J_n}} F_n + \sum_{i \neq n,m}^{k} c_i \overset{*}{\prod_{J_i}} F_i \\ &= c_m(\overset{*}{\prod_{J_m}} F_m - c \overset{*}{\prod_{J_n}} F_n) + (c_n - cc_m) \overset{*}{\prod_{J_n}} F_n + \sum_{i \neq n,m}^{k} c_i \overset{*}{\prod_{J_i}} F_i \\ &= \sum_{i'=1}^{k'} c_m c'_i \overset{*}{\prod_{J'_i}} F'_i + (c_n - cc_m) \overset{*}{\prod_{J_n}} F_n + \sum_{i \neq n,m}^{k} c_i \overset{*}{\prod_{J_i}} F_i \end{aligned}$$

For this representation we have now $|I'_t| \leq |I_t| - 1$ since $t > \mathrm{HT}(h) \geq \mathrm{HT}(\prod^*_{J'_i} F'_i)$ for $1 \leq i' \leq k'$. Now by induction assumption we can find a standard representation for f which completes the proof. □

Proposition 5.8.21 *Let F be a subset of S and let* subalg(F) *be the subalgebra generated by F. Then the following assertions are equivalent:*

1. *for all $f \in \mathrm{subalg}(F)$, $f \longrightarrow^*_F 0$,*
2. *for all $h \in H = \text{SUP-POL}(F)$, $h \longrightarrow^*_F 0$.*

Proof: (1) $\Longrightarrow$ (2): Since for $h \in H$ we have $h \in \mathrm{subalg}(F)$ and by assumption $h \longrightarrow^*_F 0$.

(2) $\Longrightarrow$ (1): By assumption all $h \in H$, $h \longrightarrow^*_F 0$. By lemma 5.8.16 this implies that all $h \in H$ have a standard representation wrt. F. By lemma 5.8.20 this implies that all $f \in \mathrm{subalg}(F)$ have a standard representation wrt. F. So by lemma 5.8.17 f is reducible to zero: $f \longrightarrow^*_F 0$. □

5.8.5 Generation of Superposition Polynomials

Define the concatenation operation '$\|$' on indexed sets J as follows:

Definition 5.8.22 *Let J_1, J_2 be indexed sets. With $J_1 = \{j_{i_1}\}_{1\leq i_1\leq k_1}$, $J_2 = \{j_{i_2}\}_{1\leq i_2\leq k_2}$ and $k_1, k_2 \in \mathbf{N}$. Then define the* concatenation *$J = J_1 \| J_2$ as $J = \{j_i\}_{1\leq i\leq k}$ with*

$$j_i = \begin{cases} j_{i_1}, & i = i_1, \quad 1 \leq i_1 \leq k_1 \\ j_{i_2}, & i = k_1 + i_2, \quad 1 \leq i_2 \leq k_2 \end{cases},$$

where $k = k_1 + k_2$.

Observe that $\|$ is associative and that $\emptyset$ is the neutral element with respect to $\|$. So the set $\mathcal{J}$ of indexed sets J forms a non-commutative monoid. In particular SUP-IDX(F) the set of superposition indexed pairs is closed under component wise concatenation and so also forms a non-commutative monoid. This suggests the following definition

Definition 5.8.23 *Let $F \subset S$. A generating set for the critical indexed sets is a subset $B =$ SUP-IDX-BASE(F) of $I =$ SUP-IDX(F), such that for every $(J_1, J_2) \in I$ there exist $(J_{1j}, J_{2j}) \in B$, $1 \leq j \leq k$ with*

$$(J_1, J_2) = (J_{11}, J_{21}) \| \ldots \| (J_{1k}, J_{2k}),$$

where $\|$ denotes the component wise concatenation.

Definition 5.8.24 *Let $F \subset S$. The* indexed generating superposition polynomials of F *are defined as*

$$\begin{aligned} \text{SUP-IDX-POL-BASE}(F) \;=\; \{\; p_1 - cp_2 \in \text{SUP-POL}(F) \;:\; p_1 = \prod_{J_1}^{*} F, p_2 = \prod_{J_2}^{*} F, \\ (J_1, J_2) \in \text{SUP-IDX-BASE}(F) \;\}. \end{aligned}$$

We will continue to call the elements of SUP-IDX-POL-BASE(F) S-polynomials.

Note that by construction SUP-IDX-POL-BASE(F) $\subseteq$ SUP-POL(F) $\subseteq$ subalg(F).

Lemma 5.8.25 *Let F be a subset of S and let* subalg(F) *be the subalgebra generated by F. If all $h \in$ SUP-IDX-POL-BASE(F) have a standard representation wrt. F, then all $g \in$ SUP-POL(F) have a standard representation wrt. F.*

Proof: Let $g \in$ SUP-POL(F). Then we have $g = p_1 - cp_2$ with $p_1 = \prod_{J_1}^{*} F_1$, $p_2 = \prod_{J_2}^{*} F_2$, HC($p_1$) $= c$ HC(p_2), HT(p_1) $=$ HT(p_2), $p_1, p_2 \in S$, $0 \neq c \in \mathbf{K}$ and $(J_1, J_2) \in$ SUP-IDX(F). Now SUP-IDX(F) is generated by $B =$ SUP-IDX-BASE(F), which means that there exists there exist $(J_{1j}, J_{2j}) \in B$, $1 \leq j \leq k$ with $(J_1, J_2) = (J_{11}, J_{21}) \| \ldots \| (J_{1k}, J_{2k})$. Let $h_j = q_{1j} - c_j q_{2j} \in$ SUP-IDX-POL-BASE(F) with $q_{1j} = \prod_{J_{1j}}^{*} F_{1j}$, $q_{2j} = \prod_{J_{2j}}^{*} F_{2j}$. By assumption each element h_j of SUP-BASE(F) has a standard representation

$$h_j = \prod_{J_{1j}}^{*} F_{1j} - c_j \prod_{J_{2j}}^{*} F_{2j} = \sum_{l_j = 1, \ldots, k_j} d_{l_j} \prod_{J_{l_j}}^{*} F_{l_j}.$$

So we write

$$\begin{aligned}
\prod^*_{J_1} F_1 &= \prod^*_{j=1,\ldots,k} (\prod^*_{J_{1j}} F_{1j}) \\
&= \prod^*_{j=1,\ldots,k} \Big(c_j \prod^*_{J_{2j}} F_{2j} + \sum_{l_j=1,\ldots,k_j} d_{l_j} \prod^*_{J_{l_j}} F_{l_j} \Big) \\
&= \prod^*_{j=1,\ldots,k} \Big(c_j \prod^*_{J_{2j}} F_{2j} \Big) + \prod^*_{j=1,\ldots,k} \Big(\sum_{l_j=1,\ldots,k_j} d_{l_j} \prod^*_{J_{l_j}} F_{l_j} \Big) \\
&= c' \prod^*_{J_2} F_2 + \sum_{l=1,\ldots,k'} d_l \prod^*_{J_l} F_l.
\end{aligned}$$

Since the term order is multiplicative on the head terms, we see that $\mathrm{HT}(\prod^*_{J_2} F_2) > \mathrm{HT}(\sum_{l=1,\ldots,k'} d_l \prod^*_{J_l} F_l)$. Furthermore since the head monomials in $\prod^*_{J_{1j}} F_{1j} - c_j \prod^*_{J_{2j}} F_{2j}$ cancel and the coefficients commute with the variables, we must also have that the head monomials in $\prod^*_{J_1} F_1 - c' \prod^*_{J_2} F_2$ cancel, which in turn implies that $c = c'$. Together with lemma 5.8.15 this shows that $\sum_{l=1,\ldots,k'} d_l \prod^*_{J_l} F$ is a standard representation of $g = \prod^*_{J_1} F_1 - c \prod^*_{J_2} F_2$, which completes the proof. □

So we get the following improvement of proposition 5.8.21.

Proposition 5.8.26 *Let F be a subset of S and let* subalg(F) *be the subalgebra generated by F. Then the following assertions are equivalent:*

1. *for all $f \in \mathrm{subalg}(F)$, $f \longrightarrow^*_F 0$,*
2. *for all $h \in H =$ SUP-IDX-POL-BASE(F), $h \longrightarrow^*_F 0$.*

Proof: (1) $\Longrightarrow$ (2): Since for $h \in H$ we have $h \in \mathrm{subalg}(F)$ and by assumption $h \longrightarrow^*_F 0$.

(2) $\Longrightarrow$ (1): By assumption for all $h \in H$, $h \longrightarrow^*_F 0$. By lemma 5.8.16 this implies that all $h \in H$ have a standard representation with respect to F. By lemma 5.8.25 this implies that all $f \in$ SUP-POL(F) have a standard representation wrt. F. and so by lemma 5.8.20 this implies that all $f \in \mathrm{subalg}(F)$ have a standard representation wrt. F. So by lemma 5.8.17 f is reducible to zero: $f \longrightarrow^*_F 0$. □

The next question is: can the set of required S-polynomials be reduced even further ? We show next, that a set of 'commutative' S-polynomials (as defined below) is not sufficient as S-polynomials.

Let $D =$ SUP-EXP(F). As for indexed sets we see that if $(e_1, e_2), (d_1, d_2) \in D$ and $\nu \in \mathbf{N}$ then also $(e_1 + d_1, e_2 + d_2) \in D$ (by component-wise addition) and $\nu\,(e_1, e_2) = (\nu e_1, \nu e_2) \in D$. This suggests the following definition

Definition 5.8.27 *Let $F \subset S$. A generating set for the superposition exponents is a subset $D =$ SUP-EXP-BASE(F) of $D' =$ SUP-EXP(F), such that for every $(e_1, e_2) \in D'$ there exist $(e_{1j}, e_{2j}) \in D$ and $\nu_j \in \mathbf{N}$ for $1 \leq j \leq k$ with*

$$(e_1, e_2) = \sum_{j=1,\ldots,k} \nu_j (e_{1j}, e_{2j}).$$

Note that by Dickson's lemma 3.1.1 D is finite if F is finite, since then $D' \subseteq \mathbf{N}^{2|F|}$ and so there exists a Dickson base for D'.

Definition 5.8.28 *The* generating superposition polynomials *are defined as*

$$\begin{aligned}\text{SUP-EXP-POL-BASE}(F) \;=\; \{\; & p_1 - cp_2 \in \text{SUP-POL}(F) \;: \\ & p_1 = \prod_{J_1}^{*} F, p_2 = \prod_{J_2}^{*} F, e_1 = E(J_1), e_2 = E(J_2), \\ & (e_1, e_2) \in \text{SUP-EXP-BASE}(F) \;\}.\end{aligned}$$

We will continue to call the elements of SUP-EXP-POL-BASE(F) S-polynomials.

Note that by construction SUP-EXP-POL-BASE(F) $\subseteq$ SUP-IDX-POL-BASE(F) $\subseteq$ SUP-POL(F) $\subseteq$ subalg(F).

The following example shows, that in general SUP-IDX-POL-BASE(F) can not be derived from SUP-EXP-POL-BASE(F).

Example 5.8.29 *Let S be a solvable polynomial ring over a field $\mathbf{K}$ and let $F \subseteq S$ with $F = \{f_1, f_2, f_3, f_4, f_5\}$. Assume that the polynomials do not commute with each other and assume furthermore that*

$$\begin{aligned}\text{HT}(f_1 * f_2) &= \text{HT}(f_4 * f_5), \\ \text{HT}(f_1) &\neq \text{HT}(f_4), \\ \text{HT}(f_2) &\neq \text{HT}(f_5),\end{aligned}$$

and that the variables in the head term of f_3 do not occur in the head terms of the other f_1, f_2, f_4, f_5. (E.g. $\text{HT}(f_1) = X_1^2X_2$, $\text{HT}(f_2) = X_1X_2^2$, $\text{HT}(f_3) = X_3$, $\text{HT}(f_4) = X_1X_2^2$, $\text{HT}(f_5) = X_1^2X_2$*)*

Then observe that for some $0 \neq c, c' \in \mathbf{K}$

$$\begin{aligned}f_1 * f_2 - cf_4 * f_5 &\in \text{SUP-EXP-POL-BASE}(F), \\ f_1 * f_3 * f_2 - c'f_4 * f_3 * f_5 &\notin \text{SUP-EXP-POL-BASE}(F), \\ f_1 * f_3 * f_2 - c'f_4 * f_3 * f_5 &\in \text{SUP-IDX-POL-BASE}(F).\end{aligned}$$

The second statement follows, since neither

$$\begin{aligned}f_1 - c''f_4 &\in \text{SUP-IDX-POL-BASE}(F), \quad \text{nor} \\ f_2 - c'''f_5 &\in \text{SUP-IDX-POL-BASE}(F)\end{aligned}$$

for some $0 \neq c'', c''' \in \mathbf{K}$ by construction of the head terms. This shows that there exist elements of SUP-IDX-POL-BASE(F) *which can not be written as $*$ products of elements of* SUP-EXP-POL-BASE(F).

Using some notations from section 5.6 on graded structures, we obtain a construction method for SUP-POL(F) up to any predescribed degree $d \in \mathbf{N}$. We will globaly assume, that for a graded solvable polynomial ring S over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$ and with corresponding compatible grading γ, the

grading γ has positive weights only.

This ensures that for any $d \in \mathbf{N}$, the set of terms $\{t \in T \ : \ \gamma(t) \leq d\}$ with degree less than or equal to d is *finite*. The finiteness of this set of terms is essential in the termination proofs of the algorithms in the sequel.

Definition 5.8.30 *Let S be a graded solvable polynomial ring over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$ and with corresponding compatible grading γ. Let F be a subset of S. Then for $d \in \mathbf{N}$*

$$\begin{aligned} \text{SUP-POL}(F,d) \ = \ \{ \ p_1 - cp_2 \ : \ p_1, p_2 \in S, \ p_1 = \prod_{J_1}^{*} F_1, p_2 = \prod_{J_2}^{*} F_2, F_1 \subset F, F_2 \subset F, \\ \text{HT}(p_1) = \text{HT}(p_2), \ \text{HC}(p_1) = c\text{HC}(p_2), 0 \neq c \in \mathbf{K}, \\ \gamma(\text{HT}(p_1)) = \gamma(\text{HT}(p_2)) \leq d \ \}. \end{aligned}$$

In slight abuse of notation the elements of SUP-POL(F,d) *will be called S-polynomials of degree d. (They are actually of degree less than or equal to d as polynomials.) Furthermore let*

$$\text{SUP-IDX-POL-BASE}(F,d) = \text{SUP-IDX-POL-BASE}(F) \cap \text{SUP-POL}(F,d).$$

Lemma 5.8.31 *Let S be a graded solvable polynomial ring over a computable field $\mathbf{K}$, with respect to a $*$-compatible admissible and decidable term order $<$ and with corresponding compatible grading γ, with given positive weights. Let $F = \{f_1, \ldots, f_m\}$ be a finite subset of S. Then there exists an algorithm which determines* SUP-POL(F,d) *and an algorithm which determines* SUP-IDX-POL-BASE(F,d) *for any $d \in \mathbf{N}$.*

Proof: The algorithm description for the construction of SUP-POL(F,d) is given in table 5.3.

In the very first step the elements of $\mathbf{K}$ are removed from F. This ensures that $\gamma(f) \geq 1$ for any $f \in F$. This is required to ensure termination and is no loss of generality since elements of $\mathbf{K}$ are not necessary to construct S-polynomals. The construction is performed in two steps

1. determination of SUP-EXP-BASE(F),
2. multiplication of elements of F with elements of SUP-EXP-POL-BASE(F), up to degree d for the product and permutation of all polynomials in the corresponding non-commutative product.

Algorithm: $SUPPOL(F, d)$
Input: $F = \{f_1, \ldots, f_m\} \subseteq S$. $d \in \mathbf{N}$.
Output: $H = \text{SUP-POL}(F, d)$ a set of S-polynomials up to degree d.
begin $F \leftarrow F \setminus \mathbf{K}$.
$D \leftarrow$ a generating set for the solution of the systems of linear
diophantine equations from the head terms of the elements of F.
$D' \leftarrow \{\ (e_1, e_2) \in D\ :\ \gamma(\text{HT}(\prod F^{e_1})) \leq d\ \}$.
$D \leftarrow D'$.
repeat
$D'' \leftarrow \{\ (e_1', e_2') = (e_1 + (\delta_{ij}), e_2 + (\delta_{ij}))\ :\ (e_1, e_2) \in D',$
$\gamma(\text{HT}(f_i \prod F^{e_1})) \leq d,\ f_i \in F, i = 1, \ldots, m\ \}$.
$D \leftarrow D \cup D''$. $D' \leftarrow D''$.
until $D'' = \emptyset$.
$J \leftarrow \bigcup_{(e_1,e_2)\in D} \{\ (J_1, J_2)\ :\ E(J_1) = e_1, E(J_2) = e_2\ \}$. J_1, J_2 indexed sets.
$H \leftarrow \emptyset$.
while $J \neq \emptyset$ **do** Let $(J_1, J_2) \in J$.
$J \leftarrow J \setminus \{(J_1, J_2)\}$.
$p_1 \leftarrow \prod^*_{J_1} F$. $p_2 \leftarrow \prod^*_{J_2} F$.
$c \leftarrow \text{HC}(p_1)\text{HC}(p_2)^{-1}$.
$H \leftarrow H \cup \{\ p_1 - cp_2\ \}$.
end.
return(H).
end $SUPPOL$.

Table 5.3: Algorithm: SUPPOL

The *first* step (the second statement in algorithm 5.3) is solved as follows:

Let S have n variables $X_1, \ldots, X_n$. Furthermore let the set of head terms of F be $\{t_i = X_1^{e_{i1}} \ldots X_n^{e_{in}} \ : \ t_i = \mathrm{HT}(f_i), f_i \in F, \ 1 \leq i \leq m \ \}$. Then by definition 5.8.19 $(e_1, e_2) \in \text{SUP-EXP}(F)$ if there exist natural numbers $\mu_1, \ldots, \mu_{m_1}$ and $\nu_1, \ldots, \nu_{m_2}$, such that $\prod_{i=1,\ldots,m_1} t_i^{\mu_i} = \prod_{i=1,\ldots,m_1} t_i^{\nu_i}$. Comparing exponents of equal variables this condition leads to a system of n linear diophantine equations for the μ_i, ν_i:

$$\sum_{i=1,\ldots,m_1} e_{ij}\mu_i - \sum_{i=1,\ldots,m_2} d_{ij}\nu_i = 0, \qquad 1 \leq j \leq n.$$

Together with the conditions $0 \leq \mu_i, \ 1 \leq i \leq m_1, \ 0 \leq \nu_i, \ 1 \leq i \leq m_2$. Now using an algorithm which can solve the problem of finding positive solutions of linear diophantine equations (see e.g. [Clausen, Fortenbacher 1989]) we can solve the S-polynomial construction problem.

The *second* step (the remaining statements in algorithm 5.3) is solved as follows:

Let $H = \text{SUP-EXP-POL-BASE}(F) \cap \text{SUP-POL}(F, d)$. Now for every $p \in H$, as long as $fp \in \text{SUP-POL}(F, d)$ for some $f \in F \setminus \mathbf{K}$ let $H = H \cup \{fp\}$. Since (also by assumtion on the grading γ) the degree of fp increases at least by 1 this process must terminate. This implies, that H is finite.

Let $H' = \emptyset$. Now for all $p \in H$, $p = p_1 - cp_2$ with $p_1 = \prod F^{e_1}, p_2 = \prod F^{e_2}$, and for all permutations of the indexed sets J_1, J_2 with $e_1 = E(J_1)$ and $e_2 = E(J_2)$ let $p' = \prod_{J_1}^* F - c' \prod_{J_2}^* F$ ($0 \neq c' \in \mathbf{K}$ appropriate) and let $H' = H' \cup \{p'\}$. Since H is finite and the set of all permuations of finite sets is finite, this process terminates and so H' is also finite. Clearly $H' \subseteq \text{SUP-POL}(F, d)$. Also every $p \in \text{SUP-POL}(F, d)$ is of the form $p = p_1 - cp_2$ with $\gamma(\mathrm{HT}(p_1)) \leq d$ and $p_1 = \prod_{J_1}^* F$ with J_1 determined as in the construction of the elements of H'. Finally, since $\text{SUP-POL}(F, d)$ is finite, the subset $\text{SUP-IDX-POL-BASE}(F, d)$ can be determined by examination of the elements of $\text{SUP-POL}(F, d)$. □

5.8.6 Subalgebra Gröbner Bases

We are going to give characterizations of confluent subalgebra reduction relations in a solvable polynomial ring by subalgebra membership tests, standard representations and S-polynomials.

Definition 5.8.32 *Let S be a solvable polynomial ring over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$. Let $F \subset S$ be a subset of S. If the subalgebra reduction relation $\longrightarrow_F$ satisfies one of the conditions of definition 4.1.4 then F is called a* subalgebra Gröbner base. *(Since $\longrightarrow_F$ is Noetherian, by lemma 4.1.5 $\longrightarrow_F$ satisfies all conditions of definition 4.1.4.)*

Theorem 5.8.33 *Let S be a solvable polynomial ring over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$. Let F be a subset of S, then the following assertions are equivalent.*

1. *F is a subalgebra Gröbner base.*
2. *For all $f, g \in S$, if $f - g \in \mathrm{subalg}(F)$ then $f \downarrow_F g$.*
3. *For all $f \in \mathrm{subalg}(F)$, $f \longrightarrow_F^* 0$.*
4. *For all $0 \neq f \in \mathrm{subalg}(F)$, $f \longrightarrow_F f'$.*
5. *For all $0 \neq f \in \mathrm{subalg}(F)$, there exists a reduction set $F_t \subset F$ such that $t = \mathrm{HT}(f)$.*
6. *For all $f \in \mathrm{subalg}(F)$, f has a standard representation wrt. F.*
7. *For all $h \in H = \mathrm{SUP\text{-}POL\text{-}BASE}(F)$, $h \longrightarrow_F^* 0$.*
8. *For all $h \in H = \mathrm{SUP\text{-}IDX\text{-}POL\text{-}BASE}(F)$, $h \longrightarrow_F^* 0$.*

Proof: (1) $\Longrightarrow$ (2): Let $f, g \in S$ such that $f - g \in \mathrm{subalg}(F)$. Then lemma 5.8.11: $f \longleftrightarrow_F^* g$. By (1) $\longrightarrow_F$ has the Church-Rosser property, so $f \downarrow_F g$.

(2) $\Longrightarrow$ (3): Specialise $g = 0$ in (2).

(3) $\Longrightarrow$ (1): We show that $\longrightarrow_F$ is confluent. Let $f, f_1, f_2 \in S$ such that $f \longrightarrow_F^* f_1$ and $f \longrightarrow_F^* f_2$, that is $f_1 \longleftrightarrow_F^* f_2$. By lemma 5.8.10 $f_1 - f_2 \in \mathrm{subalg}(F)$ and by (3) $f_1 - f_2 \longrightarrow_F^* 0$. From this by lemma 5.8.9 $f_1 \downarrow_F f_2$.

(3) $\Longrightarrow$ (4): By definition of $\longrightarrow_F^*$.

(4) $\Longrightarrow$ (3): Assume $0 \neq f \in \mathrm{subalg}(F)$ is minimal such that not $f \longrightarrow_F^* 0$. Now by (4) $f \longrightarrow_F f'$ with $f' \in \mathrm{subalg}(F)$ by lemma 5.8.10. However by definition of f: $f' \longrightarrow_F^* 0$ and so $f \longrightarrow_F^* 0$ a contradiction.

(5) $\Longrightarrow$ (4): By definition of subalgebra reduction.

(3) $\Longrightarrow$ (5): Assume $0 \neq f \in \mathrm{subalg}(F)$ and let $f \longrightarrow_F^k 0$ for some $k \in \mathbf{N}$. Let $1 \leq m \leq k$ minimal, and let $g \in F$ such that $f_m \longrightarrow_{t,F} f_{m+1}$ where $t = \mathrm{HT}(f)$. By definition of reduction this shows that there exists a reduction set F_t.

(3) $\Longleftrightarrow$ (6): follows from the equivalence of claims (1) and (2) in proposition 5.8.18.

(3) $\Longleftrightarrow$ (7): follows from the equivalence of claims (1) and (2) in proposition 5.8.21.

(3) $\Longleftrightarrow$ (8): follows from the equivalence of claims (1) and (2) in proposition 5.8.26. □

The proof of the following theorem presents the completion procedure (Buchberger algorithm) for constructing subalgebra Gröbner bases. It is known, that even in in the case of commutative polynomial rings the completion procedure may not terminate (for a certain term order $<$ or even for all term orders $<$). For examples see [Robbiano, Sweedler 1988]. In case of subalgebras of solvable polynomial rings, the completion procedure terminates for every degree bound $d \in \mathbf{N}$. However there is in general also no criterion for which d the constructed subalgebra bases are in fact a subalgebra Gröbner base.

Theorem 5.8.34 (Construction of subalgebra Gröbner bases) *Let S be a graded solvable polynomial ring over a computable field $\mathbf{K}$, with respect to a $*$-compatible admissible and decidable term order $<$ and with corresponding compatible grading γ, with given positive weights. For any finite $F \subset S$ and any degree $d \in \mathbf{N}$ one can construct a subalgebra base G_d, such that*

1. $G = \bigcup_{d \in \mathbf{N}} G_d$ *is a subalgebra Gröbner base of* $\mathrm{subalg}(F)$ *and*
2. $\mathrm{subalg}(F) = \mathrm{subalg}(G_d) = \mathrm{subalg}(G)$.

Proof: We give an algorithm which computes a subalgebra base G_d in table 5.4.

Algorithm: $SRB(F, d)$
Input: $F = \{f_1, \ldots, f_k\} \subseteq S$. $d \in \mathbf{N}$.
Output: A subalgebra base G_d such that $G = \bigcup_{d \in \mathbf{N}} G_d$ is a subalgebra Gröbner base of $\mathrm{subalg}(F)$.
begin $G_d \leftarrow F$. $d' \leftarrow 0$.
  repeat $d' \leftarrow d' + 1$.
    $B \leftarrow \mathrm{SUPPOL}(G_d, d')$.
    $C \leftarrow \emptyset$.
    while $B \neq \emptyset$ **do** Let $h' \in B$.
      $B \leftarrow B \setminus \{h'\}$.
      $h \leftarrow \mathrm{SRNF}(h', G_d)$.
      if $h \neq 0$ **then** $C \leftarrow C \cup \{h\}$. **end**.
      end.
    $G_d \leftarrow G_d \cup C$
    until $d' \geq d$.
  return(G_d).
end SRB.

Table 5.4: Algorithm: SRB

The construction of $\mathrm{SUPPOL}(G_d, d')$ in the algorithm can be done by lemma 5.8.31. Note that the construction of $\mathrm{SUPPOL}(G_d, d')$ should be optimized to avoid multiple generation and reduction of the same S-polynomials.

Termination follows since (by assumption on the grading γ) the set of terms occuring in polynomials in $B = \text{SUP-POL}(G_d, d')$ is finite for every $d' \in \mathbf{N}$ (and arbitrary G_d) and the **repeat**-loop is executed exactly d times.

To show partial correctness, observe that by construction $\mathrm{subalg}(F) = \mathrm{subalg}(G_d) = \mathrm{subalg}(G)$. To show that G is a subalgebra Gröbner base of $\mathrm{subalg}(F)$ we use theorem 5.8.33(7), i.e. we show, that all S-polynomials reduce to zero. Let $G = \bigcup_{d \in \mathbf{N}} G_d$ and let $p \in \text{SUP-POL}(G)$. By definition of G we have $p \in \text{SUP-POL}(G_d)$ for some $d \in \mathbf{N}$. If the

algorithm terminates for that d, then all S-polynomials $p_1 - cp_2 \in \text{SUP-POL}(G_d)$ with $\gamma(\text{HT}(p_1)) \leq d$ reduce to zero. In particular $p \longrightarrow^*_{G_d} 0$ and consequently $p \longrightarrow^*_G 0$. □

Theorem 5.8.35 (Subalgebra Membership) *Let S be a graded solvable polynomial ring over a computable field $\mathbf{K}$, with respect to a $*$-compatible admissible and decidable term order $<$ and with corresponding compatible grading γ, with given positive weights. Let $F \subset S$ be a finite subset of S and let $f \in S$. If $f \in \text{subalg}(F)$ then one can construct $d \in \mathbf{N}$ and a subalgebra base G_d, such that*

$$f \longrightarrow^*_{G_d} 0.$$

Proof: We give an algorithm which computes $d \in \mathbf{N}$ and G_d, if $f \in \text{subalg}(F)$ in table 5.5.

Algorithm: $SRMEM(f, F)$
Input: $f \in S$. $F = \{f_1, \ldots, f_k\} \subseteq S$.
Output: (d, G_d) if $f \in \text{subalg}(F)$, with $d \in \mathbf{N}$ and
a subalgebra base G_d such that $f \longrightarrow^*_{G_d} 0$.
Otherwise the algorithm probably does not terminate.
begin $d \leftarrow -1$.
repeat $d \leftarrow d + 1$.
$G_d \leftarrow SRB(F, d)$.
$f' \leftarrow SRNF(f, G_d)$.
until $f' = 0$.
return$((d, G_d))$.
end $SRMEM$.

Table 5.5: Algorithm: SRMEM

To prove termination if $f \in \text{subalg}(F)$ observe that by 5.8.34 there exists a subalgebra Gröbner base G of F. Then $f \longrightarrow^*_G 0$. Since only finitely many polynomials are used during this reduction we have $f \longrightarrow^*_{G'} 0$ for a finite subset G' of G. Since G' is finite and $G = \bigcup G_d$, there exists $d \in \mathbf{N}$ such that $G' \subset G_d = SRB(F, d)$ and $f \longrightarrow^*_{G_d} 0$. By this we must have $f' = 0$ at some time in the **repeat**-loop and the algorithm terminates. Partial correctness follows also from these arguments. □

The case $f \notin \text{subalg}(F)$ can not be decided by these methods, except for special F's (see 5.8.40).

Lemma 5.8.36 *Let S be a graded solvable polynomial ring over a computable field $\mathbf{K}$, with respect to a $*$-compatible admissible and decidable term order $<$ and with corresponding compatible grading γ, with given positive weights. For any finite $F \subset S$ and any degree $d \in \mathbf{N}$ one can construct a monic autoreduced subalgebra base G_d, such that*

1. $G = \bigcup_{d \in \mathbf{N}} G_d$ *is a subalgebra Gröbner base of* subalg(F) *and*
2. subalg(F) = subalg(G_d) = subalg(G).

Proof: We give an algorithm which computes a monic autoreduced subalgebra base G_d in table 5.6.

Algorithm: $SRIRRB(F, d)$
Input: $F = \{f_1, \ldots, f_k\} \subseteq S$. $d \in \mathbf{N}$.
Output: A monic autoreduced subalgebra base G_d such that $G = \bigcup_{d \in \mathbf{N}} G_d$ is a subalgebra Gröbner base of subalg(F).
begin $H' \leftarrow SRB(F, d)$.
repeat $H \leftarrow H'$.
$C \leftarrow SRIRRSET(H)$.
$H' \leftarrow SRB(C, d)$.
until $H = H'$.
return(H).
end $SRIRRB$.

Table 5.6: Algorithm: SRIRRB

To prove termination of algorithm $SRIRRB$, observe that, starting with a finite set F, at each iteration in the **repeat**-loop the sets C and H' stay finite by construction of $SRIRRSET$ and SRB. Assume for a contradiction that the algorithm does not terminate. Consider the elements of H during each iteration of the loop written as rows in a scheme, where the zeroes are also kept in the respective row. Then by the **repeat**-condition there exist a column in the scheme with an infinite sequence of polynomials $p \longrightarrow_{H_1} \ldots \longrightarrow_{H_n} p_n \longrightarrow_{H_{n+1}} \ldots$. But this contradicts the Noetherianity of the reduction relation and so proves termination.

Partial correctness of algorithm $SRIRRB$ follows from the condition subalg(F) = subalg(H) = subalg$(SBR(F, d))$ = subalg$(SBR(SRIRRSET(H), d)))$ as invariant of the **repeat**-loop. Then upon termination H is both monic autoreduced and every S-polynomial in SUP-POL(H, d) reduces to zero wrt. H. The other claims of the lemma follow as in theorem 5.8.34. □

Proposition 5.8.37 *Let S be a solvable polynomial ring over a field* $\mathbf{K}$*, with respect to a $*$-compatible admissible term order $<$. For any finite $F \subset S$ of S and any degree $d \in \mathbf{N}$, there exists a monic autoreduced subalgebra base G_d, such that*

1. *there exists a set G' which is a monic autoreduced subalgebra Gröbner base of* subalg(F) *and*
2. subalg(F) = subalg(G_d) = subalg(G').

Proof: For $d \in \mathbf{N}$ let $G_d = SRIRRB(F, d)$, if $\mathbf{K}$ is not computable or $<$ is not decidable, then the algorithm still provides the existence of such a set G_d. Assume the polynomials in the G_d's are arranged in sequences

$$\begin{array}{rcl} G_d & : & p_{d,1}, \ldots, p_{d,n_d} \\ \vdots & & \vdots \\ G_{d'} & : & p_{d',1}, \ldots, p_{d',n_{d'}}. \end{array}$$

The arrangement should have the following properties: $n_d \leq n_{d'}$ and for all $1 \leq j \leq n_d$ and any $d' \geq d$ we have

$$p_{d',j} = \begin{cases} 0 & \text{or} \\ p_{d'',j} & d \leq d'' \leq d', \quad \text{or} \\ p & p_{d,j} \longrightarrow^*_{G_{d'}} p. \end{cases}$$

Observe that for $d \in \mathbf{N}$ and for $1 \leq j \leq n_d$ the sequence $p_{m,j}$ for $m \in \mathbf{N}$ cannot be an infinite decreasing reduction sequence because of the Noetherianity of the subalgebra reduction relation.

Define G' to be the union over the sequence $\{p_k\}_{k \in \mathbf{N}}$ of the irreducible polynomials in the respective columns $\{p_{m,k}\}_{m \in \mathbf{N}}$. Let $G = \bigcup_{d \in \mathbf{N}} G_d$ then since each p_k of G' appears in some row it is an element of some G_d, so $G' \subseteq G$. To show that G' is a subalgebra Gröbner base of subalg(F) we show, that all S-polynomials reduce to zero. Let $p \in$ SUP-POL(G'). By definition of $G' \subseteq G$ we have $p \in$ SUP-POL(F, d) for some $d \in \mathbf{N}$. By 5.8.34 all S-polynomials $p \in$ SUP-POL(F, d) reduce to zero wrt. G_d. For $d \in \mathbf{N}$ let $\bar{G}_d = G_d \cap G'$. By construction of G' there exists $d' \geq d$, such that p reduces to zero wrt. $\bar{G}_{d'}$. This shows that p reduces to zero wrt. G'. By construction every $p \in G'$ is irreducible wrt. $G' \setminus \{p\}$ which shows that G' is autoreduced. $\square$

Theorem 5.8.38 *Let S be a solvable polynomial ring over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$. Let F be a finite subset of S. Let G be a monic autoreduced subalgebra Gröbner base of the subalgebra generated by F. Then G is uniquely determined by S, $<$ and F.*

Proof: Let H, G be subsets of S such that both H and G are monic autoreduced subalgebra Gröbner bases with respect to a given term order $<$ and with subalg$(H) =$ subalg(G). Assume $G \neq \{1\} \neq H$, since otherwise trivially $H = G$. Let $G \triangle H = (G \setminus H) \cup (H \setminus G)$. Assume for a contradiction, that $G \triangle H \neq \emptyset$, and let $0 \neq f \in H \triangle G$ with minimal head term, e.g let $f \in H \setminus G$. Since both H and G are reduced subalgebra Gröbner bases and $f \in$ subalg$(H) =$ subalg(G) we have $f \longrightarrow^*_G 0$.

By this there exists $Q = \{q_1, \ldots, q_k\} \subset G$, $k \in \mathbf{N}$, with HT$(\prod^*_J Q) =$ HT(f) for some indexed set J. By assumption on f we have $f \neq q_i$ and so $q_i \in G \setminus H$ for $i = 1, \ldots, k$. Let $g = \prod^*_J Q$, then $g \in$ subalg$(G) =$ subalg(H) and $g \longrightarrow^*_H 0$. Furthermore for every $q \in Q$ we have $q \in$ subalg$(G) =$ subalg(H) and $q \longrightarrow^*_H 0$. Assume wlog. $1 \notin Q$, then if $|Q| > 1$

or $|J| > 1$ or if $k > 1$ then $\mathrm{HT}(f)$ is reducible wrt. $H \setminus \{f\}$, a contradiction. This shows that $Q = \{g\}$ and $k = 1$, and $\mathrm{HT}(g) = \mathrm{HT}(f)$ and also $\mathrm{HC}(g) = 1 = \mathrm{HC}(f)$.

Since $f - g \in \mathrm{subalg}(H)$ we have $f - g \longrightarrow_H^* 0$. This either shows $f = g$ which implies $f \in G$ again a contradiction, or $f \neq g$ then there exists $s = \mathrm{HT}(f - g) \in T(f) \cup T(g)$ with $s < \mathrm{HT}(f) = \mathrm{HT}(g)$. But then there exists $P' \in H$ and a indexed set J' with $\mathrm{HT}(\prod_{J'}^* P') = s$, which shows that f or p are reducible with respect to $P' \subseteq H \setminus \{f, g\}$. Again a contradiction to the irreducibility of H. □

Corollary 5.8.39 *Let S be a solvable polynomial ring over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$. Let F be a finite subset of S. If $F = \{f\}$ then $G = \{\mathrm{HC}(f)^{-1} f\}$ is the unique monic autoreduced subalgebra Gröbner base of the subalgebra generated by F.*

Proof: Every S-polynomial of SUP-POL($\{f\}$) is identically zero. □

Corollary 5.8.40 *Let S be a solvable polynomial ring over a field $\mathbf{K}$, with respect to a $*$-compatible admissible term order $<$. Let F be a subset of S. If $\mathrm{subalg}(F) = \mathrm{subalg}(G)$ where $G = \{g\}$ is a one element set. Then then $G' = \{\mathrm{HC}(g)^{-1} g\}$ is the unique monic autoreduced subalgebra Gröbner base of the subalgebra generated by F.*

Proof: Clearly G' is a monic autoreduced subalgebra Gröbner base. Let F' be the unique monic autoreduced subalgebra Gröbner base of the subalgebra generated by F. Then, since $\mathrm{subalg}(F') = \mathrm{subalg}(F) = \mathrm{subalg}(G) = \mathrm{subalg}(G')$, by uniqueness $F' = G'$. □

Proof: For a direct proof of this claim without using uniqueness of reduced subalgebra Gröbner bases one may argue as follows: Let $F = \{f_1, \ldots, f_k\}$ and $G = \{g\}$ with $\mathrm{subalg}(F) = \mathrm{subalg}(G)$. From $F \subseteq \mathrm{subalg}(G) = \mathbf{K}\langle g \rangle = \mathbf{K}[g]$ it follows, that every $f \in F$ has a representation as univariate 'commutative' polynomial in g. Since $\mathbf{K}[g]$ is an Euclidean domain, the gcd of the elements from F exists. Let $f' = \gcd(F)$. It follows, that f' is a multiple of g and since $g \in \mathrm{subalg}(F)$ also g is a multiple of f'. So up to a factor from $\mathbf{K}$, g equals f'. □

Notes: The last two corollaries provide criterions whether for some $d \in \mathbf{N}$

$$G_d = G' \subseteq \bigcup_{d' \in \mathbf{N}} G_{d'}$$

where $G_d = SRIRRB(F, d)$ from algorithm 5.6 and G' is the reduced subalgebra Gröbner base of F.

1. If $G_d = \{g\}$ for some $d \in \mathbf{N}$, then G_d is already a reduced subalgebra Gröbner base.
2. If it is known a priori, that $\mathrm{subalg}(F) = \mathrm{subalg}(\{g\})$ for some $g \in S$, then there exists $d \in \mathbf{N}$ such that $G_d = \{g\}$. Then G_d is the reduced subalgebra Gröbner base. In this case there exists also a decision procedure for subalgebra membership: compute $G_d = \{g\}$, then $f \in \mathrm{subalg}(F)$ iff $f \in \mathrm{subalg}(G_d)$ iff $f \longrightarrow_{G_d}^* 0$.

It is also clear, that if there exists a *finite* reduced subalgebra Gröbner base G, then the sequence of bases G_d produced by the algorithm will be equal to G for some $d \in \mathbf{N}$. However this does not provide a termination criterion, since the fact that G_d is a reduced subalgebra Gröbner base of F can not be tested. It would be necessary to test whether $G_d = G' \subseteq \bigcup_{d' \in \mathbf{N}} G_{d'}$ or not in a finite number of steps.

Further questions are: under what conditions finite subalgebra bases do exist. In the case of commutative polynomial rings a result from [Robbiano, Sweedler 1988] says, that *if there exists a finitely generated subalgebra, which is integral over the graded subalgebra under consideration, then there exists a* finite *subalgebra Gröbner base (of the later).* It is open if such a result also holds in case of solvable polynomial rings.

Chapter 6

Implementation

In this chapter we present implemented optimized algorithms (and prove their correctness) for computation in solvable polynomial rings: non-commutative products with respect to commutator relations, left reduction, left (and two-sided) Gröbner bases and elements in the center. The algorithms are stated in the frame work of [Kandri-Rody, Weispfenning 1988] where a solvable polynomial ring is an ordinary commutative polynomial ring $\mathbf{R} = \mathbf{K}[X_1, \ldots, X_n]$ equipped with a new non-commutative multiplication $*$. The field $\mathbf{K}$ is assumed to be commutative and the elements of $\mathbf{K}$ are assumed to commute with the indeterminates $X_1, \ldots, X_n$. The algorithms are implemented for the case, that the coefficient field $\mathbf{K}$ is the field of rational numbers. Examples computed in the MAS system are included.

6.1 Introduction

One of the most important tools in the algorithmic theory of commutative polynomial rings is the calculation of Gröbner bases by Buchbergers algorithm [Buchberger 1965]. Several implementations of this algorithm have been reported, to mention a few [Winkler *et. al.* 1985], [Gebauer, Kredel 1984], [Böge *et. al.* 1986].

Algorithms for Gröbner Bases in enveloping algebras of finite dimensional Lie algebras have been studied by Apel and Lassner [Apel, Lassner 1988]. An implementation of their algorithms was given by Petermann and Apel [Petermann, Apel 1988] in the LOGLAN system [Bartol *et. al.* 1983].

In physics there are several computer algebra systems and application programs dealing with non-commutative multiplications. Most of them use the method of matching and term rewriting to manipulate non-commutative expressions. (e.g. in REDUCE with the so called 'LET-rules'.) Special systems have been designed to handle the tremendous sets of millions of terms generated during rewriting. As reference we only note the journal of 'Symbolic Computation' [J. Symb. Comp. 1986-], where many overview articles on this topic can be found.

In this chapter we describe an implementation of the theory of Kandri-Rody and Weispfenning in the MAS system [Kredel 1990]. The implementation is based on an earlier implementation in the ALDES / SAC-2 system [Collins, Loos 1980]. We include correctness proofs for the algorithms and show examples computed with the MAS system. To improve efficiency of the non-commutative product algorithm, we introduce the method of incrementaly computed relation tables.

We proof the correctness of the presented algorithms using the definitions and propositions of [Kandri-Rody, Weispfenning 1988] and of chapters 3 and 4. In order to make the chapter mostly self contained we summarize most required items. For a full statement of all propositions and theorems together with the proofs see the chapters 3 and 4.

The correctness proof of the $*$-product algorithm is different to the existence proof in the original article, since the induction hypothesis does not coincide with the recursive application of the $*$-algorithm. Also the original $*$-algorithm can not be modified to include the relation table handling with out making the proof invalid.

We prove furthermore the correctness of the reduction (normal form) and the set reduction algorithm. The computation of a reduced Gröbner base can be made more efficient when the Gröbner base properties are exploited. Finally a more efficient version of the algorithm for the computation of two-sided GB's is presented.

In more detail the main implementation design considerations can be summarized as follows:

1. The algebras of solvable type are commutative polynomial rings equipped with a non-commutative product. In the implementation we use an ordinary commutative (distributive) polynomial representation. Actually the Distributive Polynomial System of [Gebauer, Kredel 1983], implemented in the SAC-2 / ALDES system is used.

2. The non-commutative product $*$ is defined via relations, which are elements of a free associative algebra. These relations are implemented as triples (u, v, p) of (commutative) terms u, v and a (commutative) polynomial p, such that $u * v = p$.

3. Besides the defining relations between variables of the non-commutative product, many relations between powers of variables and terms are derived during computation. These relations are incrementaly stored in a so called relation table. Each time a product of terms is to be computed the relation table is scanned for an applicable relation. Missing relations are treated as if the two variables commute.

   An implementation of a product algorithm without the relation table method was given by [Apel, Klaus 1990]. An example with timings is presented in table 6.6 and shows the need for our method.

4. Once the non-commutative product algorithm is available, the input-routines for polynomials can be setup to respect the order of variables in the products.

5. For the rest of the Gröbner base algorithms the existing ones from the Buchberger algorithm system of [Gebauer, Kredel 1984] could be used as a starting point. However great care was inorder to assure that for no algorithm the input parameters where commuted. Furthermore the non-commutative product modifies the leading coefficients of the product polynomials, so the order of computation steps had also to be checked.

6. It is known, that not all criteria derived by Buchberger for the detection of unnecessary reductions are valid in the non-commutative case. The valid criterion BBEC is implemented as in the commutative case and leads to similar improvements of computing time.

7. The computation of two-sided Gröbner bases uses an improved way of including right variable multiples during the main Buchberger loop instead of iterating the left Buchberger algorithm on bases given by right variable multiples of polynomials.

The plan of this chapter is as follows: In section 2 we will summarize some of the theory and discuss some fundamental representation issues. In section 3 we will discuss the non-commutative product algorithm, the relation table handling and some examples for the complexity of the $*$-product. Section 4 will contain the reduction algorithm for polynomials and sets of polynomials, section 5 the S-polynom computation and the Buchberger algorithm for left-sided Gröbner bases and section 6 will consist of a description of the two-sided Gröbner base construction. In section 7 a small example showing the usage of the algorithms in the MAS system is discussed. In the final section 8 we will summarize some computing times and draw some conclusions.

6.2 Polynomial Rings of Solvable Type

In this section we first summarize some of the theory of chapter 3 and 4 adapted to the current situation.

Recall that a solvable polynomial ring is an ordinary commutative polynomial ring $\mathbf{R} = \mathbf{K}[X_1, \ldots, X_n]$ equipped with a new non-commutative multiplication $*$. The field $\mathbf{K}$ is assumed to be commutative and to commute with the indeterminates $X_1, \ldots, X_n$. The set T of terms (power-products of indeterminates) is supposed to be linearly ordered by an admissible order $<_T$. Recall the axioms of solvable polynomial rings 3.2.1 adapted for the current situation:

Axioms 6.2.1 *$R = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ denotes a polynomial ring of solvable type over a field $\mathbf{K}$ in the variables $\{X_1, \ldots, X_n\}$ for a fixed term order $<_T$ if the following axioms are satisfied:*

1. *$(R, 0, 1, +, -, *, <)$ is an associative ring extending $\mathbf{K}$ and with admissible term order $<$.*

2. *(a) For all* $a, b \in \mathbf{K}$, $t \in T(X_1, \ldots, X_n)$, $a * b * t = a * (bt) = (a \cdot b) \cdot t = abt$.
   (b) For all $1 \leq i \leq n$, $s \in T(X_1, \ldots, X_i)$, $t \in T(X_i, \ldots, X_n)$, $s * t = st$.

3. *For all* $1 \leq i < j \leq n$ *there exist* $0 \neq c_{ij} \in \mathbf{K}$, $p_{ij} \in R$ *such that*

$$X_j * X_i = c_{ji} X_i X_j + p_{ij}$$

   and $p_{ij} < X_i X_j$ *in the quasi-order on* R *induced by the termorder on* T. *Moreover if*

4. *For all* $1 \leq i \leq n$ *and all* $0 \neq a \in \mathbf{K}$

$$X_i * a = a X_i.$$

The notation for solvable polynomial rings will be

$$R = \mathbf{K}\{X_1, \ldots, X_n; Q\},$$

where Q denotes the commutator relations of axiom 6.2.1(3). The commutator relations Q' of axiom 6.2.1(4) will not be written according to our earlier convention.

By the following lemmas, the determination of the $*$-product is extended to arbitrary polynomials in $\mathbf{R}$.

Lemma 6.2.2 *(cf. 3.2.4) Let* $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n, Q\}$ *be a solvable polynomial ring, let* $1 \leq i \leq n$ *and let* $f \in \mathbf{K}[X_1, \ldots, X_i]$, $g \in \mathbf{K}[X_i, \ldots, X_n]$. *Then*

$$f * g = f \cdot g.$$

Lemma 6.2.3 *(cf. 3.2.5) Let* $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n, Q\}$ *be a solvable polynomial ring, let* $<_T$ *be a* $*$*-compatible admissible term order, and let* $f, g \in \mathbf{R}$. *Then there exists an* $h \in \mathbf{R}$ *such that*

$$f * g = c \cdot f \cdot g + h$$

and $h <_T f \cdot g$. *Moreover,* c *and* h *are uniquely determined by* f *and* g.

For the proofs and further details see chapters 3 and 4

6.2.1 Implementation Considerations

The non-commutative polynomials are represented as ordinary commutative polynomials. The implementation of the algorithms uses the Distributive Polynomial System [Gebauer, Kredel 1983]. A polynomial in distributive representation is a list of so called exponent vectors and so called base coefficients. Algorithm names for constructors and selectors for distributive polynomials begin with `DIP`, for exponent vectors with `EV`, for

base coefficients with `RN` (for rational numbers). The coefficient field **K** is the field of rational numbers in the current implementation.

The commutator relations from 6.2.1(3) are implemented as triples of commutative polynomials. More precisely a relation $X_j * X_i = c_{ij}X_iX_j + p_{ij}$ for some $1 \leq i \leq j \leq n$ is represented as triple

$$(X_j, X_i, c_{ij}X_iX_j + p_{ij})$$

of distributive polynomials. Missing relations are treated as if the relation $X_j * X_i = X_iX_j$ was specified, i. e. as if a relation with $c_{ij} = 1$ and $p_{ij} = 0$ was defined.

The set of all commutator relations is stored in a list called *relation table*. So in order to compute the product $X_j * X_i$ one has to look for a triple starting with (X_j, X_i, r) and the take the third polynomial in this triple.

We will now discuss the $*$-product algorithm and the relation table handling in detail.

6.3 The Non-commutative Product

In this section we will first sketch the product algorithm, then we discuss the Modula-2 listing of the implemented algorithm and then we proof the correctness. In a separate subsection the relation table handling is discussed.

The product of two non-commutative polynomials is formed as the sum over the products of the terms (power-products). The product of terms are formed as commutative product or by looking for appropriate commutator relations and recursive application of the (polynomial) product algorithm.

During the algorithm many products of powers of variables are formed. In order to save computation time, these products are stored in the so called relation table. The next time such a product is needed it can be taken from the table without being recomputed. Only commutator relations of the form $X_j^{e_j} * X_i^{e_i} = q$ are stored since the storage of arbitrary product relations would waste to much memory.

More precisely, let u, v be two terms, and assume we want to compute $u * v$, with $u \in T(X_1, \ldots, X_j)$ and $v \in T(X_i, \ldots, X_n)$, for $1 \leq i, j \leq n$. Then we proceed as follows:

1. If by lemma 6.2.2 $u * v = u \cdot v$ then we are done, otherwise proceed as follows:

2. Split each term into three parts $u * v = u_1 \cdot u_2 \cdot u_3 * v_3 \cdot v_2 \cdot v_1$, where $u_2 \cdot u_3 = X_j^{e_j}, v_3 \cdot v_2 = X_i^{e_i}$ and $u_1 \in T(X_1, \ldots, X_{j-1})$, $v_1 \in T(X_{i+1}, \ldots, X_n)$. u_3, v_3 are determined by the largest existing relation table entry for the product of powers of variables. Let the product $u_3 * v_3$ be p.

3. Compute the product $u_2 * (p * v_2)$ by two fold recursive application of the product algorithm. Let the results be q and q'.

4. Add the triples $(u_3, X_i^{e_i}, q)$ and $(X_j^{e_j}, X_i^{e_i}, q')$ to the relation table. Note that during the recursion all triples $(X_j^{l_j}, X_i^{l_i}, q')$ with $l_j < e_j$ and $l_i < e_i$ are already added to the relation table.

5. Finally form the product $u_1 * (q * v_1)$ by recursion.

The Modula-2 listing of the algorithm is given in table 6.1. The step numbers `(*n*)` correspond to the numbers in the description above. The algorithms starting with `EV` do manipulations on terms (called exponent vectors). `DINPTL` and `DINPTU` do the relation table lookup and update (see section 6.3.1). `DIPMAD` and `DIPFMO` selectors and constructors for distributive polynomials. `DIRPPR`, `DIRPRP`, `DIRPSM` and `RNPROD` are polynomial and rational number arithmetic functions. `SIL` denotes the empty list.

Although this algorithm seems to be quite effective, it is difficult to prove its correctness. The proof of lemma 6.2.3 can not be applied directly to the algorithm, since the usage of the induction hypothesis in the proof does not coincide with the recursive application of the product algorithm. On the other hand, in the product algorithm in [Kandri-Rody, Weispfenning 1988](section 2), which is designed after the proof, the products $X_j^{e_j} * X_i^{e_i}$ are not computed, and therefore they can not be put into a relation table.

Lemma 6.3.1 *Algorithm* `DINPPR` *is correct with respect to its specification.*

Proof: We have to show that the algorithm terminates and that it computes the $*$-product of two polynomials. The proof proceeds by noetherian induction on $u \cdot v$ with respect to $<_T$. We assume the correctness of the relation table handling.

The correctness of the trivial cases (step `(*a*)`) is clear from the definition of the solvable polynomial ring 6.2.1 and serves as induction base.

The multiplication of terms performed in the two `REPEAT`-loops (step `(*b*)`) follows directly from the distributive law of the solvable polynomial ring 6.2.1 and from the induction hypothesis. The correctness of the commutative case (step `(*1*)`) follows from lemma 6.2.2.

The remaining case is the determination of the $*$-product of terms u and v, where $u \in T(X_h, \ldots, X_j)$ and $v \in T(X_i, \ldots, X_k)$ with $j > i$. Let $u = u'X_j^e$ and $v = X_i^l v'$, with $e \geq 1$ and $l \geq 1$ and $u' \in T(X_h, \ldots, X_{j-1})$ and $v' \in T(X_{i+1}, \ldots, X_k)$. Then the product is formed as follows:

$$\begin{aligned} u * v &= u'X_j^{e-1}X_j * X_iX_i^{l-1}v' \\ &= u' * ((X_j^{e-1} * ((X_j * X_i) * X_i^{l-1})) * v') \\ &= u' * ((X_j^{e-1} * ((c_{ij}X_iX_j + p_{ij}) * X_i^{l-1})) * v') \\ &= c_{ij}u' * ((X_j^{e-1} * ((X_iX_j) * X_i^{l-1})) * v') + u'X_j^{e-1} * (p_{ij} * X_i^{l-1}v') \end{aligned}$$

with parenthesis indicating the sequence of computation in the algorithm.

```
PROCEDURE DINPPR(T,A,B: LIST): LIST;
(*Distributive polynomial non commutative product.
A and B are distributive polynomials. T is a table
of distributive polynomials specifying the non commutative
relations. C=A*B, the non commutative product of A and B.
The table T may be modified. *)
VAR  AL, AP, BL, BP, C, C1, C2, CL, CS, E1, E2, E3, E4, EL,
     EL1, EL1S, EP, F1, F2, F3, FL, FL1, FL1S, FP, FS, GL, J1Y, N,
     O, RL, XL, XL1, XL2: LIST;
BEGIN
(*a*) (*trivial cases. *) C:=0;
      IF A = 0 THEN RETURN(C); END;
      IF B = 0 THEN RETURN(C); END;
      IF DIRPON(A) = 1 THEN C:=B; RETURN(C); END;
      IF DIRPON(B) = 1 THEN C:=A; RETURN(C); END;
      O:=RNINT(1); RL:=DIPNOV(A); N:=EVZERO(RL);
(*b*) (*loop on a and b. *) AP:=A;
      REPEAT DIPMAD(AP, AL,EL,AP); BP:=B;
             REPEAT DIPMAD(BP, BL,FL,BP); EP:=EVDOV(EL); EL1:=RL+1;
                    IF EP <> SIL THEN EL1:=FIRST(EP); END;
                    FP:=EVDOV(FL); FL1:=0;
                    IF FP <> SIL THEN FS:=CINV(FP); FL1:=FIRST(FS);
                       END;
                    FL1S:=RL+1-FL1; EL1S:=RL+1-EL1;
(*1*)               IF EL1S <= FL1S THEN GL:=EVSUM(EL,FL);
(*1*)                  CS:=DIPFMO(O,GL);
                       ELSE (* e1 * e2 = el, f1 * f2 = fl.*)
(*2*)                  EVSU(EL,EL1,0, E1,XL1); EVSU(FL,FL1,0,F1,XL2);
(*2*)                  EVCADD(N,EL1,XL1, E2,XL);
(*2*)                  EVCADD(N,FL1,XL2, F2,XL);
(*2*)                  DINPTL(T,E2,F2,CS,E3,F3);
                       IF F3 <> SIL THEN C2:=DIPFMO(O,F3);
(*3*)                     CS:=DINPPR(T,CS,C2);
(*3*)                     IF E3 = SIL THEN E4:=E2; ELSE
(*3*)                        E4:=EVDIF(E2,E3); END;
(*4*)                        DINPTU(T,E4,F2,CS); END;
(*3*)                  IF E3 <> SIL THEN C1:=DIPFMO(O,E3);
(*4*)                     CS:=DINPPR(T,C1,CS); DINPTU(T,E2,F2,CS) END;
(*5*)                  C1:=DIPFMO(O,E1); C2:=DIPFMO(O,F1);
(*5*)                  CS:=DINPPR(T,CS,C2); CS:=DINPPR(T,C1,CS) END;
                    CL:=RNPROD(AL,BL); CS:=DIRPRP(CS,CL);
                    C:=DIRPSM(C,CS);
                    UNTIL BP = SIL;
             UNTIL AP = SIL;
(*c*) (*finish. *) RETURN(C);
(*d*) END DINPPR;
```

Table 6.1: Algorithm: DINPPR

The product $X_j * X_i$ is determined by relation table lookup as $c_{ij}X_iX_j + p_{ij}$. Since $p_{ij} <_T X_iX_j$ the product of the second summand $u'X_j^{e-1} * (p_{ij} * X_i^{l-1}v')$ can be handled by twofold recursive application of the product algorithm with induction assumption.

Now for the product $(X_iX_j) * X_i^{l-1}$ in the first summand the induction hypothesis may not be fulfilled (namely if $u' = v' = 1$ and $e = 1$). But observe that within the recursive application of the algorithm the product is formed as: $X_i * (X_j * v'')$ with $v'' = X_i^{l-1}$. So the induction hypothesis can be applied to $X_j * v''$ yielding $c'v'' \cdot X_j +$ rest ($c' \in \mathbf{K}*$). For the first summand we have $X_i * (c'v'' \cdot X_j) = X_i \cdot c'v'' \cdot X_j$ since $i < j$ (according to 6.2.2). Since rest $<_T v''$ the product $X_i *$ rest can be computed by induction hypothesis. This shows that $(X_iX_j) * X_i^{l-1} = cX_i^lX_j +$ rest with $0 \neq c \in \mathbf{K}$ and rest $<_T X_i^lX_j$.

For the next product $X_j^{e-1} * (X_i^lX_j)$ the induction hypothesis may not be fulfilled (in case $u' = v' = 1$). But during recursive applications of the algorithm the product is formed as

$$\underbrace{X_j * (\ldots(X_j}_{e-1 \text{ times}} * X_i^l)\ldots)X_j$$

and the induction hypothesis applies to all successive products on the right side. This yields a polynomial with commutative head term $X_i^lX_j^e$ and some rest which is smaller than the head term.

Next the product $(X_i^lX_j^e) * v'$ is by recursion formed as $X_i^l * (X_j^e * v')$. Again the induction hypothesis can be applied to $X_j^e * v'$ yielding $cX_j^e \cdot v' +$ rest, with $0 \neq c \in \mathbf{K}$ and rest $<_T X_j^e \cdot v'$. Since $i < j$ and $v'' \in T(X_{i+1}, \ldots, X_k)$ we get for the first summand by 6.2.2 $X_i^l * (X_j^e \cdot v') = X_i^l \cdot X_j^e \cdot v'$.

Finally the product $u' * (X_i^lX_j^ev')$ is by recursion computed as $u'' * (X_{j-1}^o * (X_i^lX_j^ev'))$. Again for the right products the induction hypothesis is fulfilled in the recursion.

So we get $u * v = cu \cdot v +$ rest with $0 \neq c \in \mathbf{K}$ and rest $<_T uv$. This shows the correctness of the term product. Since $<_T$ is noetherian the algorithm terminates. This concludes the proof. □

We turn now to the relation table algorithms. An example for the complexity of the $*$-product, is included in section 6.3.2.

6.3.1 Relation Tables

As noted in the section on the product algorithm the relation table must be maintained through recursive applications of the $*$-product algorithm. Naturally we want to use all computed relations to be accessible at any time during further recursive calls.

The relation table is implemented as a list of distributive polynomials:

$$T = (u_1, v_1, p_1, \ldots, u_t, v_t, p_t)$$

where the $u_i = X_{j_i}^{e_i}$, $v_i = X_{k_i}^{l_i}$ and $p_i = c_i \cdot X_{k_i}^{l_i} \cdot X_{j_i}^{e_i} + p_i'$. The table entries are partially ordered with respect to divisibility of the relation heads (u_i, v_i).

Definition 6.3.2 *Let $T = (u_1, v_1, p_1, \ldots, u_t, v_t, p_t)$ be a relation table. Then the following condition must hold:*

$$\textit{for all } 1 \leq i \leq t \textit{ there does not exist } 1 \leq i < j \leq t \textit{ such that } u_i \mid u_j \textit{ and } v_i \mid v_j.$$

I.e. relation heads which are 'later' in the table may divide relation heads, which come 'earlier' in the table.

If T is empty at the beginning, i.e. in this case **all** variables commute, then no non-commuting relation will ever be computed during `DINPPR` and T will remain empty.

The search for a product relation goes from left to right in the list so one finds a relation with maximal exponents. The search is successful, if both exponents of u_i and v_i divide the exponents of the relation we look for. If no relation matches, we assume the variables to commute, i.e. we assume $c = 1$ and $p = 0$. The Modula-2 algorithm listing is given in table 6.2. The variables are named according to the ALDES naming convention: e = `EL` = `el`, e' = `EP`, etc.

```
PROCEDURE DINPTL(T,EL,FL: LIST;  VAR C,EP,FP: LIST);
(*Distributive polynomial non commutative product table lookup.
e and f are exponent vectors. T is a table
of distributive polynomials specifying the non commutative
relations. C is the non-commutative product of x**es and x**fs.
ep and fp are exponent vectors with es+ep=e and fs+fp=f.
If e=es or f=fs then ep=() or fp=(). *)
VAR   GL, GL1, GL2, O, PP, Q1, Q2, SL, TL: LIST;
BEGIN
(*1*) (*initialize.*) PP:=T; EP:=SIL; FP:=SIL;
(*2*) (*search polynomials in pp. *)
      WHILE PP <> SIL DO ADV3(PP, Q1,Q2,C,PP);
            GL1:=DIPEVL(Q1); GL2:=DIPEVL(Q2);
            SL:=EVMT(EL,GL1); TL:=EVMT(FL,GL2);
            IF (SL*TL = 1) THEN EP:=EVDIF(EL,GL1);
               FP:=EVDIF(FL,GL2);
               IF EVSIGN(EP) = 0 THEN EP:=SIL; END;
               IF EVSIGN(FP) = 0 THEN FP:=SIL; END;
               RETURN; END;
            END;
(*3*) (*not found, use symmetric product. *)
      GL:=EVSUM(EL,FL); O:=RNINT(1);
      C:=DIPFMO(O,GL); RETURN;
(*6*) END DINPTL;
```

Table 6.2: Algorithm: DINPTL

Proposition 6.3.3 *Algorithm* `DINPTL` *is correct with respect to its specification.*

Proof: Given X^e and X^f (multi indices), the algorithm determines $C \in \mathbf{R}$, and e' and f' such that

$$X^e \cdot X^f = X^{e'} \cdot HT(C) \cdot X^{f'}.$$

In the `WHILE`-loop the relation table is scanned for a relation which satisfies this condition. Therefore `EVMT` tests if the first argument is a (commutative) multiple of the second argument.

If no relation in the table divides both e and f, then the loop is terminated by exhausting the relation list. In this case the commutative product of the two terms is formed in step (3) and e' and f' are set to fulfil the output condition. This setting of e' and f' is tested in the product algorithm and inhibits the algorithm `DINPTU` from being called in this case.

In the other case, when a matching relation is found, e' and f' are determined according to the head term of C and the inputs e and f. Then the loop is exited and the algorithm terminates. □

The relation table update algorithm determines the correct position if the new relation according to condition 6.3.2. Then it inserts the relation without modifying the list pointer to the table. This is important to make the information which is stored in recursive calls of `DINPPR` available to all further (top-level) calls of the product algorithm. The Modula-2 listing is given in table 6.3.

Proposition 6.3.4 *Algorithm* `DINPTU` *is correct with respect to its specification.*

Proof: Let $T = (u_1, v_1, p_1, \ldots, u_t, v_t, p_t)$, $t > 0$ upon entry into the algorithm. For empty T the algorithm is never be called.

In step (3) the correct position of the new relation in the table is determined according to condition 6.3.2. The variable `TS` remembers the position behind last position in T when the table condition would be not fulfilled. Then the new relation can be entered just before this position.

In step (4) the location of T is not modified. If no position in T was found in step (3), then the new relation is placed in front of the table. In this case it is required that T is not empty.

The `FIRST` field of `TS` is modified to C_1 and the `RED` field of `TS` is modified to the list $(C_2, C, u_i, v_i, p_i, \ldots, u_t, v_t, p_t)$. So T becomes

$$(u_1, v_1, p_1, \ldots, u_{i-1}, v_{i-1}, p_{i-1}, C_1, C_2, C, u_i, v_i, p_i, \ldots, u_t, v_t, p_t)$$

as desired. □

One *optimization* of the table implementation would be to built separate table entries for each pair of non-commuting *variables*. Then the search for a relation could be restricted to a certain sub table. However for the scope of examples which can be computed the current table implementation suffices.

```
PROCEDURE DINPTU(T,EL,FL,C: LIST);
(*Distributive polynomial non commutative product table update.
e and f are exponent vectors. T is a table
of distributive polynomials specifying the non commutative
relations. C is a distributive rational polynomial. The relation
e * f = C is added to T. T is modified. *)
VAR  C1, C2, GL1, GL2, O, PL, PP, Q1, Q2, SL, TL, TP, TS, V: LIST;
BEGIN
(*1*) (*generate polynomials corresponding to el and fl.*)
      O:=RNINT(1); C1:=DIPFMO(O,EL); C2:=DIPFMO(O,FL);
(*2*) (*message. *)
      IF VALIS <> SIL THEN V:=VALIS; SWRITE("NEW RELATION = ");
         DIRPWR(C1,V,-1); SWRITE(" .*. "); DIRPWR(C2,V,-1);
         SWRITE(" = "); DIRPWR(C,V,-1); BLINES(0); END;
(*3*) (*search position in t. *) TS:=SIL; PP:=T;
      WHILE PP <> SIL DO
            ADV2(PP, Q1,Q2,PP); PP:=RED(PP); GL1:=DIPEVL(Q1);
            GL2:=DIPEVL(Q2); SL:=EVMT(GL1,EL); TL:=EVMT(GL2,FL);
            IF (SL*TL = 1) THEN TS:=PP; END;
            END;
(*4*) (*update ts. *)
      IF TS = SIL THEN TS:=T; END;
      ADV(TS, PL,TP); TP:=COMP3(C2,C,PL,TP);
      SFIRST(TS,C1); SRED(TS,TP);
      RETURN;
(*7*) END DINPTU;
```

Table 6.3: Algorithm: DINPTU

6.3.2 Examples of Complexity

During the computation of a $*$-product of two terms many new multiplications of terms may occur. E. g. if the commutator relations contain high degree polynomials or if the commutator relations are dense polynomials even of low degree. So we discuss three examples to give some impression of the complexity of the algorithm.

1. Let $\mathbf{R} = \mathbf{Q}[x, y, z]$ be a ring with the commutator relations

$$\begin{aligned} y * x &= xy + x^d \\ z * x &= xz + y^d \\ z * y &= yz + y^d \end{aligned}$$

   where $<_T$ is the inverse lexicographical term order. Note that this ring is only a solvable polynomial ring in case $d = 0, 1$. If $d > 1$ the ring defined by this relations is not associative. However as an example for the product algorithm it may be accepted. In this example the commutator relations are 'sparse' with 'high' degree.

2. Let $\mathbf{R} = \mathbf{Q}[x, y, z]$ be a ring with the commutator relations

$$\begin{aligned} y * x &= xy + x + y + z \\ z * x &= xz + x + y + z \\ z * y &= yz + x + y + z \end{aligned}$$

   where $<_T$ is the total degree (inverse graduated) term order. The commutator relations are 'dense' of 'low' degree.

3. [Apel, Klaus 1990] Let $\mathbf{R} = \mathbf{Q}[x, y, z]$ be a solvable polynomial ring (a Lie algebra) with the commutator relations

$$\begin{aligned} y * x &= xy - z \\ z * x &= xz + y \\ z * y &= yz - x \end{aligned}$$

   where $<_T$ is the total degree (inverse graduated) term order.

We want to compute the product

$$z^c * y^c * x^c$$

for varying parameters d and c in examples 1 and 2, and the product

$$(x + y + z)^c$$

for varying parameter c in example 3.

We will observe the following output parameters:

Example	d	c	r	p	t
1	2	1	5	6	0
	2	2	21	15	8
	2	3	45	28	26
	2	4	73	45	68
	3	1	9	7	2
	3	2	37	38	18
	3	3	92	90	96
	4	1	15	8	6
	4	2	61	46	36
	4	3	134	110	204
	5	1	23	9	10
	5	2	83	54	64
	6	1	33	10	18
	6	2	104	62	96
	6	3	314	150	958
	7	1	45	11	28
	8	1	59	12	46

Table 6.4: Complexity of the $*$ product, example 1

Example	d	c	r	p	t
2	1	1	3	10	0
	1	2	10	41	14
	1	3	23	105	158
	1	4	42	214	1412

Table 6.5: Complexity of the $*$ product, example 2

r the number of commutator relations after the computation of the product,

p the number of terms in the product, and

t the computing time on an Atari ST.

t' the computing time on an IBM AT 286, in example 3.

The results are summarized in tables 6.4 and 6.5. They show, that the complexity depends both on the degree and density of the commutator relations. In example 1 more commutator relations are computed compared to example 2. In example 2 at a certain stage no new commutator relations are computed and only the relations from the relation table are used. Example 3 in table 6.6 shows the advantage of the relation table method compared to the method of Apel and Klaus without storing new relations.

Example	c	r	p	t Atari ST	t' AT 286
3	3	6	17	2	2
	4	10	34	8	9
	5	14	52	20	29
	6	18	83	50	82
	7	22	113	114	222
	8	26	164	228	540
	9	30	214	436	–

Table 6.6: Complexity of the $*$ product, example 3

6.4 Left Normal Form and Left Irreducible Sets

First recall the following definitions from 4.2.1:

Let $\mathbf{R}$ be a solvable polynomial ring, $f, f', p \in \mathbf{R}$. The reduction $f \longrightarrow_{t,p} f'$ is defined as follows: Let $t \in T(f)$ such that $\mathrm{HT}(p)$ divides t (in the commutative sense). Now let a be the coefficient of t in f and $b = \mathrm{HC}(p)$ be the head coefficient of p (also called 'leading base coefficient' in ALDES / SAC-2). Furthermore let $s = \frac{\mathrm{HT}(p)}{t}$ and $c = \mathrm{HC}(s * \mathrm{HT}(p))/\mathrm{HC}(s\mathrm{HT}(p))$ then

$$f' = f - \frac{a}{bc} s * p.$$

Since s is multiplied from the left to p, $f \longrightarrow_{t,p} f'$ is a *left* reduction. For a *right* reduction s is multiplied from the right to p. If $d = \mathrm{HC}(s * p)/\mathrm{HC}(sp)$ then f' can also be written as $f - \frac{a}{d} s * p$.

The reductions with respect to a polynomial $f \longrightarrow_p f'$ and with respect to a set P of polynomials $f \longrightarrow_P f'$ are defined similar as in the commutative case, see also 4.2.1. If f can not be reduced with respect to P we say that f is irreducible with respect to P or that f is in normalform with respect to P. P is irreducible or in normalform or autoreduced, if all $f \in P$ are irreducible with respect to $P \setminus \{f\}$.

We will now turn to the algorithms which implement these reductions. Once the algorithm for the non-commutative product is available, the implementation of the reduction algorithm for polynomials and sets of polynomials are straightforward modifications of the respective algorithms in the commutative case [Gebauer, Kredel 1984].

The algorithm `DINLNF` computes a normalform R of a polynomial S with respect to a set (list) of polynomials P. Every term t in S (or some reduct of S) is checked if there exists a polynomial q in P such that $\mathrm{HT}(q)$ divides t. If such a q exists, the a one step reduction is carried out, otherwise the term t is irreducible and it is placed in the output polynomial R.

The Modula-2 listing of the normalform algorithm is given in table 6.7:

Proposition 6.4.1 *Algorithm* `DINLNF` *is correct with respect to its specification.*

```
PROCEDURE DINLNF(T,P,S: LIST): LIST;
(*Distributive non-commutative polynomial left normal form.
P is a list of non zero polynomials in distributive rational
representation in r variables. S is a distributive rational
polynomial. R is a polynomial such that S is left reducible to R
modulo P and R is in normalform with respect to P.
T is a table of distributive polynomials specifying the
non-commutative relations. *)
VAR  AP, APP, BL, FL, OL, PP, Q, QA, QE, QP, R, SL, SP, SPP, TA, TE:
     LIST;
BEGIN
(*1*) (*s=0. *)
      IF (S = 0) OR (P = SIL) THEN R:=S; RETURN(R); END;
(*2*) (*reduction step.*) R:=SIL; SP:=S; OL:=RNINT(1);
      REPEAT DIPMAD(SP, TA,TE,SPP); PP:=P;
             REPEAT ADV(PP, Q,PP); DIPMAD(Q, QA,QE,QP);
                    SL:=EVMT(TE,QE);
                    UNTIL (PP = SIL) OR (SL = 1);
             IF SL = 0 THEN R:=DIPMCP(TE,TA,R);
                IF SPP = SIL THEN SP:=0; ELSE SP:=SPP; END;
                ELSE FL:=EVDIF(TE,QE); AP:=DIPFMO(OL,FL);
                APP:=DINPPR(T,AP,Q); BL:=DIPLBC(APP);
                BL:=RNQ(TA,BL); APP:=DIRPRP(APP,BL);
                SP:=DIRPDF(SP,APP); END;
             UNTIL SP = 0;
(*3*) (*finish.*)
      IF R = SIL THEN R:=0; ELSE R:=INV(R); END;
(*6*) RETURN(R); END DINLNF;
```

Table 6.7: Algorithm: DINLNF

Proof: As loop invariant we take $S - \sum b_i a'_i * q_i = R' + S'$. Here R' denotes the polynomial corresponding to `R`. In the inner loop we search for a polynomial q such that HT(Q) divides HT(S'). R' is irreducible since no head term of polynomials in P divide any term in R' (for terms in R' we have `SL = 0`). After each loop $S'_{(i)} >_T S'_{(i+1)}$. So partial correctness and termination follows from lemma [Kandri-Rody, Weispfenning 1988] (section 3.2) respectively 4.2.4. I.e. S' becomes zero at some stage so the algorithm terminates. Upon termination we still have R' to be irreducible, and from the loop invariant we have $R' = S - \sum b_i a'_i * q_i$. □

The algorithm uses two strategies, which are not fixed by lemma 4.2.4 respectively in section 3.2 of [Kandri-Rody, Weispfenning 1988].

1. By the outer loop always the greatest (w.r.t. $<_T$) remaining reducible term is reduced. This seems natural, to avoid unnecessary double reductions of terms in $rest(Q)$ introduced to S'.

2. By the inner loop always the first Q which reduces HT(S') is chosen. So the strategy depends on the way the polynomials appear in P. The most efficient way seems to be again to order the polynomials such that the polynomial with greatest head term (w.r.t. $<_T$) comes first in the list. This again avoids unnecessary double reductions.

The following algorithm `DINLIS` computes an monic irreducible set (or monic autoreduced set) P of polynomials. The number of irreducible polynomials is initially set to zero. Then every p in P is checked if it is in normalform with respect to $P \setminus \{p\}$. If this is the case, then the polynomial is counted as irreducible, otherwise the polynomial was reducible and might now be able to reduce further polynomials in $P \setminus \{p\}$. Therefore the number of irreducible polynomials must be reset to zero. The algorithm terminates, if the number of irreducible polynomials is equal to the total number of polynomials. The Modula-2 listing is given in table 6.8.

Proposition 6.4.2 *Algorithm* `DINLIS` *is correct with respect to its specification.*

Proof: In the first step `(*1*)` the polynomials are made monic by algorithm `DIRPMC` and zero polynomials are removed.

As loop invariant in the second step `(*2*)` we may take $\text{ideal}_l(P) = \text{ideal}_l(P' \cup \{p\})$. This is true, since polynomials in P' are replaced by there normal form with respect to $P' \setminus \{p\}$. During each loop two cases occur:

1. a head term of a polynomial p is reduced and irr is set to zero

2. no head term is reduced and irr is increased by 1.

So termination follows from the fact, that no infinite descending (w.r.t $<_T$) sequence of terms exist. So at some stage case (1) can no more occur, and since P was finite irr becomes equal to $length(P') = |P'|$.

```
PROCEDURE DINLIS(T,P: LIST): LIST;
(*Distributive non-commutative polynomial list left irreducible
(autoreduced) set. P is a list of distributive rational polynomials,
PP is the result of left reducing each p element of P modulo P-(p)
until no further reductions are possible.
T is a table of distributive polynomials specifying the
non-commutative relations. *)
VAR  EL, FL, IRR, LL, PL, PP, PS, RL, RP, SL: LIST;
BEGIN
(*1*) (*initialise. *) PP:=P; PS:=SIL;
      WHILE PP <> SIL DO ADV(PP, PL,PP); PL:=DIRPMC(PL);
            IF PL <> 0 THEN PS:=COMP(PL,PS); END;
            END;
      RP:=PS; PP:=INV(PS); LL:=LENGTH(PP); IRR:=0;
      IF LL <= 1 THEN RETURN(PP); END;
(*2*) (*reduce until all polynomials are irreducible. *)
      LOOP ADV(PP, PL,PP); EL:=DIPEVL(PL); PL:=DINLNF(T,PP,PL);
           IF PL = 0 THEN LL:=LL-1;
              IF LL <= 1 THEN EXIT END;
              ELSE FL:=DIPEVL(PL); SL:=EVSIGN(FL);
              IF SL = 0 THEN PP:=LIST1(PL); EXIT END;
              SL:=EQUAL(EL,FL);
              IF SL = 1 THEN IRR:=IRR+1; ELSE IRR:=0;
                 PL:=DIRPMC(PL); END;
              PS:=LIST1(PL); SRED(RP,PS); RP:=PS; END;
           IF IRR = LL THEN EXIT END;
           END;
(*3*) (*finish. *) RETURN(PP);
(*6*) END DINLIS;
```

Table 6.8: Algorithm: DINLIS

To prove that P' is autoreduced, it remains to be shown that each $rest(p)$ is irreducible with respect to $P' \setminus \{p\}$ since the head terms are irreducible by construction. Therefore consider the stage of the loop, after the last head term was reduced. At this point we have $irr = 0$. Now once again every polynomial and especially every rest of a polynomial is reduced with respect to $P' \setminus \{p\}$ until $irr = len$. Although P' changes during the loop, we know that the head terms of polynomials in P' change no more, so the first reduced rests remain irreducible with respect to the later reduced polynomials. □

This algorithm makes maximal use of the fact, that for reducibility of a polynomial only the head terms of the reducing set of polynomials have any influence. In this view the loop consists of two stages: a *first* stage which reduces all head terms (and probably many terms in the rests) and a *second* stage (in the same loop) where the (remaining) rests are reduced in $length(P')$ steps.

Upon termination the order of the polynomials in P' with respect to their head terms may be disturbed.

6.5 S-Polynomials and Left Gröbner Bases

Recall that left Gröbner bases, are defined as sets of polynomials P such that the left reduction $\longrightarrow_P^*$ is confluent. It has already been shown, that it is sufficient for P to be a left Gröbner base, that all left S-polynomials of polynomials $f, g \in P$ reduce to zero with respect to P. Left S-polynomials are defined before section 3.9 in [Kandri-Rody, Weispfenning 1988], respectively definition 4.5.6 of the this work.

Definition 6.5.1 *Let $f, g \in \mathbf{R}$, $w = lcm(\mathrm{HT}(f), \mathrm{HT}(g))$, $u = \frac{w}{\mathrm{HT}(f)}$, $v = \frac{w}{\mathrm{HT}(g)}$. Furthermore let $a' = \mathrm{coeff}(w, u * f)$, $b' = \mathrm{coeff}(w, v * g)$ and let $a = \frac{1}{a'}$, $b = \frac{1}{b'}$. Then the left S-polynomial of f and g is defined as:*

$$\mathrm{LSP}(f, g) = au * f - bv * g.$$

The implementation of the S-polynomial algorithm is straightforward. Only some care is needed to get the coefficients right.

Proposition 6.5.2 *Algorithm* `DINLSP` *is correct with respect to its specification.*

Proof: Follows directly from the definition 6.5.1 of S-polynomials. □

6.5.1 Buchberger Algorithm

Buchberger's algorithm for constructing Gröbner bases is based on the following theorem. In the commutative case it was proved in [Buchberger 1965] and [Buchberger 1985]. In the case of enveloping algebras of Lie algebras and a total degree admissible term order is was proved by [Apel, Lassner 1988].

```
PROCEDURE DINLSP(T,A,B: LIST): LIST;
(*Distributive non-commutative polynomial left S-polynomial.
A and B are rational polynomials in distributive representation.
C is the left S-polynomial of A and B.
T is a table of distributive polynomials specifying the
non-commutative relations. *)
VAR  AL, AP, APP, BL, BP, BPP, C, EL, EL1, FL, FL1, GL, OL: LIST;
BEGIN
(*1*) (*a=0 or b=0. *) C:=0;
      IF (A = 0) OR (B = 0) THEN RETURN(C); END;
      EL:=DIPEVL(A); FL:=DIPEVL(B); OL:=RNINT(1);
(*2*) (*least common multiple. *) GL:=EVLCM(EL,FL);
      EL1:=EVDIF(GL,EL); FL1:=EVDIF(GL,FL);
(*3*) (*non-commutative products. *) APP:=DIPFMO(OL,EL1);
      BPP:=DIPFMO(OL,FL1); APP:=DINPPR(T,APP,A);
      BPP:=DINPPR(T,BPP,B);
(*4*) (*adjust coefficients. *) AL:=DIPLBC(APP);
      BL:=DIPLBC(BPP);
      APP:=DIRPRP(APP,BL); BPP:=DIRPRP(BPP,AL);
(*5*) (*difference. *) C:=DIRPDF(APP,BPP);
(*8*) RETURN(C); END DINLSP;
```

Table 6.9: Algorithm: DINLSP

Theorem 6.5.3 *(cf. 4.6.2) Let G be a finite set of polynomials in $\mathbf{R}$. Then G is a left Gröbner base iff for all $f, g \in G$, $\mathrm{LSP}(f,g) \longrightarrow_G^* 0$.*

The algorithm of Buchberger takes as input a finite set of polynomials and delivers a Gröbner base as output. In a main loop in the algorithm for all pairs of polynomials the S-polynomials are constructed and reduced to their normal form modulo the set of polynomials. If the resulting polynomial is non zero, the polynomial is added to the set of polynomials. The algorithm terminates when all S-polynomials of all pairs can be reduced to zero. Termination is assured by Dickson's lemma and upon termination the condition of theorem 6.5.3 shows that the output polynomial set is a Gröbner base.

Buchberger showed also, that the construction of certain S-polynomials and their reduction could be avoided if some conditions on the head terms of the polynomials and the sequence in which the S-polynomials are constructed are fulfilled. For the definitions of this criteria see also 4.5.10 and 4.5.8.

The first of Buchberger's criteria states that $\mathrm{HT}(f)\mathrm{HT}(g) = \mathrm{lcm}(\mathrm{HT}(f), \mathrm{HT}(g)) \Longrightarrow \mathrm{SP}(f,g) \longrightarrow_G^* 0$. This criterion is no more valid in the non-commutative case as the counter example from 4.5.11 shows:

Example 6.5.4 *Let $\mathbf{R} = \mathbf{K}\{X, Y; Y * X = XY - 1\}$ be the first Weyl algebra. Consider the following ideal generated by two polynomials $p = X$, $q = Y$. Then $\mathrm{HT}(p)\mathrm{HT}(q) = \mathrm{lcm}(\mathrm{HT}(p), \mathrm{HT}(q)) = XY$, but $\mathrm{LSP}(p,q) = X * Y - Y * X = XY - XY + 1 = 1 \neq 0$ and 1 is irreducible wrt. $\{p, q\}$.*

The second criterion of Buchberger states that,

$$\exists h \in G \ : \ \mathrm{HT}(h) \text{ divides } \mathrm{lcm}(\mathrm{HT}(f), \mathrm{HT}(g)) \text{ and } \mathrm{SP}(f,h) \longrightarrow_G^* 0 \text{ and } \mathrm{SP}(h,g) \longrightarrow_G^* 0. \implies \mathrm{SP}(f,g) \longrightarrow_G^* 0$$

This criterion has been proven to be correct in proposition 4.5.8 or 4.6.2(7). It is implemented like in [Gebauer, Kredel 1984] and has been used in the examples following.

The implementation of the algorithm is a straight forward modification of the commutative Buchberger algorithm in [Gebauer, Kredel 1984]. The listing in Modula-2 is given in table 6.10.

In step 1 the input polynomials are made monic and some trivial checks are made if we already have a Gröbner base. The resulting list of polynomials is `PP`. In step 2 the list of all pairs of polynomials `B` and an auxiliary list `D` are constructed in subalgorithm `DILCPL`. Since it is still true, that $\mathrm{LSP}(p,q) = -\mathrm{LSP}(q,p)$ it suffices to consider only pairs of polynomials (f_i, f_j) with $i < j$ as in the commutaive case. The list `D` determines the sequence in which the S-polynomials are constructed. The pairs in `D` are ordered such that the pair (f,g) with the smallest (with respect to $<_T$) $\mathrm{lcm}(\mathrm{HT}(f), \mathrm{HT}(g))$ is selected first.

Steps 3 and 4 comprise the main Buchberger loop. In 3 some bookkeeping is done and in 4 the condition BBEC is checked if the reduction of the S-polynomial is necessary (program `DIGBC3`). If required a S-polynomial `S` is constructed and reduced modulo the list `PP` of polynomials. Then some checks for special cases are made and if the reduced S-polynomial `H` is non zero the lists `B` and `D` are updated in subalgorithm `DILUPL`. If `D` is empty, i.e. if all S-polynomials have been considered, the algorithm proceeds with step 5.

Finally in step 5 the reduced Gröbner base is constructed in subalgorithm `DINLGM` and the algorithm terminates.

Proposition 6.5.5 *Algorithm* `DINLGB` *is correct with respect to its specification.*

Proof: Follows directly from theorems 6.5.3 respectively 4.6.2. The correctness of `DINLGM` is proved in the next section. □

6.5.2 Left Reduced Gröbner bases

Besides the application of the `LRED` in [Kandri-Rody, Weispfenning 1988] (section 2) or our `DINLIS` algorithm to compute a left reduced Gröbner base there is some cheaper way to obtain the same result. As in the commutative case by [Buchberger 1985], one can exploit the fact that we already have a Gröbner base.

Lemma 6.5.6 *Let G be a left GB in* $\mathbf{R}$ *and let $g, h \in G$ such that* $\mathrm{HT}(h)$ *divides* $\mathrm{HT}(g)$. *Then $G' = G \setminus \{g\}$ is still a Gröbner base and* $\mathrm{ideal}_l(G) = \mathrm{ideal}_l(G')$.

```
PROCEDURE DINLGB(T,P,TF: LIST): LIST;
(*Distributive non-commutative polynomials left Groebner basis.
P is a list of rational polynomials in distributive representation
in r variables. PP is the left Groebner basis of P. t is the
trace flag. T is a table of distributive polynomials specifying
the non-commutative relations. *)
VAR   B, C, CPI, CPJ, CPP, D, DL, EL, ELI, ELJ, H, IL, K, PLI, PLIP,
      PLJ, PP, PPP, PPR, PS, Q, QP, RL, S, SL, SL3, TL, TR: LIST;
BEGIN
(*1*) (*prepare input. *)
      IF P = SIL THEN PP:=P; RETURN(PP); END;
      PS:=P; PPR:=SIL;
      WHILE PS <> SIL DO ADV(PS, PLI,PS);
            IF PLI <> 0 THEN PLIP:=DIRPMC(PLI); SL:=DIRPON(PLIP);
               IF SL = 1 THEN PP:=LIST1(PLIP); RETURN(PP); END;
               PPR:=COMP(PLIP,PPR); END;
            END;
      PP:=INV(PPR);
      IF (PP = SIL) OR (RED(PP) = SIL) THEN RETURN(PP); END;
(*2*) (*construct b and d. *)
      PPR:=DIPLPM(PP); PP:=INV(PPR); DILCPL(PP, D,B);
(*3*) (*loop until no more pairs left. *)
LOOP  IF D = SIL THEN EXIT END;
      ADV(D, DL,D); FIRST3(DL, EL,CPI,CPJ); ADV(CPI, QP,C);
      PLI:=FIRST(QP); PLJ:=FIRST(RED(CPJ));
      CPP:=RED(RED(CPJ)); SRED(CPJ,CPP);
      IF CPP = SIL THEN Q:=LAST(QP); SFIRST(C,Q); END;
(*4*) (*s-pol and reduction step. *)
      LOOP SL:=DIGBC3(B,PLI,PLJ,EL); IF SL = 0 THEN EXIT END;
           S:=DINLSP(T,PLI,PLJ); IF S = 0 THEN EXIT END;
           H:=DINLNF(T,PP,S); IF H = 0 THEN EXIT END;
           H:=DIRPMC(H); SL:=DIRPON(H);
           IF SL = 1 THEN PP:=LIST1(H); RETURN(PP); END;
           D:=DILUPL(H,PP,D,B);
           EXIT END;
      END (*3*);
(*5*) (*finish. *) PP:=DINLGM(T,PP);
(*6*) RETURN(PP); END DINLGB;
```

Table 6.10: Algorithm: DINLGB

Proof: Let G be a Gröbner base, then by definition $\longrightarrow_G$ is a confluent reduction relation. So lemma 4.3.2 shows that $\longrightarrow_{G'}$ is a confluent reduction relation and 4.4.4 shows that $\text{ideal}_l(G) = \text{ideal}_l(G')$. □

With this lemma it is sufficient to remove polynomials with head terms that are divided by some other polynomials in the base. This avoids the reduction of these polynomials. For the remaining polynomials only the reductas must be reduced to normal form to obtain a reduced basis. This can be done by `LRED` or preferably `DINLIS`, since `DINLIS` needs only one loop through the base. The listing of the resulting algorithm is given in table 6.11.

```
PROCEDURE DINLGM(T,P: LIST): LIST;
(*Distributive non-commutative minimal ordered left groebner basis.
P is a list of non zero rational polynomials in distributive
representation in r variables, P is a left groebner basis.
PP is the minimal normed and ordered left groebner basis.
T is a table of distributive polynomials specifying the
non-commutative relations. *)
VAR  AL, EI, EJ, EL, PB, PI, PJ, PP, PS, QP, TL: LIST;
BEGIN
(*1*) (*length p le 1. *) PP:=P;
      IF (P = SIL) OR (RED(P) = SIL) THEN RETURN(PP); END;
(*2*) (*search for exponent vector .*) PS:=PP; QP:=SIL;
      REPEAT ADV(PS, PI,PS); PB:=PS; EI:=DIPEVL(PI); TL:=0;
             WHILE (PB <> SIL) AND (TL = 0) DO ADV(PB, PJ,PB);
                   EJ:=DIPEVL(PJ); TL:=EVMT(EI,EJ); END;
             PB:=QP;
             WHILE (PB <> SIL) AND (TL = 0) DO ADV(PB, PJ,PB);
                   EJ:=DIPEVL(PJ); TL:=EVMT(EI,EJ); END;
             IF TL = 0 THEN QP:=COMP(PI,QP); END;
             UNTIL PS = SIL;
      PP:=INV(QP);
      IF (PP = SIL) OR (RED(PP) = SIL) THEN RETURN(PP); END;
(*3*) (*get irreducible set. *) PP:=DINLIS(T,PP);
(*4*) (*sort. *) PP:=DIPLPM(PP);
(*7*) RETURN(PP); END DINLGM;
```

Table 6.11: Algorithm: DINLGM

Proposition 6.5.7 *Algorithm* `DINLGM` *is correct with respect to its specification.*

Proof: The correctness of step 2 follows from lemma 6.5.6: In the `REPEAT`-loop each polynomial of the list is selected and checked if its head term is divisible. In the first `WHILE`-loop the polynomials following in the list are used for the check and in the second `WHILE`-loop the 'good' polynomials before the actual polynomial are used for the check.

The correctness of step 3 follows from the correctness of algorithm `DINLIS` by proposition 6.4.2 and proposition [Kandri-Rody, Weispfenning 1988] (proposition 4.5) respectively 4.3.5. The sorting of the polynomials in step 4 is assumed to be correct. □

6.6 Two-sided Gröbner Bases

Besides the left ideals and left Gröbner bases in solvable polynomials rings, Kandri-Rody and Weispfenning characterize also two-sided ideals and two-sided Gröbner bases constructively. Their main observation is that two-sided GB's can be obtained by left GB construction combined with taking right variable multiples of all polynomials in the base.

More precisely let $\text{ideal}_t(G)$ denote the two-sided ideal generated by $G \subset \mathbf{R}$. Then the finite set G of polynomials in $\mathbf{R}$ is a two-sided Gröbner base if satisfies the equivalent conditions of the theorem [Kandri-Rody, Weispfenning 1988] (theorem 5.4) respectively 4.11.6:

Theorem 6.6.1 *Let G be a finite set of polynomials in $\mathbf{R}$. Then the following assertions are equivalent:*

(4) *For all $f \in \text{ideal}_t(G)$, $f \longrightarrow_G^* 0$ (left reduction).*

(6) *G is a left GB and for all $1 \leq i \leq r$, $p \in G$, $p * X_i \longrightarrow_G^* 0$.*

Based on this theorem it is easy to give an algorithm for the construction of two-sided GB's: Iterate the computation of left GB's G and the combination with polynomials $p * X_i$:

$$G_{k+1} := G_k \cup \{p * X_i \longrightarrow_G^* \mid \ p \in G,\ 1 \leq i \leq r\}$$

until $G_{k+1} = G_k$.

This gives the algorithm `GROEBNER` in section 2 of [Kandri-Rody, Weispfenning 1988].

The algorithm given in table 6.12 is slightly different: Take the algorithm for the computation of left GB's and start the algorithm with the combined set $G \cup \{p * X_i \longrightarrow_G^* \mid \ p \in G,\ 1 \leq i \leq r\}$. At any time a S-polynomial is reduced to a polynomial $h \neq 0$, combine G not only with $\{h\}$ but additionally with the set $\{h * X_i \longrightarrow_G^* \mid \ 1 \leq i \leq r\}$. Furthermore modify the lists `B` and `D` as appropriate.

The listing of this algorithm, called `DINCGB`, is given in table 6.12. Note, that singleton sets of polynomials may not be two-sided GB's any more. So the respective case detections in algorithm `DINLGB` can not be carried over to algorithm `DINCGB`.

Proposition 6.6.2 *Algorithm* `DINCGB` *is correct with respect to its specification.*

Proof: Termination is guaranteed by Dickson's lemma.

Upon termination of steps 3 and 4 `PP` is a left Gröbner base since all S-polynomials reduce to zero, either by direct verification or by condition BBEC. Condition (6) of 6.6.1 is fulfilled since for any polynomial p also the normal form of $p * X_j$ $(1 \leq j \leq r)$ is in the base. This shows that `PP` is a (non reduced) two-sided Gröbner base.

The correctness of step 5 follows from theorem 5.4 of [Kandri-Rody, Weispfenning 1988] respectively our theorem xreftgb.th and the correctness of algorithm `DINLGM`. □

This completes the discussion of the algorithms. We turn now to a small example.

```
PROCEDURE DINCGB(T,P,TF: LIST): LIST;
(*Distributive non-commutative polynomials two-sided groebner basis.
P is a list of rational polynomials in distributive representation in r
variables. PP is the groebner basis of P. t is the trace flag. T is a table
of distributive polynomials specifying the non-commutative relations. *)
VAR   B, C, CPI, CPJ, CPP, CR, D, DL, EL, ELI, ELJ, F, H, IL, K, N, O, PL,
      PLI, PLIP, PLJ, PP, PPP, PPR, PS, Q, QL, QP, RL, S, SL, TL, X: LIST;
BEGIN
(*1*) (*prepare input. *) IF P = SIL THEN PP:=P; RETURN(PP); END;
      PS:=P; PPR:=SIL;
      WHILE PS <> SIL DO ADV(PS, PLI,PS);
            IF PLI <> 0 THEN PLIP:=DIRPMC(PLI); SL:=DIRPON(PLIP);
               IF SL = 1 THEN PP:=LIST1(PLIP); RETURN(PP); END;
               PPR:=COMP(PLIP,PPR); END; END;
      PP:=INV(PPR); IF PP = SIL THEN RETURN(PP); END;
      RL:=DIPNOV(FIRST(PP)); IF RL = 0 THEN RETURN(PP); END;
      N:=EVZERO(RL); O:=RNINT(1); X:=SIL;
      FOR IL:=1 TO RL DO EVSU(N,IL,1, EL,XL); XP:=DIPFMO(O,EL);
          X:=COMP(XP,X); END;
(*2*) (*add right multiples of polynomials and single variables. *) F:=PP;
      REPEAT ADV(F, PL,F); XS:=X;
             REPEAT ADV(XS, XP,XS); QL:=DINPPR(T,PL,XP);
                    QL:=DINLNF(T,PP,QL); QL:=DIRPMC(QL);
                    SL:=DIRPON(QL);
                    IF SL = 1 THEN PP:=LIST1(QL); RETURN(PP) END;
                    IF QL <> 0 THEN PP:=COMP(QL,PP); END;
                    UNTIL XS = SIL;
             UNTIL F = SIL;
      PPR:=DIPLPM(PP); PP:=INV(PPR); DILCPL(PP, D,B);
(*3*) (*loop until no more pairs left. *)
LOOP  IF D = SIL THEN EXIT END;
      ADV(D, DL,D); FIRST3(DL, EL,CPI,CPJ); ADV(CPI, QP,C);
      PLI:=FIRST(QP); PLJ:=FIRST(RED(CPJ));
      CPP:=RED(RED(CPJ)); SRED(CPJ,CPP);
      IF CPP = SIL THEN Q:=LAST(QP); SFIRST(C,Q); END;
(*4*) (*reduction step. *)
      LOOP SL:=DIGBC3(B,PLI,PLJ,EL); IF SL = 0 THEN EXIT END;
           S:=DINLSP(T,PLI,PLJ); IF S = 0 THEN EXIT END;
           H:=DINLNF(T,PP,S); IF H = 0 THEN EXIT END;
           H:=DIRPMC(H); SL:=DIRPON(H);
           IF SL = 1 THEN PP:=LIST1(H); RETURN(PP); END;
           D:=DILUPL(H,PP,D,B); XS:=X;
           REPEAT ADV(XS, XP,XS); QL:=DINPPR(T,H,XP);
                  QL:=DINLNF(T,PP,QL);
                  QL:=DIRPMC(QL); SL:=DIRPON(QL);
                  IF SL = 1 THEN PP:=LIST1(QL); RETURN(PP) END;
                  IF QL <> 0 THEN D:=DILUPL(QL,PP,D,B) END;
                  UNTIL XS = SIL;
           EXIT END;
      END (*3*);
(*5*) (*finish. *) PP:=DINLGM(T,PP);
(*9*) RETURN(PP); END DINCGB;
```

Table 6.12: Algorithm: DINCGB

6.7 Computation Example

So far we have discussed the non-commutative product and Buchberger algorithm. We will now discuss an example computed with the MAS system and give some computing times on several machines.

6.7.1 Polynomial Input and Output

Since polynomials are internally represented by lists over atoms (integers with absolute value less than 2^{29}) we need some facilities to display or input polynomials in more natural form.

For the display routines the standard display routines for the (commutative) distributive rational polynomials can be used. For the input routines the non-commutative product algorithm can be incorporated to respect the order of the variables in the polynomials.

The syntax (in EBNF) of a polynomial accepted by the input routines is given in table 6.13.

```
poly   = ( rat | var | "(" sum ")" )
sum    = term { ( "+" | "-" ) term }
term   = factor { [ "*" ] factor }
factor = poly [ "**" nat ]
rat    = int [ "/" int ]
```

Table 6.13: Polynomial Syntax in EBNF

`nat` denotes a positive atom, `int` denotes an integer, `rat` denotes a rational number and `var` denotes a variable name defined in the polynomial variable list.

The specification of the multiplication operator `*` is optional. In any case the product is the non-commutative $*$-product. During input the polynomials are multiplied out to obtain the internal canonical form of distributive rational polynomials. In the output the polynomials are therefore represented as sums over monomials.

The listing of an example is given in table 6.14. The input of non-commutative polynomials consists of two steps:

1. the input of the commutator relations together with the list of variables of the polynomial ring and the desired term order,
2. the input of the non-commutative polynomials itself.

The commutator relations are a list of commuting polynomials which are read by the MAS function `PREAD`. `PREAD` reads from the current input stream and returns a list of distributive rational polynomials in internal representation. `PREAD` expects the following items:

1. The variable list: `(a, x, y)`. A variable name may consist of a alpha-numerical character sequence starting with a letter. All variables occurring in the polynomials must be specified.

2. The desired term order: `L`. The term order may be one of the following:

   L for the inverse lexicographical term order

   G for the inverse graduated term order

   polynomial list a list of univariate (integral) polynomials in the variable `T` (this name is fixed). The list length must be the same as the number of variables. The list is interpreted as the coefficients of a linear form which defines a term order. See [Weispfenning 1987] for details.

   There is no check if the term order is compatible with the commutator relations or if the linear form defines an admissible term order.

3. The commutator relations themselves: `( y ), ( x ), ( x y + a )`. This relation is interpreted as $y * x = xy + a$. Not specified relations are interpreted as if the variables commute. In this example a commutes both with x and y. The relations must be given as a list (!) of polynom triples.

The second input consists of the non-commutative polynomials. `NPREAD` takes as input a relation table and reads a list (!) of polynomials from the current input stream. The output is a list of distributive rational polynomials. `**` denotes exponentiation, the multiplication operator `*` may be omitted. I.e. `x y` denotes `x * y`. All multiplications of variables mean the non-commutative $*$-product. It is possible to specify also more complex polynomial expressions. See 6.13 for the accepted syntax. Be sure to include enough parenthesis to avoid ambiguities.

6.7.2 Procedure Calling

Next three of the above discussed algorithms are called:

1. `LIRRSET` Left IRReducible SET, algorithm `DINLIS`. The input parameters are `t` the relation table and `p` the polynomial list. The output `c` is the left irreducible set of the input.

2. `LGBASE` Left Gröbner BASE, algorithm `DINLGB`, The input parameters are `t` the relation table, `p` the polynomial list and `1` a trace flag (0 = on trace, 1 = trace reduced S-polynomials, >1 = trace as much as possible). The output `c` is the left Gröbner base of the input.

3. `TSGBASE` Two-Sided Gröbner BASE, algorithm `DINCGB`. The input parameters are `t` the relation table and `p` the polynomial list. The output `c` is the two-sided Gröbner base of the input.

```
(* Commutator relations: *)
t:=PREAD().
(a,x,y) L
(
( y ), ( x ), ( x y + a ),
)
PWRITE(t).

(* Non-commutative polynomials: *)
p:=NPREAD(t).
(
( y**3 + x**2 y + x y ),
( x**2 + x )
)
PWRITE(p).

c:=LIRRSET(t,p). (* Left Normalform *)
PWRITE(c).

c:=LGBASE(t,p,1). (* Left G-base *)
PWRITE(c).

c:=TSGBASE(t,p,1). (* Two sided G-base *)
PWRITE(c).
```

Table 6.14: Computing example input

Note that during the computations the number of known commutator relations is increased. At the end 5 new commutator relations have been computed.

In any case the output polynomials are printed to the current output stream with the procedure `PWRITE`. `PWRITE` prints the actual variable list, the actual term order and the list of polynomials, each polynomials starting on a new line.

The produced output is shown in tables 6.15, 6.16 and 6.17.

```
Polynomial in the variables: (a,x,y)
Term ordering:  inverse lexicographical.
Polynomial list:
          (  y**3 -2 a x - a )
          (  x**2 + x )
```

Table 6.15: Computing example left irreducible set

```
Polynomial in the variables: (a,x,y)
Term ordering:  inverse lexicographical.
Polynomial list:
            a**2
          (  x**2 + x )
            a y**2
          (  y**3 -2 a x - a )
```

Table 6.16: Computing example left Gröbner base

```
Polynomial in the variables: (a,x,y)
Term ordering:  inverse lexicographical.
Polynomial list:
            a
          (  x**2 + x )
            y**3
```

Table 6.17: Computing example two-sided Gröbner base

6.7.3 Summary of Computing Times

A summary of computing times for ALDES on IBM 9370/VM, for MAS on an Atari 1040 ST (8 Mhz), an PC AT/386SX (16 Mhz) and an IBM RS6000-520 (20 Mhz) are given

in table 6.18. The timings are obtained with a fresh list of commutator relations in each case, i. e. not in the sequence suggested by the above input listing.

'DINLGB, - irred.' means that the algorithm did not compute a reduced (irreducible) GB. 'DINLGB, + irred.' means that the algorithm computed a reduced (irreducible) GB. 'DINLGB, BBEC, + irr.' means that the algorithm computed a reduced (irreducible) GB and used the condition 'BBEC' to avoid unnecessary reductions. In the later case 22 polynomials have not been reduced according to the criterion from a total of 34 S-polynomials.

'DIN1GB' denotes the MAS algorithm corresponding to algorithm 'GROEBNER'. 'DINCGB' is superior to 'DIN1GB' due to the fact, that the polynomials $p * X_i$ are added to the base at the beginning of the computation, so much more polynomials will be reducible later on. 'DINCGB, BBEC' means that the algorithm computed a reduced (irreducible) two-sided GB and used the condition 'BBEC' to avoid unnecessary reductions. In the later case 9 polynomials have not been reduced according to the criterion from a total of 14 S-polynomials.

Algorithm	IBM 9370/VM ALDES/SAC-2	Atari ST MAS	PC AT/386sx MAS	IBM RS6000 MAS
DINLIS	0.03	< 1.0	< 1.0	0.03
DINLGB, - irred.	1.47			
DINLGB, + irred.	1.47	18.0	13.0	1.30
DINLGB, BBEC, + irr.		6.0		0.47
DIN1GB	1.93			
DINCGB	0.58	8.0	5.0	0.45
DINCGB, BBEC		4.0		0.23

Computing time in seconds.

Table 6.18: Computing Time Summary: Gröbner Bases

The two examples from [Apel, Lassner 1988] need 2 respectively 6 seconds for a reduced left Gröbner base on an Atari ST.

A more complicated example from [Stokes 1989] needs 54 seconds on an Atari ST (respectively 34 seconds using condition BBEC, avoiding 9 of 33 reductions). The problem is to compute a left Gröbner base of the polynomials

```
(  v5 v6 - v2 v3 )
(  v4 v5 - v1 v3 )
```

in an exterior algebra over a vector space generated by `(v1,v2,v3,v4,v5,v6)`. The computation can be done by specification of the commutator relations as $c_{ij} = -1$ and $p_{ij} = 0$, $(1 \leq i < j \leq n)$ and adding the polynomials v_i^2 $(1 \leq i \leq n)$ to the ideal base. The resulting Gröbner base is

```
( v4 v5 - v1 v3 )
```

```
( v5 v6 - v2 v3 )
( v1 v3 v4 )
( v1 v3 v5 )
( v2 v3 v5 )
( v1 v3 v6 - v2 v3 v4 )
( v2 v3 v6 )
```

6.8 Minimal Polynomial in Ideal

In this section we present an algorithm which computes the univariate polynomials of minimal degree in an ideal with finite dimensional residue class vectorspace.

The algorithm takes the commutator relations '`T`' and a left Gröbner base '`F`' as input. Furthermore a natural number $1 \leq i \leq n$ to indicate the variable for which the univariate polynomial is to bee computed.

The Modula-2 listing of the minimal polynomial in an ideal is given in table 6.19:

In step (1) the variable X_i is represented as multivariate polynomial.

In step (2) the powers X_i^k are computed by program `DIPMPV` and the left normal form of the power is computed by program `DINLNF`. Then a system of linear equations between the representations of the powers is constructed. With algorithm `DIRLIS` the system is transformed to row echelon form. Then program `DIGBZT` checks if the system has a solution. If so, the repeat-loop is terminated; otherwise the loop is continued with the next higher power of X_i.

In step (3) finally the univariate polynomial is constructed from the solution of the system of linear equations.

Proposition 6.8.1 *Algorithm* `DINLMPG` *is correct with respect to its specification.*

Proof: This follows from lemma 5.4.3 under the foregoing considerations. The termination follows form the existence of such a polynomial which in turn follows since the vector space dimension of $R/\text{ideal}_l(F)$ is finite. □

6.9 Computation of the Center

We will now turn to the algorithms which implement the computation of elements in the center of a solvable polynomial ring S. Let S be $\mathbf{Q}\{X_1, \ldots, X_n, Q\}$ over the rational numbers $\mathbf{Q}$ with commutator relations Q.

The algorithm `DINCCP` takes the commutator relations and a set of terms as input. It computes a polynomial with indeterminate coefficients (parametric coefficients) which lies in the center of the solvable polynomial ring for any specialization to field elements of the parameters.

```
PROCEDURE DINLMPG(T,i,F: LIST): LIST;
(*Distributive non-commutative left rational minimal polynomial for a
G basis. F is a non-commutative left groebner basis. T is a relation
table. PP is the left minimal polynomial for the i-th variable for F. *)
VAR   C, c, CLP, CP, CS, EINS, e, z, j, EVOREM, EVOCOR,
      l, n, P, p, PP, r, rs, t, X, XP, YP: LIST;
      ec: BOOLEAN;
BEGIN
(*1*) (*initialise. *)
      IF F = SIL THEN PP:=0; RETURN(PP); END;
      z:=FIRST(F); r:=DIPNOV(z); EINS:=RNINT(1); e:=SIL;
      FOR j:=1 TO r DO e:=COMP(0,e); END;
      X:=DIPFMO(EINS,e); l:=1; n:=r+l; PFDIP(X, rs,P);
      P:=PINV(r,P,1); P:=PMPV(n,P,l,1);
(*2*) (*solve linear systems of equations to get the coefficients. *)
      REPEAT XP:=DIPMPV(X,i,l); (*commut.*) l:=l+1;
             XP:=DINLNF(T,F,XP); (*non-commutative*)
             PFDIP(XP, rs,YP); YP:=PINV(r,YP,l); n:=r+l;
             YP:=PMPV(n,YP,l,1); (*commut.*)
             P:=PINV(r,P,1); P:=RPSUM(n,P,YP);
             CP:=PBCLI(r,P); C:=DILFPL(l,CP); CS:=SIL;
             WHILE C <> SIL DO ADV(C, c,C); c:=DIRPEM(c,EINS);
                   CS:=COMP(c,CS); END;
             C:=INV(CS); C:=DIRLIS(C); (*commut.*) t:=DIGBZT(C);
             UNTIL t = 0;
      l:=l-1;
(*3*) (*constuct minimal polynomial. *) PP:=PMON(EINS,l);
      WHILE C <> SIL DO ADV(C, c,C); e:=DIPEVL(c);
            n:=l-FIRST(EVDOV(e));  CLP:=RNNEG(DIPTBC(c));
            p:=PMON(CLP,n); PP:=RPSUM(1,PP,p); END;
      PP:=DIPFP(1,PP);
(*6*) RETURN(PP); END DINLMPG;
```

Table 6.19: Algorithm: DINLMPG

There are routines, which generate sets of terms up to a desired total degree or where the exponents are in a specified range. Furthermore there is a 'driver' program, which calls DINCCP and then substitutes the values 0 and 1 into the center polynomial with indeterminate coefficients to obtain generating elements of the center.

The center polynomial algorithm is constructed after the proof of proposition 3.6.4. The Modula-2 listing of the center polynomial algorithm is given in tables 6.20 and 6.21. The statements concerned with the correct handling of the term orders of the generated systems of linear equations are omitted.

```
PROCEDURE DINCCP(T, E: LIST): LIST;
(*Distributive rational non-commutative polynomial center polynomial.
E is a list of exponent vectors. T is the relation table.
A polynomial in the center of the polynomial ring is returned. *)
VAR   C, CL, CP, EINS, V, EVOREM, EVOCOR, ES, EP, EH, EB, e, ep, f, l,
      n, m, a, P, PP, PE, p, pp, r, r1, r2, rp,  X, Y, Z: LIST;
      ec: BOOLEAN;
BEGIN
(*1*)   (*initialise. *) PP:=0; IF E = SIL THEN RETURN(PP); END;
(*2*)   (*build polynomials from variables. *)
        e:=FIRST(E); r:=LENGTH(e); EINS:=RNINT(1);
        IF r = 0 THEN PP:=DIPFMO(EINS,COMP(1,e)); RETURN(PP) END;
        EP:=EVLGTD(r,1,SIL); EP:=SECOND(EP);
        PE:=DILFEL(EINS,EP); PE:=INV(PE);
        EH:=DILFEL(EINS,E); EH:=DIPLPM(EH);
(*3*)   (*generate linear systems of equations for the coefficients. *)
        EP:=PE; C:=SIL;
        WHILE EP <> SIL DO ADV(EP,Z,EP); P:=0; l:=0; n:=r; ES:=EH;
              REPEAT ADV(ES,X,ES); P:=PINV(r,P,1); l:=l+1; n:=r+l;
                     Y:=DINCCO(T,X,Z);
                     IF Y <> 0 THEN PFDIP(Y, rp,Y); Y:=PINV(r,Y,l);
                        Y:=PMPV(n,Y,l,1); P:=RPSUM(n,P,Y); END;
                     UNTIL ES = SIL;
              CP:=PBCLI(r,P); CP:=DILFPL(l,CP); C:=CCONC(CP,C);
(*3.1*)       C:=DIRLIS(C); (* evord ! *) END;
```

Table 6.20: Algorithm: DINCCP

In step (2) the required polynomials are generated for each variable and from the input terms.

In step (3) the set of linear equations, according to proposition 3.6.4, are generated from the commutators $z * X_i - X_i * z$ for each variable X_i and each input term z. The variable Z contains the term (as polynomial), the variable X contains the variable (as polynomial) and the variable C contains the set of equations. The commutator is computed by algorithm DINCCO. After a commutator has been computed, the augmented set of equations is transformed to staggered form by algorithm DIRLIS. Note, that since $\mathbf{Q}$ is in the center of S, the system of equations is homogeneous and therefore has always a solution.

```
(*5*)   (*construct center polynomial. *)
        PP:=0; r1:=LENGTH(EH); r2:=LENGTH(C); rp:=r1-r2;
        IF rp > 0 THEN EB:=EVLGTD(rp,1,SIL); EB:=SECOND(EB);
                  ELSE EB:=SIL END;
        ES:=EVLINV(EB,0,r); ES:=INV(ES); (*parameters*)
        m:=0; EP:=SIL;
        WHILE C <> SIL DO ADV(C, CL,C); (* CL <> 0 ! *) m:=m+1;
(*5.1*)       (*head term, left hand side*)
              DIPMAD(CL,a,f,CL); (*a = 1 !*)
              e:=EVDOV(f); n:=l-FIRST(e)+1; (*e <> () !*)
              e:=LELT(EH,n); e:=DIPEVL(e); (*wg. sorted *)
              e:=EVINV(e,r,rp); p:=DIPFMO(a,e);
(*5.2*)       (*check for new parameters. *) EP:=INV(EP);
              WHILE m < n DO ADV(ES,ep,ES); EP:=COMP(ep,EP);
                    e:=LELT(EH,m); e:=DIPEVL(e); (*wg. sorted *)
                    e:=EVINV(e,r,rp); e:=EVSUM(e,ep);
                    pp:=DIPFMO(EINS,e); PP:=DIRPSM(PP,pp);
                    m:=m+1; END;
              EP:=COMP(4711,EP); EP:=INV(EP);
(*5.3*)       (*get right hand side. *) pp:=SIL;
              WHILE CL <> SIL DO DIPMAD(CL,a,f,CL); a:=RNNEG(a);
                    e:=EVDOV(f); n:=l-FIRST(e)+1; (*e <> () !*)
                    e:=LELT(EP,n); (*parameters*)
                    pp:=DIPMCP(e,a,pp); END;
              pp:=INV(pp);
              IF pp <> SIL THEN pp:=DIRPPR(p,pp); PP:=DIRPSM(PP,pp) END;
              END;
(*5.4*)   (*check for new parameters. *) EP:=INV(EP);
        WHILE ES <> SIL DO ADV(ES,ep,ES); EP:=COMP(ep,EP);
              e:=LELT(EH,m); e:=DIPEVL(e); (*wg. sorted *)
              e:=EVINV(e,r,rp); e:=EVSUM(e,ep);
              pp:=DIPFMO(EINS,e); PP:=DIRPSM(PP,pp);
              m:=m+1; END;
(*7*)   RETURN(PP); END DINCCP;
```

Table 6.21: Algorithm: DINCCP, contd.

Some caution is required to use the correct term order both for the computations in the polynomial ring respectively in the (commutative) coefficient ring.

At the beginning of step (5) the system of linear equations is in staggered form. Then the solutions are computed as usual by bringing things to the right hand side of the equation. With solutions the coefficients of the center polynomials are constructed. Independent variables are introduced as parameters in the resulting polynomial.

Finally in step (7) the center polynomial is returned.

Proposition 6.9.1 *Algorithm* `DINCCP` *is correct with respect to its specification.*

Proof: This follows directly from the proof of proposition 3.6.4 and the remarks about the algorithm before. Termination follows from the finiteness of the set of input terms. □

As can be seen from the examples, the resulting polynomial with parametric coefficients is not very readable. Therefore in a post processing step we specialize some values for the parameters. Let m be the number of parameters, denote the parameters by y_i, and let $\sigma_j : \{y_1, \ldots, y_m\} \longrightarrow \mathbf{Q}$ be a variable assignment for $1 \leq j \leq m$.

Then define

$$\sigma_j(y_i) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

for $1 \leq i, j \leq m$. In other words, we specialize values such that the resulting polynomials form a linear independent set of solutions considered as vectors.

The listing of the specialization algorithm is not given, but in the examples both the center polynomial and the specialized polynomials will be shown.

6.9.1 Centers of Enveloping Algebras of some Lie Algebras

We include some examples of the computation of centers of enveloping algebras of some finite dimensional Lie algebras over the rational numbers.

The examples are taken from [Patera *et. al.* 1976] and compared to their results. The enumeration of the Lie algebras is as follows: $A_{i,j}$ denotes the j-th Lie algebra of dimension i. The examples are contained in tables 6.22, 6.23, 6.24, 6.25 and 6.26. Note that we only present examples which have polynomial invariants. Actually there are also rational functions and analytical functions which are invariant under the commutator product of the Lie algebra (see example 6.22).

In the examples we list

1. the defining commutator relations of the enveloping algebra of a Lie algebra,
2. the statement for the generation of the terms,
3. the center polynomial with parametric coefficients,

4. the specialized center polynomials,

5. the computing time on an Atari 1040 ST.

The input syntax is as described in section 6.7. `CenterPol` denotes the 'driver' algorithm, which calls `DINCCP` and then specializes the coefficients according to the scheme defined earlier.

`EVLGIL` takes a list of exponents $(e_1, \ldots, e_n)$ and delivers a set of terms with exponents $(a_1, \ldots, a_n)$ with $0 \leq a_i \leq e_i$ for $1 \leq i \leq n$.

`EVLGTD` has inputs (n, d, E), where n is the number of variables, d is the total degree and E is a list of already computed terms (used for internal recursion). It returns a list $(E_0, \ldots, E_d)$ where each E_i is a list of exponents of terms in n variables and of total degree exactly i.

The output furthermore shows the indication on the parameter variables in the coefficients, then the full center polynomial with parametric coefficients and then the specialized polynomials.

The computing times are splitted into the time for input '`read =`', time for evaluation '`eval =`', time for output '`print =`' and time spend in garbage collection '`gc =`'. The first three times do not include garbage collection times. The computing times are summarized also in table 6.27.

```
(* Commutator relations: *) t:=PREAD().
(e1,e2,e3) G
(
( e3 ), ( e1 ), ( e1 e3 - e1 ),
( e3 ), ( e2 ), ( e2 e3 - e2 ),
)
(*generate terms. *) e:=EVLGIL(LIST(1,1,1)).
(*compute polynomial in the center. *) x:=CenterPol(t,e).

Parameters: (X1)

Center polynomial:
          X1

Specialized center polynomials:
          1

Time: read = 0, eval = 4, print = 0, gc = 0.
```

Table 6.22: Lie Algebra: $A_{3,2}$

Note, that in example 6.22 we do not find a polynomial in the center. But in [Patera *et. al.* 1976] it is shown that there are analytic functions, which are invariant under the commutator product in the Lie algebra. Namely $e_1 \exp(-\frac{e_2}{e_1})$.

```
(* Commutator relations: *) t:=PREAD().
(e1,e2,e3) G
(
( e3 ), ( e1 ), ( e1 e3 - e1 ),
( e3 ), ( e2 ), ( e2 e3 + e2 ),
)
(*generate terms. *)
e:=EVLGTD(3,2,NIL). e:=INV(e). e:=FIRST(e).
(*compute polynomial in the center. *) x:=CenterPol(t,e).

Parameters: (X1)

Center polynomial:
            X1 e1 e2

Specialized center polynomials:
            e1 e2

Time: read = 0, eval = 4, print = 0, gc = 0.
```

Table 6.23: Lie Algebra: $A_{3,4}$

In example 6.23 we do not obtain the constants of $\mathbf{Q}$ respectively the specialized polynomial 1, since we did not ask for it. We only asked for polynomials in the center of homogeneous total degree 2.

In example 6.26 we obtain more polynomials than [Patera *et. al.* 1976]. But observe, that the first polynomial is the product of polynomials 4 and 5 and the second polynomial is the product of the polynomials 5 and 6. This raises the question of canonical bases for subrings.

6.9.2 Summary of Computing Times

A summary of the computing times for MAS on an Atari 1040 ST is contained in table 6.27. We list the respective Lie algebra in column one, the dimension of the Lie algebra in column 2, then the total degree and the exponents as input to the term generating algorithm. The last column contains the computing times. The column entitled 'polynomials' contains before slash '/' the number of specialized polynomials as produced by the algorithms and after the slash the number of polynomials as listed in [Patera *et. al.* 1976].

6.10 Example $U(sl(2), f)$

The next examples are taken from [Smith 1990]. He studies a class of algebras which are similar to the enveloping algebra of $sl(2, \mathbf{C})$ over the complex numbers $\mathbf{C}$.

```
(* Commutator relations: *) t:=PREAD().
(e1,e2,e3) G
(
( e2 ), ( e1 ), ( e1 e2 - e3 ),
( e3 ), ( e2 ), ( e2 e3 - e1 ),
( e3 ), ( e1 ), ( e1 e3 + e2 ),
)
(*generate terms. *) e:=EVLGIL(LIST(2,2,2)).
(*compute polynomial in the center. *) x:=CenterPol(t,e).

Parameters: (X1,X2)

Center polynomial:
            (  X2 e3**2 + X2 e2**2 + X2 e1**2 + X1 )

Specialized center polynomials:
            (  e3**2 + e2**2 + e1**2 )
            1

Time: read = 0, eval = 64, print = 0, gc = 16.
```

Table 6.24: Lie Algebra: $A_{3,9}$

```
(* Commutator relations: *) t:=PREAD().
(e1,e2,e3,e4) G
(
( e4 ), ( e2 ), ( e2 e4 - e1 ),
( e4 ), ( e3 ), ( e3 e4 - e2 ),
)
(*generate terms. *) e:=EVLGIL(LIST(0,1,2,1)).
(*compute polynomial in the center. *) x:=CenterPol(t,e).

Parameters: (X1,X2,X3)

Center polynomial:
            ( -2 X3 e1 e3 + X3 e2**2 + X2 e1 + X1 )

Specialized center polynomials:
            ( -2 e1 e3 + e2**2 )
            e1
            1

Time: read = 0, eval = 6, print = 0, gc = 8.
```

Table 6.25: Lie Algebra: $A_{4,1}$

```
(* Commutator relations: *) t:=PREAD().
(e1,e2,e3,e4,e5,e6) G
(
( e2 ), ( e1 ), ( e1 e2 - e3 ),
( e3 ), ( e1 ), ( e1 e3 - e4 ),
( e5 ), ( e1 ), ( e1 e5 - e6 ),
)
(*generate terms. *) e:=EVLGIL(INV(LIST(0,1,2,1,1,1))).
(*compute polynomial in the center. *) x:=CenterPol(t,e).

Parameters: (X1,X2,X3,X4,X5,X6,X7)

Center polynomial:
            ( -2 X7 e2 e4 e6 + X7 e3**2 e6 + X6 e4 e6 -
               X5 e3 e6 + X5 e4 e5 -2 X4 e2 e4 + X4 e3**2 +
               X3 e6 + X2 e4 + X1 )

Specialized center polynomials:
            ( -2 e2 e4 e6 + e3**2 e6 )
            e4 e6
            ( - e3 e6 + e4 e5 )
            ( -2 e2 e4 + e3**2 )
            e6
            e4
            1

Time: read = 0, eval = 140, print = 0, gc = 24.
```

Table 6.26: Lie Algebra: $A_{6,1}$

Lie Algebra	dim	total degree	exponents	polynomials	time
$A_{3,2}$	3	≤ 3	$(1,1,1)$	1/2	4
$A_{3,4}$	3	$= 2$		1/2	4
$A_{3,9}$	3	≤ 6	$(2,2,2)$	2/2	64
$A_{4,1}$	4	≤ 4	$(0,1,2,1)$	3/3	6
$A_{6,1}$	6	≤ 6	$(0,1,2,1,1,1)$	7/5	140

Computing time in seconds.

Table 6.27: Computing Time Summary: Center

The Lie algebra $sl(2)$ over $\mathbf{C}$ is generated by three elements x, y, h with Lie product

$$[x, y] = h, \quad [h, x] = x, \quad [h, y] = -y.$$

The enveloping algebra of $sl(2)$ can be regarded as solvable polynomial ring with respect to a term order $h < x < y$ as

$$S = \mathbf{C}\{h, x, y; \{y * x = xy - h, x * h = hx - x, y * h = hy + y\}\}.$$

As one can see from this representation, we need not take a total degree ordering as term order. So an inverse lexicographical term order is suitable, which suggests, that S could be considered as some Ore extension. This is indeed shown by Smith, that

$$S \cong U(b)[y, \sigma, \delta],$$

where

1. $U(b)$ denotes the enveloping algebra of the 2-dimensional non-abelian Lie algebra b, generated by h and x with commutator relation $[h, x] = x$,
2. σ is defined by $\sigma(x) = x$ and $\sigma(h) = h - 1$ and
3. δ is defined by $\delta(x) = h$ and $\delta(h) = 0$.

Now Smith observes, that by this definition as Ore extension, the definition of $\delta(x)$ can be deliberately replaced by any univariate polynomial in h without loosing the property of being an Ore extension:

$$\delta(x) = f(h).$$

The resulting algebra will be denoted by $R = U(sl(2), f)$ or as solvable polynomial ring by

$$S = \mathbf{C}\{h, x, y; \{y * x = xy - f(h), x * h = hx - x, y * h = hy + y\}\}.$$

Now Smith shows, that the center of R is generated by a unique polynomial which is determined as expression in f

$$\Omega = x * y + y * x + g(h) \in \mathrm{cen}(R).$$

Furthermore let $R' = R/\mathrm{ideal}_t(\Omega)$ and let $I = \mathrm{ideal}_t(w_1, w_2)$ in R' be a two-sided ideal in R'. Then he shows, that any such two-sided ideal I, generated by $w_1 = x^i$ and $w_2 = y^j$ for $i \geq n_\Omega$ and $j \geq n_\Omega$, where $0 < n_\Omega \in \mathbf{N}$ is 'sufficiently' large, is uniquely determined by Ω and hence by f.

In the following examples we took $f = 3/2h(h + 1)$ from [Smith 1990] example 2.4. We first compute $\Omega \in \mathrm{cen}(S)$ in table 6.28 as $\Omega = -2xy - h^3 + h$. Computing times for various sets of terms, determined by exponent vectors, are given in table 6.30.

Having Ω we compute a Gröbner base of a two-sided ideal generated by Ω and various other elements of the form x^i, y^j and products and sums of them. If $i \geq 2$ and $j \geq 2$ then the ideals are all equal to the ideal generated by

$$(h^2 + h), (hx), (x^2), (hy + y), (xy), (y^2).$$

Computing times for various generating sets for the ideal are also given in table 6.30.

```
(* Commutator relations: *) t:=PREAD().
(h,x,y) L
(
( x ), ( h ), ( h x - x ),
( y ), ( h ), ( h y + y ),
( y ), ( x ), ( x y - 3/2 h ( h + 1 ) ),
)

(*generate terms. *) e:=EVLGIL(LIST(1,1,4)).

(*compute polynomial in the center. *) x:=CenterPol(t,e).

Parameters: (X1,X2)

Center polynomial:
            ( -2 X2 x y - X2 h**3 + X2 h + X1 )

Specialized center polynomials:
            ( -2 x y - h**3 + h )
             1

Time: read = 0, eval = 50, print = 0, gc = 16.
```

Table 6.28: Center of $U(sl(2), f)$

```
(* Non-commutative polynomials: *) p:=NPREAD(t).
(
( -2 x y - h**3 + h ),
( x**3 ),
( y**3 ),
)

(* Two sided G-base: *) c:=TSGBASE(t,p,1).

Polynomial in the variables: (h,x,y)

Term ordering:  inverse lexicographical.

Polynomial list:
            (  h**2 + h )
            (  h x )
            (  x**2 )
            (  h y + y )
            (  x y )
            (  y**2 )
```

Table 6.29: Two-sided Ideal in $U(sl(2), f)$

6.10.1 Summary of Computing Times

A summary of the computing times of the above examples are given in table 6.30.

The first column denotes what has been computed: Ω in the center, or the two-sided ideals $\text{ideal}_t(\Omega, w_1, w_2)$. The other generators w_1, w_2 are of the form x^i, y^j and products and sums of them. If $i \geq 2$ and $j \geq 2$ then the generators of the ideal from table 6.29 are computed. Otherwise the two-sided Gröbner base of the ideal is equal to $\{x, y\}$ and $\{1\}$ respectively.

The second column shows the maximal exponent vectors for the searched center polynomial. So an entry (l, m, n) means, that the terms have degrees $0 \leq i \leq l$ in the variable y, $0 \leq i \leq m$ in the variable x and $0 \leq i \leq n$ in the variable h.

The third column shows the computing times in seconds for MAS on an Atari 1040 ST. As can be seen the times vary drastically by the number of terms requested for the center polynomial and the degrees of the generating elements of the two-sided ideals.

	exponents	time
Ω	$(1,1,3)$	30
Ω	$(1,1,4)$	50
Ω	$(1,1,5)$	76
Ω	$(1,1,6)$	112
Ω	$(1,1,7)$	160
Ω	$(1,1,8)$	242
Ω	$(2,2,3)$	144
Ω	$(2,2,4)$	284
$\text{ideal}_t(\Omega, 1)$		0
$\text{ideal}_t(\Omega, x, y)$		4
$\text{ideal}_t(\Omega, x^2, y^2)$		26
$\text{ideal}_t(\Omega, x^3, y^3)$		64
$\text{ideal}_t(\Omega, x^4, y^4)$		130
$\text{ideal}_t(\Omega, x^5, y^5)$		226
$\text{ideal}_t(\Omega, x + y)$		4
$\text{ideal}_t(\Omega, x^2 + y^2)$		24
$\text{ideal}_t(\Omega, x^3 + y^3)$		92
$\text{ideal}_t(\Omega, x^2)$		34
$\text{ideal}_t(\Omega, x^3)$		66
$\text{ideal}_t(\Omega, (x + y)^3)$		688

Computing time in seconds.

Table 6.30: Computing Time Summary: $U(sl(2), f)$

6.11 Concluding Remarks

We have presented efficient algorithms for the computation in solvable polynomial rings. The algorithms may be used for computations of ideal bases in enveloping algebras of finite dimensional Lie algebras, in iterated differential operator rings or in Clifford algebras.

Furthermore the algorithms may serve as a base for the implementation of further constructive methods such as computation of syzygies, quotient fields, residue class rings, etc.

There are several possible improvements to the algorithms. One important improvement would be to incorporate an fast algorithm for the solution of systems of linear equations for the computation of elements in the center.

An implementation of the algorithms for syzygy computations is given in [Philipp 1991]. The algorithms for parametric Gröbner bases in the commutative case are implemented in [Schönfeld 1991].

Chapter 7

Comprehensive Gröbner Bases

In this chapter we extend the theory of comprehensive Gröbner bases, as introduced in [Weispfenning 1990], from commutative polynomial rings to solvable polynomial rings. An outline of this theory was given in [Kredel, Weispfenning 1990]. In the current setting we assume that the coefficients commute with the variables.

The main point of comprehensive Gröbner bases is that the construction of a Gröbner base is not performed over a field, but over a ring (with parameters) such that the specialization of the parameters to elements of **any** field leads to a Gröbner base over this field. In this sense such an ideal base is a *comprehensive Gröbner base*. In general the property of beeing a Gröbner base is lost under specialization of the coefficients as the following example from [Weispfenning 1990] shows. Let $S = \mathbf{Q}[U][X, Y]$ be a polynomial ring in X, Y with parameter U and with $X < Y$. Let

$$F = \{X + 1, UY + X\},$$

then F is a Gröbner base in $\mathbf{Q}[U, X, Y]$ wrt. $<$. Let $\sigma : \mathbf{Q}[U] \longrightarrow \mathbf{K}$ be a specialization, which embedds $\mathbf{Q}$ into $\mathbf{K}$ and with $\sigma(U) \in \mathbf{K}$. Then $\sigma(F)$ (defined by applying σ to the coefficients) is a Gröbner base in $\mathbf{K}[X, Y]$ for any σ with $\sigma(U) \neq 0$. But for a specialization with $\sigma(U) = 0$ we have $\sigma(F) = \{X + 1, X\}$ and we see that $1 \in \text{ideal}(\sigma(F))$ but 1 is not reducible with respect to $\sigma(F)$. So $\sigma(F)$ can not be a Gröbner base. To obtain a comprehensive Gröbner base one would consider also the case when $U = 0$ and under this condition the polynomial $X + 1 - (UY + X) = -UY + 1 \in \text{ideal}(F)$. So in this example

$$G = \{X + 1, UY + X, -UY + 1\}$$

would be a comprehensive Gröbner base, since now also under the specialization $\sigma(U) = 0$ we see that $\sigma(G) = \{X + 1, X, 1\}$ is a Gröbner base.

The plan for this chapter is as follows. In the first section we recall some definitions and we extend the $*$ product to a parametric $*$-product, i.e. to a $*$-product in a solvable polynomial ring over a 'parameter ring'. Furthermore we present a parametric reduction and a parametric S-polynomial. Next we give a precise statement of specializations and

give a criterion on the head terms of a Gröbner base under specialization. Then we define comprehensive Gröbner bases.

The construction of a comprehensive Gröbner base is performed by the usual process of building S-polynomials and reductions. But now the conditions under which the steps are performed are recorded in a set of conditions. This leads first to a tree of ideal bases where the nodes are labeled by the set of conditions under which the step has been performed. This tree of ideal bases is called a Gröbner system and a comprehensive Gröbner base is afterwards obtained by taking the union of all ideal bases at the leaves of the tree. A condensed coding of the conditions applied to the coefficients of the polynomials under consideration is called a *colouring*. A coefficient is coloured *red* if it is non-zero under the current set of conditions, it is coloured *green* if it is zero under the current set of conditions, otherwise is coloured *white*. A determined set of polynomials is a set of polynomials together with a set of conditions such that the first non-green term of a polynomial is coloured red. This term then serves as a head term during the following steps of the reduction and S-polynomial construction. Using these constructions the algorithms for the construction of left (right, two-sided) Gröbner systems are developed.

Finally the parametric ideal member ship problem is discussed. It has important applications in the proof of the strong Nullstellensatz. We have not included a treatment of parametric modules of syzygies and deformation of residue algebras, this will be some future work. Applications to quantifier elimination are discussed in chapter 8 when we have introduced the required Nullstellen Sätze.

7.1 Parametric Solvable Algebras

Let $\mathbf{R}$ be a commutative Noetherian domain and let $\mathbf{R}[U_1,\ldots,U_m]$ be a polynomial ring in the commuting variables $\{U_1,\ldots,U_m\} = U$. Assume furthermore, that the variables commute with the coefficients. For a two-sided ideal I in $\mathbf{R}[U_1,\ldots,U_m]$ with $I \cap \mathbf{R} = \{0\}$ define $R = \mathbf{R}[U_1,\ldots,U_m]/I$ so that $R = \mathbf{R}[u_1,\ldots,u_m]$ with $u_i = U_i + I$ for $i = 1,\ldots,m$. Recall the axioms of solvable polynomial rings 3.2.1 adapted for the current situation:

Axioms 7.1.1 *$S = R\{X_1,\ldots,X_n;Q\}$ denotes a polynomial ring of solvable type over R in the variables $\{X_1,\ldots,X_n\}$ for a fixed term order $<_T$ if the following axioms are satisfied:*

1. *$(S,0,1,+,-,*,<)$ is an associative ring extending R and with admissible term order $<$.*
2. *(a) For all $a,b \in R$, $t \in T(X_1,\ldots,X_n)$, $a*b*t = a*(bt) = (a\cdot b)\cdot t = abt$.*
   (b) For all $1 \leq i \leq n$, $s \in T(X_1,\ldots,X_i)$, $t \in T(X_i,\ldots,X_n)$, $s*t = st$.
3. *For all $1 \leq i < j \leq n$ there exist $0 \neq c_{ij} \in \mathrm{cen}(R)$, $p_{ij} \in S$ such that*

$$X_j * X_i = c_{ji}X_iX_j + p_{ij}$$

and $p_{ij} < X_iX_j$ in the quasi-order on S induced by the termorder on T. Moreover if C is the multiplicative subset generated by the c_{ij} in R, then $0 \notin C$.

4. *For all $1 \leq i \leq n$ and all $0 \neq a \in R$*

$$X_i * a = aX_i.$$

In the special case when $\mathbf{R}$ is a field and $m = 0$ we obtain a solvable polynomial ring as defined in axioms 3.2.1(1, 2, 3, 4) in case the $c_{ai} = 1$ and the $p_{ai} = 0$ for $1 \leq i \leq n$ and $a \in R$. The notation for parametic solvable polynomial rings will be

$$S = R\{X_1, \ldots, X_n; Q\},$$

where Q denotes the parametric commutator relations of axiom 7.1.1(3). The commutator relations Q' of axiom 7.1.1(4) will not be written according to our earlier convention. S will be called the *polynomial ring*, R will be called the *coefficient ring* and $\mathbf{R}$ will be called the *base coefficient ring*.

The next goals considered in the rest of the section are to prove a parametric product lemma and some notes on parametric reduction and S-polynomials.

7.1.1 Parametric Product

Lemma 7.1.2 *Let $\mathbf{R}$ be a commutative Noetherian domain, $m \in \mathbf{N}$, $R = \mathbf{R}[u_1, \ldots, u_m]$. Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable algebra as defined in 7.1.1 with respect to a $*$-compatible term order $<$. Let C be the multiplicative subset of R generated by the c_{ij} from the commutator relations Q. Then for $0 \neq f, g \in S$ one can compute $0 \neq c \in C$ and $p \in S$ with $p < f \cdot g$ such that*

$$f * g = c \cdot f \cdot g + p.$$

c and p are uniquely determined by these properties and the coefficients of p in R are polynomials in the c_{ij}, the coefficients of all p_{ij} from the commutator relations Q and of the coefficients of f, g. Furthermore these polynomials are formed uniformly, independently of the ring R.

The proof requires some preparations. In the following let $n \in \mathbf{N}$ be fixed and let $<$ be a fixed admissible $*$-compatible term order.

Definition 7.1.3 *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring. For $1 \leq i < j \leq n$ let T_{ij} be finite subsets of T. Let $\mathcal{T} = \{T_{ij} \ : \ 1 \leq i < j \leq n\}$. Then S* is of type *$\mathcal{T}$ if all terms occurring in some commutator polynomial p_{ij} from Q are elements of T_{ij} for $1 \leq i < j \leq n$. In other words $T(p_{ij}) \subseteq T_{ij}$. $\mathcal{T}$ is called a* type for a solvable algebra *if for a given term order $<$ on T we have $t < X_iX_j$ for all $t \in T_{ij}$ for $1 \leq i < j \leq n$.*

The proof of the parametric product lemma is by the following two lemmas, which depend inductively on each other.

Lemma 7.1.4 *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable polynomial ring with terms T. Let $\mathcal{T}$ be a type of a solvable polynomial ring and let Q be the parametric commutator relations: $Q = \{X_j * X_i = c_{ij}X_iX_j + \sum_{e\in J_{ij}} d_{eij}e \ : \ J_{ij} \in \mathcal{T}\}$. If lemma 7.1.5 holds for all $\vartheta' < \vartheta$, $\vartheta, \vartheta' \in T$, then for $u, v \in T$ with $uv = \vartheta$ one can construct an expression*

$$h_{uv\vartheta} = \sum_{e\in J_{uv}} z_{e,uv\vartheta}e = h_{uv\vartheta}(\{c_{ij}\}, \{d_{eij}\}),$$

such that

1. *$J_{uv} = J(u, v, \vartheta)$ and*
2. *the $z_{e,uv\vartheta} = z_{e,uv\vartheta}(\{c_{ij}\}, \{d_{eij}\})$ for $e \in J_{uv}$ are multivariate polynomials in the $\{c_{ij}\}$ and the $\{d_{eij}\}$ with integer coefficients.*
3. *For every ground ring $\mathbf{K}$ and every specialization of the c_{ij} to elements $0 \neq \hat{c}_{ij} \in \mathbf{K}$ and of d_{eij} to elements $\hat{d}_{eij} \in \mathbf{K}$ such that $\hat{S} = \mathbf{K}\{X_1, \ldots, X_n; Q(\{\hat{c}_{ij}\}, \{\hat{d}_{eij}\})\}$ is a solvable polynomial ring the following holds*

$$u * v = h_{uv\vartheta}(\{\hat{c}_{ij}\}, \{\hat{d}_{eij}\}).$$

Moreover $\mathrm{HT}(u * v) = \mathrm{HT}(h_{uv\vartheta}) = uv$, $\mathrm{HC}(u * v) = \mathrm{HC}(h_{uv\vartheta}) = z_{(uv),uv\vartheta}$.

Notation: $Z_{uv\vartheta} = \{z_{e,uv\vartheta}\}_{e\in J_{uv}}$.

Proof: The proof is by Noetherian induction on $t = uv$ assuming that lemma 7.1.5 holds for all products $f * g$ with $\mathrm{HT}(f)\mathrm{HT}(g) = \vartheta' < t$.

Case: $u = 1$ respectively $v = 1$. Then according to lemma 3.2.4(3) we have $u * v = uv$ and so let 1) $J_{uv} = \{v\}$, 2) $z_{v,uv\vartheta} = 1$, 3) $h_{uv\vartheta} = v$, respectively let 1) $J_{uv} = \{u\}$, 2) $z_{u,uv\vartheta} = 1$, 3) $h_{uv\vartheta} = u$.

Case: $t > 1$ and assume the claim is true for all $t' < t$ and that lemma 7.1.5 holds for all products $f * g$ with $\mathrm{HT}(f)\mathrm{HT}(g) < t$. If $u \in T(X_1, \ldots, X_i)$, $v \in T(X_i, \ldots, X_n)$ for some $1 \leq i \leq n$ then again by lemma 3.2.4(3) we have $u * v = uv = t$ and so 1) $J_{uv} = \{t\}$, 2) $z_{t,uv\vartheta} = 1$, 3) $h_{uv\vartheta} = uv$ and we are done. Otherwise let $u \in T(X_h, \ldots, X_j)$, $v \in T(X_i, \ldots, X_k)$ with $1 \leq h \leq j \leq n$, $1 \leq i \leq k \leq n$, $i < j$ and h, i maximal, j, k minimal and consider the following subcases.

Subcase 1, $\underline{h \leq i}$: Let $u = x_h u'$ with $u' \in T(X_h, \ldots, X_j)$, then $u' < u$ and $u * v = X_h u' * v = X_h * u' * v$. By induction assumption $u * v = X_h * h_{u'v\vartheta} = X_h * \sum_{e\in J_{u'v}} z_{e,u'v\vartheta}e$ $= \sum_{e\in J_{u'v}} z_{e,u'v\vartheta}X_h * e = z_{(u'v),u'v\vartheta}X_h * u'v + \sum_{e\in J_{u'v}\setminus\{u'v\}} z_{e,u'v\vartheta}X_h * e$. Since $X_h * e < uv$ for all $e \in J_{u'v} \setminus \{u'v\}$, the induction assumption can be applied to the products in the second sum. Let $X_h * e = \sum_{e'\in J_{X_h e}} z_{e',X_h e\vartheta}e'$ then

$$u * v = z_{(u'v),u'v\vartheta}uv + \sum_{e''\in J_{uv}} z_{e'',uv\vartheta}e'' \qquad (*)$$

where 1) $J_{uv} = \{ee' \ : \ e \in J_{u'v}, e' \in J_{X_h e}\}$, 2) $z_{e,uv\vartheta} = z_{e,uv\vartheta}(\{c_{ij}\},\{d_{kij}\})$ for $e \in J_{uv}$, 3) $h_{uv\vartheta}$ as in $(*)$.

The subcase 2, $\underline{j \leq k}$ is handled similarly. Subcase 3, $\underline{i < h \text{ and } k < j}$ is handled as follows: Let $u = u'X_j$, $v = X_i v'$ with $u' \in T(X_h,\ldots,X_j)$, $v' \in T(X_i,\ldots,X_k)$, then $u' < u$, $v < v'$ and $u * v = u' * X_j * X_i * v' = u' * (c_{ij}X_iX_j + p_{ij}) * v' = u' * (c_{ij}X_iX_j) * v' + u' * (p_{ij}) * v'$. Now since $\mathrm{HT}(u')\mathrm{HT}(p_{ij})\mathrm{HT}(p') < t$ lemma 7.1.5 can be applied (two times) to the second summand, which gives $J_{u'X_iX_jv'}$ and the respecive z and h. If we can furthermore construct J', z', h' for the first summand we have 1) $J_{uv} = J' \cup J_{u'X_iX_jv'}$, 2) $z_{e'',uv\vartheta} = z'_{e'} + z_{e,uv\vartheta}$ if $e'' = e + e'$, 3) $h_{uv\vartheta} = h_{uv\vartheta}(\{c_{ij}\},\{d_{kij}\})$ as claimed.

For the first summand observe that $u' * c_{ij}X_i < uv$ and $X_j * v' < uv$. So induction can be applied to the partial products $(u' * c_{ij}X_i) * (X_j * v') = (z_{d'}c_{ij}X_iu' + h'_{X_iu'\vartheta}) * (z_{d''}v'X_j + h'_{v'X_j\vartheta})$, where h' is h without headterm. Distributing $*$ over $+$ and applying three times lemma 7.1.5 to the three last summands (yielding h'') we obtain $u * v = (z_{d'}c_{ij}X_iu') * (z_{d''}v'X_j) + h''_{X_iu'v'X_j\vartheta}$. To the first summand by axiom 3.2.1(2) or 7.1.1(2) the assumption of the third subcase can be applied so $z_{d'}c_{ij}X_i * (u' * z_{d''} * v') * X_j = z_{d'}c_{ij}X_i * (z_{d'''}u'v' + h'_{u'v'\vartheta}) * X_j$. Since $X_i * h'_{u'v'\vartheta} * X_j < uv$ we can expand the products and apply lemma 7.1.5 on the second product. By assumption of subcase 3 the first summand is now a commutative product $z_{d'}c_{ij}X_iz_{d'''}u'v'X_j = z_{(uv),uv\vartheta}uv$. Collecting all coefficients of equal terms we obtain the desired J', $z' = z_{(uv),uv\vartheta}$ and the h'. This proves all subcases and cases and thus proves the lemma. □

Lemma 7.1.5 *Let $S = R\{X_1,\ldots,X_n;Q\}$ be a parametric solvable polynomial ring with terms T. Let $\mathcal{T}$ be a type of a solvable polynomial ring and let Q be the parametric commutator relations: $Q = \{X_j * X_i = c_{ij}X_iX_j + \sum_{e\in J_{ij}} d_{eij}e \ : \ J_{ij} \in \mathcal{T}\}$. Then for polynomials $0 \neq f, g \in S$ with $\mathrm{HT}(f)\mathrm{HT}(g) = \vartheta$, $\vartheta \in T$, under the assumption that lemma 7.1.4 holds for ϑ, with indeterminate coefficients $f = \sum_{e\in J_f} a_e e$ and $g = \sum_{e'\in J_g} b_{e'}e'$ one can construct an expression*

$$h_{fg\vartheta} = \sum_{e\in J_{fg}} z_{e,fg\vartheta}e = h_{fg\vartheta}(\{c_{ij}\},\{d_{eij}\},\{a_k\},\{b_k\}),$$

such that

1. *$J_{fg} = J(f,g,\vartheta)$ and*
2. *the $z_{e,fg\vartheta} = z_{e,fg\vartheta}(\{c_{ij}\},\{d_{eij}\},\{a_k\},\{b_k\})$ for $e \in J_{fg}$ are multivariate polynomials in the coefficients $\{c_{ij}\},\{d_{eij}\},\{a_k\},\{b_k\}$ with integer coefficients.*
3. *For every ground ring $\mathbf{K}$ and every specialization of the c_{ij} to elements $0 \neq \hat{c}_{ij} \in \mathbf{K}$ and of d_{eij} to elements $\hat{d}_{eij} \in \mathbf{K}$ such that $\hat{S} = \mathbf{K}\{X_1,\ldots,X_n;Q(\{\hat{c}_{ij}\},\{\hat{d}_{eij}\})\}$ is a solvable polynomial ring and of a_k, b_k to arbitrary elements $\hat{a}_k, \hat{b}_k \in \mathbf{K}$ the following holds*

   $$f * g = h_{fg\vartheta}(\{\hat{c}_{ij}\},\{\hat{d}_{eij}\},\{a_k\},\{b_k\}).$$

   Moreover $\mathrm{HT}(f*g) = \mathrm{HT}(h_{fg\vartheta}) = \mathrm{HT}(f)\mathrm{HT}(g)$, $\mathrm{HC}(f*g) = \mathrm{HC}(h_{fg\vartheta}) = z_{(uv),fg\vartheta}$, where $u = \mathrm{HT}(f)$ and $v = \mathrm{HT}(g)$.

Notation: $Z_{fg\vartheta} = \{z_{e,fg\vartheta}\}_{e \in J_{fg}}$.

Proof: By induction on the product of the head terms of f and g and using lemma 7.1.4. By distributivity $f * g = (\sum_{e \in J_f} a_e e) * (\sum_{e' \in J_g} b_{e'} e') = \sum_{e \in J_f} \sum_{e' \in J_g} a_e e * b_{e'} e'$. So

$$f * g = \sum_{e \in J_f} \sum_{e' \in J_g} a_e b_{e'} e * e'.$$

By lemma 7.1.4 (using also induction assumption) each parametric product of $e * e'$ is an expression

$$h_{ee'\vartheta}(\{c_{ij}\}, \{d_{kij}\}).$$

Collecting the coefficients of the same terms we obtain

$$f * g = \sum_{e \in J_{fg}} z_{e,fg\vartheta} e$$

where each $z_{e,fg\vartheta}$ is a multivariate polynomial in the $\{c_{ij}\}, \{d_{kij}\}, \{a_k\}, \{b_k\}$ with integer coefficients. Moreover for the head term $\mathrm{HT}(f * g) = \mathrm{HT}(f)\mathrm{HT}(g) = w$ and the head coefficient of $\mathrm{HC}(f * g)$ is $a_u b_v z_{w,uv\vartheta}$, where $\mathrm{HT}(f) = u$ and $\mathrm{HT}(g) = v$. □

Proof: of Lemma 7.1.2. In lemma 7.1.5 specialize the $\{c_{ij}\}, \{d_{kij}\}, \{a_k\}, \{b_k\}$ to the coefficients of the polynomials f, g and to the coefficients of the commutator relations in Q. Combining lemma 7.1.5 and lemma 7.1.4, we see that lemma 7.1.5 holds for all $\vartheta \in T$. Then the claim follows by lemma 7.1.5. □

7.1.2 Parametric Reduction and S-Polynomial

Left reduction and S-polynomials in parametric solvable polynomial rings are defined in a way that no divisions by elements in the coefficient ring are necessary. Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable polynomial ring.

Left reduction: let $f, f' \in S$ and let $H \subseteq S$. Then $f \longrightarrow_H f'$ if there exists a polynomial $0 \neq p \in H$ with $\mathrm{HT}(p) = t$, a term $s \in T(f)$ such that $s = ut$ and

$$f' = df - d'u * p,$$

where $d, d' \in R$ with $d' = \mathrm{coeff}(s, f)$, $d = \mathrm{coeff}(s, u * p)$. By construction we have $d \cdot f - f' \in \mathrm{ideal}_l(H)$.

S-polynomial: let $f, g \in S$ and let $u, v \in T$ such that $\mathrm{lcm}(\mathrm{HT}(f), \mathrm{HT}(g)) = u\mathrm{HT}(f) = v\mathrm{HT}(g)$. Let $a = \mathrm{coeff}(t, v * g)$ and $b = \mathrm{coeff}(t, u * f)$, then

$$\mathrm{LSP}(f, g) = au * f - bv * g.$$

Lemma 7.1.6 *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable polynomial ring with commutator relations Q. Let $0 \neq f, g \in S$, $f' \in S$ and let $H \subseteq S$. Then the following hold:*

1. *If $f \longrightarrow_H f'$ in S, then the coefficients of f' in R are polynomials in the coefficients in R of the polynomials in $\{f\} \cup H \cup Q$. Moreover $f' < f$.*

2. *The coefficients in R of $h = \mathrm{LSP}(f, g)$ are polynomials in the coefficients in R of the polynomials in $\{f, g\} \cup Q$.*

Proof: In both cases f' and h are differences of products of parametric polynomials, so the claim follows by the parametric product lemma 7.1.2. The product lemma shows also that the polynomials are formed uniformly, independently of the ring R if $\mathbf{R}$ is commutative.

The claim $f' < f$ follows from the fact, that the term s in f does no more appear in f', all terms $u \in T(f)$ with $u > s$ remain in $T(f')$ and that only terms less than s from $u * p$, $0 neq p \in H$ are newly entered into $T(f')$. □

7.2 Specializations

Recall that $\mathbf{R}$ denotes an commutative domain. Furthermore assume that $\mathbf{R}$ and consequently by the Hilbert basis theorem $R = \mathbf{R}[u_1, \ldots, u_m]$ is Noetherian.

Definition 7.2.1 *A* specialization *of $R = \mathbf{R}[u_1, \ldots, u_m]$ is a ring homomorphism $\sigma : R \longrightarrow \mathbf{K}'$, where $\mathbf{K}'$ is a commutative field. Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable algebra over R. Let $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q'\}$ be a solvable polynomial ring over $\mathbf{K}'$ with commutator relations Q' such that for all $1 \leq i < j \leq n$ there exist $0 \neq c'_{ij} \in \mathbf{K}'$, $p'_{ij} \in S'$ such that*

$$X_j * X_i = c'_{ji} X_i X_j + p'_{ij} \quad \in Q'$$

and $p'_{ij} < X_i X_j$. Let $\bar{\sigma} : S \longrightarrow S'$ be the natural extension of σ obtained by applying σ coefficientwise. Then σ is called admissible for S and S' *if for $1 \leq i < j \leq n$*

$$\sigma(c_{ij}) = c'_{ij} \quad \text{and} \quad \bar{\sigma}(p_{ij}) = p'_{ij}.$$

Let $\mathbf{K}'$ be an extension field of $\mathbf{K}$, then a specialization $\sigma : R \longrightarrow \mathbf{K}'$ of R is called *epi specialization* if $\mathbf{K}' = Q(\sigma(R))$, the quotient field of $\sigma(R)$. Since R is assumed to be a commutative Noetherian domain, and σ is injective, then $\sigma(R)$ is a commutative Noetherian domain too, so the quotient field $Q(\sigma(R))$ always exists.

Lemma 7.2.2 *Let $\sigma : R \longrightarrow \mathbf{K}'$ be a specialization of R that is admissible for $S = R\{X_1, \ldots, X_n; Q\}$ and $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q'\}$. Then $\bar{\sigma} : S \longrightarrow S'$ is a ring homomorphism with respect to $*$. So whenever $0 \neq f, g \in S$ and $f * g = c \cdot f \cdot g + p$ and $\bar{\sigma}(f) * \bar{\sigma}(g) = c' \cdot \bar{\sigma}(f) \cdot \bar{\sigma}(g) + p'$ are as in proposition 3.2.5 then*

$$c' = \sigma(c) \quad \text{and} \quad p' = \bar{\sigma}(p).$$

Proof: By the parametric product lemma 7.1.2. □

Proposition 7.2.3 *Let $<$ be a term order on T and let $\mathcal{T}$ be a type for a solvable algebra wrt. $<$. Let $\mathbf{R}$ be a commutative Noetherian domain. Then there exists a ring $R = \mathbf{R}[u_1, \ldots, u_m] = \mathbf{R}[U_1, \ldots, U_m]/I$, I a two-sided ideal, and a parametric solvable algebra $S = R\{X_1, \ldots, X_n; Q\}$ such that for all fields $\mathbf{K}'$, all solvable algebras $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q'\}$ of type $\mathcal{T}$ and all ring homomorphisms $\phi : \mathbf{R} \longrightarrow \mathbf{K}'$, ϕ has an extension to a specialization $\sigma : R \longrightarrow \mathbf{K}'$ that is admissible for S and S'. In particular if σ is surjective then $S' = \sigma(S)$.*

Proof: Let $\mathcal{T} = \{T_{ij} \ : \ 1 \leq i < j \leq n\}$. For all $1 \leq i < j \leq n$ we let c_{ij} be an indeterminate and p_{ij} the most general polynomial with indeterminate coefficients containing all terms in T_{ij}. Let $U_1, \ldots, U_m$ be a list of all these indeterminates. For every pair of terms $s, t \in T$ let c_{st} and p_{st} be determined by the parametric product lemma 7.1.2 in such a way that

$$s * t = c_{st} st + p_{st} \text{ with } 0 \neq c_{st} \in C' \text{ and } p_{st} < st \tag{1}$$

in every parametric solvable algebra $S = R'\{X_1, \ldots, X_n; Q\}$ satisfying axioms 7.1.1, and $R' = \mathbf{R}[U_1, \ldots, U_m]$. Then (1) together with 7.1.1 (2) determines the structure constants in R' of S with respect to the basis T of S. By proposition 3.3.6 (see also [Jacobson 1962](p 4)), there exists a set A of polynomials in these structure constants with the following property: for $u_1, \ldots, u_m \in \mathbf{R}$, $q(u_1, \ldots, u_m) = 0$ for all $q \in A$ iff the algebra on the free $\mathbf{R}$-module with basis T and multiplication $*$ defined by (1) is associative. Let now I be the ideal generated by A in the polynomial ring $\mathbf{R}[U_1, \ldots, U_m]$. Then $I \cap \mathbf{R} = \{0\}$ since there exists the solvable algebra $\mathbf{K}'[X_1, \ldots, X_n]$, where $\mathbf{K}' = Q(\mathbf{R})$ is the quotient field of $\mathbf{R}$. Define $R = \mathbf{R}[U_1, \ldots, U_m]/I = \mathbf{R}[u_1, \ldots, u_m]$, $u_i = U_i + I$ for $1 \leq i \leq m$ and define the R-algebra S with basis T over R by (1). Then by construction S is associative and hence a parametric solvable polynomial ring over R satisfying 7.1.1.

Let now $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q'\}$ be a solvable algebra of type $\mathcal{T}$ over a field $\mathbf{K}'$ satisfying for $1 \leq i <\leq n$:

$$X_j * X_i = c'_{ij} X_i X_j + p'_{ij} \quad \in Q'$$

with $0 \neq c'_{ij} \in \mathbf{K}'$ and $p'_{ij} \in S'$, $p'_{ij} < X_i X_j$. Let $v_1, \ldots, v_m$ be the m-tuple consisting of c'_{ij} and the coefficients of the p'_{ij} listed in the same order as the m-tuple $(U_1, \ldots, U_m)$ for the c_{ij} and the coefficients of the p_{ij}. Let $\phi : \mathbf{R} \longrightarrow \mathbf{K}'$ be a ring homomorphism and let $\bar{\phi} : \mathbf{R}[U_1, \ldots, U_m] \longrightarrow \mathbf{K}'$ be its canonical extension with $\bar{\phi}(U_i) = v_i$. Then by definition of A, $\bar{\phi}(g(U_1, \ldots, U_m)) = 0$ for all $q \in A$. Consequently $\ker(\bar{\phi}) \supseteq I$ and so $\bar{\phi}$ induces a specialization $\sigma : R \longrightarrow \mathbf{K}'$ with $\bar{\sigma}(u_i) = v_i$. By construction σ is admissible for S and S' and so by lemma 7.2.2 $\bar{\sigma} : S \longrightarrow S'$ is a ring homomorphism. Finally $\bar{\sigma}$ is surjective if σ is surjective. $\square$

7.2.1 Prime Spectrum

Let R be a ring, then the set of all prime ideals is called the *prime spectrum of* R and is denoted by spec(R). The set of all complete prime ideals is called the *complete prime*

spectrum of R and is denoted by c-spec(R). In this section we need some facts about Noetherian integral domains and the so called Ore condition as discussed in section 8.2.2. Although we assume the coefficient ring R to be commutative, and so the sets of prime and complete prime ideals coincide, we will speak of complete prime ideals to stress this fact.

Definition 7.2.4 *Let* $S = R\{X_1, \ldots, X_n; Q\}$ *be a parametic solvable algebra over* R. *Recall that for* $f \in S$, $T(f)$ *denotes the set of all terms that occur in* f *with non vanishing coefficient:* $T(f) = \{t \in T \ : \ \text{coeff}(t, f) \neq 0\}$. *For* $\pi \in$ c-spec(R) *let* $T_\pi(f)$ *denote the set of all terms that occur in* f *with coefficient not in* π*:*

$$T_\pi(f) = \{t \in T \ : \ \text{coeff}(t, f) \notin \pi\}.$$

$\text{HT}_\pi(f)$ *denotes the maximal element of* $T_\pi(f)$ *with respect to the given term order.* $\text{HC}_\pi(f) = \text{coeff}(\text{HT}_\pi(f), f)$. *If* $T_\pi(f) = \emptyset$ *then* $\text{HT}_\pi(f)$ *and* $\text{HC}_\pi(f)$ *are undefined. For* $F \subseteq S$ *let* $\text{HT}_\pi(F) = \{\text{HT}_\pi(f) \ : \ f \in F\}$.

If R is an integral domain then for $\pi = \{0\}$ note that $T_{\{0\}}(f) = T(f)$, $\text{HT}_{\{0\}}(f) = \text{HT}(f)$ and $\text{HC}_{\{0\}}(f) = \text{HC}(f)$.

Lemma 7.2.5 *Let* $S = R\{X_1, \ldots, X_n; Q\}$ *be a parametic solvable algebra over a (commutative Noetherian domain)* R.

1. *For every specialization* $\sigma : R \longrightarrow \mathbf{K}'$, *where* $\mathbf{K}'$ *is a field,* $\ker(\sigma)$ *is a complete prime ideal. In particular* $\ker(\sigma) \in$ c-spec(R).

2. *Let* $\pi \in$ c-spec(R) *be a complete prime ideal, then* π *determines a specialization* σ_π *with kernel* π.

Proof: (1) Since $\mathbf{K}'$ is a field and R is a domain $ab \in \ker(\sigma)$ implies $0 = \sigma(ab) = \sigma(a)\sigma(b)$. So $\sigma(a) = 0$ or $\sigma(b) = 0$ and so $a \in \ker(\sigma)$ or $b \in \ker(\sigma)$ which shows that $\ker(\sigma)$ is a complete prime ideal.

(2) Since π is a complete prime ideal, R/π is an (commutative) domain. So there exists the quotient field $\mathbf{K}_\pi = Q(R/\pi)$. Then the canonical homomorphism $\sigma_\pi : R \longrightarrow \mathbf{K}_\pi$ is a specialization. $\square$

Lemma 7.2.6 *Let* $S = R\{X_1, \ldots, X_n; Q\}$ *be a parametic solvable algebra over* R. *Let* I_l *(*I_r, I_t*) be a left (right, two-sided) ideal of* S *and let* G *be a finite subset of* S. *Let* $\pi \in$ c-spec(R) *be a complete prime ideal,* $\mathbf{K}_\pi = Q(R/\pi)$ *and let* $\sigma_\pi : R \longrightarrow \mathbf{K}_\pi$ *be an epi specialization, such that* $\bar{\sigma_\pi}$ *is admissible for* S *and* $S' = \mathbf{K}_\pi\{X_1, \ldots, X_n; Q\}$. *Then the following are equivalent:*

1. $\bar{\sigma_\pi}(G)$ *is a left (right, two-sided) Gröbner base of* $\text{ideal}_l(\bar{\sigma_\pi}(I_l))$ *(respectively* $\text{ideal}_r(\bar{\sigma_\pi}(I_r))$ *or* $\text{ideal}_t(\bar{\sigma_\pi}(I_t))$*) in* $\mathbf{K}_\pi\{X_1, \ldots, X_n; Q\}$,

2. *for all* $f \in I_l$ *(respectively* I_r, I_t*) with* $T_\pi(f) \neq \emptyset$*, there exists* $g \in G$ *such that* $\mathrm{HT}_\pi(g) \mid \mathrm{HT}_\pi(f)$.

Proof: We verify conditions 4.6.2(5), 4.10.3(5) and 4.11.6(7) for left (right, two-sided) Gröbner bases.

(1) $\Longrightarrow$ (2): Let $f \in I_l$ with $T_\pi(f) \neq \emptyset$, then $\bar{\sigma_\pi}(f) \neq 0$. Since $\bar{\sigma_\pi}(G)$ is a Gröbner base of $\mathrm{ideal}_l(\bar{\sigma_\pi}(I_l))$ we have $\bar{\sigma_\pi}(f) \in \mathrm{ideal}_l(\bar{\sigma_\pi}(G))$. So there exists $\bar{\sigma_\pi}(g) \in \bar{\sigma_\pi}(G)$ with $\mathrm{HT}_\pi(g) = \mathrm{HT}(\bar{\sigma_\pi}(g)) \mid \mathrm{HT}(\bar{\sigma_\pi}(f)) = \mathrm{HT}_\pi(f)$. Similarly for $f \in I_r$ and $f \in I_t$.

(2) $\Longrightarrow$ (1): Let $f \in \mathbf{K}_\pi\{X_1, \ldots, X_n; Q\}$ such that $0 \neq f \in \mathrm{ideal}_l(\bar{\sigma_\pi}(I_l))$. Then there exists $c \in R \setminus \pi$ such that there exists $h \in I_l$ with $\bar{\sigma_\pi}(h) = cf$. Since $f \neq 0$ we have $T_\pi(h) \neq \emptyset$. By assumption there exists $g \in G$ with $\mathrm{HT}(\bar{\sigma_\pi}(g)) = \mathrm{HT}_\pi(g) \mid \mathrm{HT}_\pi(h) = \mathrm{HT}(\bar{\sigma_\pi}(h)) = \mathrm{HT}(\bar{\sigma_\pi}(f))$. That is $\bar{\sigma_\pi}(G)$ is a left Gröbner base as claimed. Similarly for right and two-sided Gröbner bases I_r and I_t. □

7.3 Comprehensive Gröbner Bases

In this section we give the definition of comprehensive Gröbner bases and state the main theorem on comprehensive Gröbner bases, which will then be proved in the rest of the chapter.

Definition 7.3.1 *Let* $S = R\{X_1, \ldots, X_n; Q\}$ *be a parametric solvable polynomial ring over a ring* $R = \mathbf{R}[u_1, \ldots, u_m]$ *over a commutative Noetherian domain* $\mathbf{R}$*. Let* I *be a left (right, two-sided) ideal in* S *and let* G *be a finite subset of* S*. Then* G *is a* comprehensive left (right, two-sided) Gröbner base of I*, if for all solvable polynomial rings* $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q\}$ *over a field* $\mathbf{K}'$ *and all specializations* $\sigma : R \longrightarrow \mathbf{K}'$ *that are admissible for* S *and* S'*,*

> $\bar{\sigma}(G)$ *is a left (right, two-sided) Gröbner base of the left (right, two-sided) ideal* $\mathrm{ideal}_l(\bar{\sigma}(I))$ *(*$\mathrm{ideal}_r(\bar{\sigma}(I))$, $\mathrm{ideal}_t(\bar{\sigma}(I))$*) in* S'.

Lemma 7.3.2 *Let* $S = R\{X_1, \ldots, X_n; Q\}$ *be a parametic solvable polynomial ring over a ring* $R = \mathbf{R}[u_1, \ldots, u_m]$ *over a commutative Noetherian domain* $\mathbf{R}$*. Let* G *be a finite subset of* S*. Then the following are equivalent:*

1. G *is a left (right, two-sided) comprehensive Gröbner base with respect to* $<_T$,
2. *for all epi specializations* $\sigma : R \longrightarrow \mathbf{K}'$*, that are admissible for* S *and* $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q\}$, $\bar{\sigma}(G)$ *is a left (right, two-sided) Gröbner base in* S'.

Proof: (1) $\Longrightarrow$ (2): admissible epi specializations are in particular admissible specializations.

(2) $\Longrightarrow$ (1): Let $\sigma : R \longrightarrow \mathbf{K}'$ be a specialization that is admissible for S and S'. Let $\mathbf{K}'' = Q(\sigma(R))$ be the quotient field of $\sigma(R)$. By the universal property of quotient fields we may assume $\mathbf{K}'' \subseteq \mathbf{K}'$, that is $\mathbf{K}'$ can be considered as an extension field of $\mathbf{K}''$. Now define an epi specialization by $\sigma' : R \longrightarrow \mathbf{K}''$ and extend it to an admissible specialization $\bar{\sigma}' : S \longrightarrow S'' = \mathbf{K}''\{X_1, \ldots, X_n; Q\}$ setting $\bar{\sigma}'(X_i) = \bar{\sigma}(X_i)$, $(i = 1, \ldots, n)$. By assumption $\bar{\sigma}'(G)$ is a left (right, two-sided) Gröbner base in S''. Since Gröbner bases are stable under field extensions by 5.2.1, $\bar{\sigma}'(G)$ is a left (right, two-sided) Gröbner base in $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q\}$. Furthermore $\bar{\sigma}$ extends $\bar{\sigma}'$ so that $\bar{\sigma}(G)$ is a Gröbner base in S'. □

Proposition 7.3.3 *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametic solvable polynomial ring over a ring $R = \mathbf{R}[u_1, \ldots, u_m]$ over a commutative Noetherian domain $\mathbf{R}$. Let G be a finite subset of S. Then the following are equivalent:*

1. *G is a left (right, two-sided) comprehensive Gröbner base with respect to $<_T$,*
2. *for all $\pi \in$ c-spec(R) (i.e. π complete prime) and all $t \in \mathrm{HT}_\pi(\mathrm{ideal}_l(G))$ (respectively $t \in \mathrm{HT}_\pi(\mathrm{ideal}_r(G))$, $t \in \mathrm{HT}_\pi(\mathrm{ideal}_t(G))$) there exists $g \in G$ with $\mathrm{HT}_\pi(g) \mid t$.*

Proof: (1) $\Longleftrightarrow$ for all admissible epi specializations $\sigma : R \longrightarrow \mathbf{K}'$, $\sigma(G)$ is a left (right, two-sided) Gröbner base (by lemma 7.3.2) $\Longleftrightarrow$ (2) by proposition 7.2.6. □

Our next goal is the proof of the following central theorem:

Theorem 7.3.4 (Comprehensive Gröbner Base) *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametic solvable polynomial ring over a ring $R = \mathbf{R}[u_1, \ldots, u_m]$ over a commutative Noetherian domain $\mathbf{R}$. Let F be a finite subset of S. Then one can construct a comprehensive left (right, two-sided) Gröbner base of* $\mathrm{ideal}_l(F)$ *(*$\mathrm{ideal}_r(F)$, $\mathrm{ideal}(F)$*) in S. The construction is algorithmic relative to the term order $<$ on T and computations in the ground ring $\mathbf{R}$.*

To prove the theorem we need several preparations, which we will introduce in the next sections on conditions, reductions and Gröbner systems.

7.4 Conditions and Colourings

Definition 7.4.1 *Let $R = \mathbf{R}[u_1, \ldots, u_m]$ be a ring over a commutative Noetherian domain $\mathbf{R}$. A* condition *$\gamma = \{\phi_1, \ldots, \phi_{i_\gamma}\}$ is a finite set of polynomial equations and polynomial inequations*

$$\phi_i : \begin{cases} g(u_1, \ldots, u_m) = 0, \text{ or} \\ g(u_1, \ldots, u_m) \neq 0. \end{cases}$$

Any condition determines a constructible subset c-spec$_\gamma$ *of* c-spec(R)*:*

$$\text{c-spec}_\gamma = \{\pi \in \text{c-spec}(R) \ : \ g \in \pi \text{ for } (g = 0) \in \gamma \text{ and } g' \notin \pi \text{ for } (g' \neq 0) \in \gamma\}.$$

Notice that c-spec$_\gamma$ may be empty, e.g.

1. if $1 \in \text{ideal}(g_1, \ldots, g_\gamma)$, where $g_i(u_1, \ldots, u_m) = 0$ are polynomial equations in γ, or
2. if for some g both $g(u_1, \ldots, u_m) = 0$ and $g(u_1, \ldots, u_m) \neq 0$ are in γ.

Definition 7.4.2 *A finite set Γ of conditions is a* case distinction, *if for all $\gamma, \gamma' \in \Gamma$,*

$$\gamma \neq \gamma' \Longrightarrow \text{c-spec}_\gamma \cap \text{c-spec}_{\gamma'} = \emptyset.$$

Γ is a cover of a condition δ, *if Γ is a case distinction and*

$$\bigcup_{\gamma \in \Gamma} \text{c-spec}_\gamma = \text{c-spec}_\delta.$$

Γ is a cover of a case distinction Δ, *if Γ is of the form*

$$\Gamma = \bigcup_{\delta \in \Delta} \Gamma_\delta$$

where each Γ_δ is a cover of δ.

Γ is a complete case distinction *(ccd), if Γ is a cover of the empty condition.*

In particular $\Gamma = \{\emptyset\}$ is a complete case distinction since c-spec$_\emptyset$ = c-spec(R).

Definition 7.4.3 *Let $g \in R$ and let Γ be a set of conditions. Let*

$$\begin{aligned} \Gamma_1 &= \{\gamma \cup \{g(u_1, \ldots, u_m) = 0\} \ : \ \gamma \in \Gamma\} \\ \Gamma_2 &= \{\gamma \cup \{g(u_1, \ldots, u_m) \neq 0\} \ : \ \gamma \in \Gamma\}. \end{aligned}$$

If Γ is a complete case distinction, then $\Gamma_1 \cup \Gamma_2$ is a complete case distinction that refines *Γ. If Γ is a cover of a condition δ (or of a case distinction Δ) then $\Gamma_1 \cup \Gamma_2$ is a cover of a condition δ (or of a case distinction Δ) that* refines *Γ. The conditions $\gamma \cup \{g(u_1, \ldots, u_m) = 0\}$ and $\gamma \cup \{g(u_1, \ldots, u_m) \neq 0\}$ are called* successors *of the condition γ.*

Thus we can consider the set of all conditions as a tree under the set inclusion relation and the empty condition $\emptyset$ as root.

Definition 7.4.4 *Let $R = \mathbf{R}[u_1, \ldots, u_m]$ be a ring over a commutative Noetherian domain $\mathbf{R}$. Let $\mathcal{F}$ be the set of all $\mathbf{R}$-terms with variables $u_1, \ldots, u_m$ and operations $+, -, \cdot$. So every $a \in \mathcal{F}$ corresponds to an $a' \in R$. A* colouring *of $\mathcal{F}$ is a map*

$$col : \mathcal{F} \longrightarrow \{white, green, red\}$$

such that $col(a) = green$ if a is equal to 0 and $col(a) = red$ if a is a non-zero element of $\mathbf{R}$. A condition γ determines a colouring of $\mathcal{F}$ by

$$col_\gamma : \mathcal{F} \longrightarrow \{white, green, red\}$$

where again $col_\gamma(a) = green$ *if* a *is equal to* 0 *and* $col_\gamma(a) = red$ *if* a *is a non-zero element of* $\mathbf{R}$. *Furthermore*

$$\begin{aligned} col_\gamma(a) &= green, \text{ if } (a(u_1, \ldots, u_m) = 0) \in \gamma \text{ and} \\ col_\gamma(a) &= red, \text{ if } (a(u_1, \ldots, u_m) \neq 0) \in \gamma. \end{aligned}$$

And by recursion let

$$\begin{aligned} col_\gamma(-a) &= col_\gamma(a), \\ col_\gamma(a \cdot b) &= \begin{cases} red & \text{if } col_\gamma(a) = red \text{ and } col_\gamma(b) = red, \\ green & \text{if } col_\gamma(a) = green \text{ or } col_\gamma(b) = green, \\ white & \text{in all other cases,} \end{cases} \\ col_\gamma(a + b) &= \begin{cases} red & \text{if } col_\gamma(a) = red \text{ and } col_\gamma(b) = green, \\ red & \text{if } col_\gamma(a) = green \text{ and } col_\gamma(b) = red, \\ green & \text{if } col_\gamma(a) = green \text{ and } col_\gamma(b) = green, \\ white & \text{in all other cases.} \end{cases} \end{aligned}$$

So a is coloured *green* by γ if $(a = 0)$ can be deduced, by the recursive rules given above, from the conditions in γ and a is coloured *red* by γ if $(a \neq 0)$ can be deduced, by the recursive rules given above, from the conditions in γ. If neither $(a = 0)$ nor $(a \neq 0)$ can be deduced from γ by these rules, then a is coloured *white*.

7.5 Determining Polynomials

Definition 7.5.1 *For any* $f \in S$ *a colouring of* R *with respect to a condition* γ *induces a colouring of* $T(f)$ *by*

$$col_\gamma(t) = col_\gamma(\text{coeff}(t, f)).$$

Definition 7.5.2 *Let* $c \in \{green, red, white\}$ *then define*

$$T_{c,\gamma}(f) = \{t \in T(f) \ : \ col_\gamma(t) = c\}.$$

Furthermore define

$$T_{R,\gamma}(f) = \{t \in T_{red,\gamma}(f) \ : \ \text{for all } t' \in T(f), \text{ if } t' > t, \text{ then } col_\gamma(t') = green\}$$

and

$$T_{W,\gamma}(f) = \{t \in T_{white,\gamma}(f) \ : \ \text{for all } t' \in T(f), \text{ if } t' > t, \text{ then } col_\gamma(t') = green\}.$$

Lemma 7.5.3 *Both* $T_{R,\gamma}(f)$ *and* $T_{W,\gamma}(f)$ *are either empty or consist of exactly one element. More precisely:*

1. *If* $T(f) = T_{green,\gamma}(f)$ *then* $T_{R,\gamma}(f) = T_{W,\gamma}(f) = \emptyset$.

2. *If* $T(f) \neq T_{green,\gamma}(f)$ *then either*

   (a) $T_{R,\gamma}(f) \neq \emptyset$ *and* $T_{W,\gamma}(f) = \emptyset$, *or*

   (b) $T_{R,\gamma}(f) = \emptyset$ *and* $T_{W,\gamma}(f) \neq \emptyset$.

Proof: (1) if there are only *green* terms, then obviously there are no *red* and no *white* terms. (2) The highest non *green* term must be either *red* or *white*. □

Definition 7.5.4 *For* $f \in S$ *and a condition* γ, *such that* $T_{R,\gamma}(f) \neq \emptyset$, *we define the* γ*-head term of* f*:*

$$\mathrm{HT}_\gamma(f) = t, \text{where } t \in T_{R,\gamma}(f).$$

So $\mathrm{HT}_\gamma(f)$ *may be undefined for certain* f *and* γ. *If* $\mathrm{HT}_\gamma(f)$ *is defined then the leading* γ *coefficient is* $\mathrm{HC}_\gamma(f) = \mathrm{coeff}(\mathrm{HT}_\gamma(f), f)$.

Definition 7.5.5 *Let* F *be a finite set of polynomials in* S. *A condition* γ determines F, *if for every* $f \in F$, $\mathrm{HT}_\gamma(f)$ *is defined or* $T(f) = T_{green,\gamma}(f)$. *A finite set of conditions* Γ determines F, *if for every* $\gamma \in \Gamma$, γ *determines* F.

Lemma 7.5.6 *For any condition* γ *and any finite subset* $F = \{f_1, \ldots, f_k\}$ *of* S *one can construct a cover* Δ *of* γ, *such that* Δ *determines* F. *Moreover* $|\Delta| \leq \prod_{i=1}^{k}(|T(f_i)| + 1)$.

Proof: We give an algorithm which computes Δ in table 7.1.

Partial correctness follows from the properties of $T_{W,\gamma}(f_i)$: as long as there exist white head terms in f_i with respect to γ its coefficient is either coloured red and the condition $\{\mathrm{HC}(f_i) \neq 0\} \cup \gamma$ is placed in Δ or it is coloured green and γ is extended by the condition $\mathrm{HC}(f_i) = 0$. Termination follows, since F is finite, for every $f \in F$, $T(f)$ is finite and Δ is finite in each loop. The bound follows from the fact, that the inner **while** loop produces at most $|T(f_i)|$ new conditions and after their termination one more condition is added. □

7.6 Reduction and Normal Form

In this section we define polynomial reductions relative to conditions and relate them to reductions under specializations.

Definition 7.6.1 Left reduction relative to γ: *Let* $f, f', p \in S$ *and let* γ *be a condition. Then*

$$f \longrightarrow_p f' \ [\gamma]$$

iff $T_{R,\gamma}(p) \neq \emptyset$, *say* $t \in T_{R,\gamma}(p)$, *and there exists* $s \in T_{red,\gamma}(f) \cup T_{white,\gamma}(f)$ *and* $u \in T$ *such that* $s = ut$ *and*

$$f' = c \cdot f - d \cdot s * p.$$

Algorithm: $DETER(\gamma, F)$
Input: A condition γ and $F = \{f_1, \ldots, f_k\} \subseteq S$.
Output: A cover Δ of γ that determines F.
begin $\Delta \leftarrow \{\gamma\}$. $i \leftarrow 0$.
  while $i < k$ **do** $i \leftarrow i + 1$.
    $\Delta' \leftarrow \Delta$. $\Delta \leftarrow \emptyset$.
    while $\Delta' \neq \emptyset$ **do** Let $\gamma \in \Delta'$.
      $\Delta' \leftarrow \Delta' \setminus \{\gamma\}$. $\gamma' \leftarrow \gamma$.
      while $T_{W,\gamma'}(f_i) \neq \emptyset$ **do** Let $t \in T_{W,\gamma'}(f_i)$.
        $a \leftarrow \mathrm{coeff}(t, f_i)$.
        $\Delta \leftarrow \Delta \cup \{\gamma' \cup \{(a \neq 0)\}\}$.
        $\gamma' \leftarrow \gamma' \cup \{(a = 0)\}$.
        end.
      $\Delta \leftarrow \Delta \cup \{\gamma'\}$.
      end.
    end.
  return(Δ).
end $DETER$.

Table 7.1: Algorithm: DETER

where $d = \mathrm{coeff}(s, f)$ *and* $c = \mathrm{HC}_\gamma(s * p)$. *In this case we say* f left reduces to f' modulo p relative to γ.

For $P \subseteq S$ *define* $f \longrightarrow_P f'\ [\gamma]$ *if there exists* $p \in P$ *such that* $f \longrightarrow_p f'[\gamma]$. *Iterated reductions etc. are defined as usual.*

Right reductions are defined similarly.

Remark: If $\gamma \subseteq \delta$ then $f \longrightarrow_p f'[\gamma]$ implies $f \longrightarrow_p f'[\delta]$.

Definition 7.6.2 S-polynomial relative to γ: *Let* $f, g \in S$ *and let* γ *be a condition. Assume* $T_{R,\gamma}(f) \neq \emptyset$ *and* $T_{R,\gamma}(g) \neq \emptyset$. *Let* $u, v \in T$ *such that* $\mathrm{lcm}(\mathrm{HT}_\gamma(f), \mathrm{HT}_\gamma(g)) = u\mathrm{HT}_\gamma(f) = v\mathrm{HT}_\gamma(g)$. *Furthermore let* $b = \mathrm{coeff}(t, u * f)$, $a = \mathrm{coeff}(t, v * g)$, *then*

$$\mathrm{LSP}(\gamma, f, g) = a \cdot u * f - b \cdot v * g.$$

Lemma 7.6.3 *Let* $P \subseteq S$, $f, f', g \in S$. *Let* γ *be a condition such that* c-spec$_\gamma \neq \emptyset$, *let* $\pi \in$ c-spec$_\gamma$ *and let* σ_π *be the corresponding specialization. Then*

$$f \longrightarrow_P f'\ [\gamma] \implies \sigma_\pi(f) \longrightarrow_{\sigma_\pi(P)} \sigma_\pi(f') \ \text{ or } \ \sigma_\pi(f') = c\sigma_\pi(f)$$

for some $0 \neq c \in \mathbf{K}'$ *and*

$$\mathrm{LSP}(\gamma, f, g) = \mathrm{LSP}(\sigma_\pi(f), \sigma_\pi(g)).$$

Proof: Follows from $\mathrm{HT}_\gamma(p) = \mathrm{HT}(\sigma_\pi(p))$ for all involved polynomials, since $\mathrm{HT}_\gamma(p)$ is coloured *red* under γ which means that $\mathrm{coeff}(\mathrm{HT}_\gamma(p), p) \notin \pi$. □

Notice that $f \longrightarrow_p f'[\gamma]$ does not imply $f' < f$ (in S).

For a polynomial $g \in S$ and a condition γ define the *essential part of g with respect to* γ as $g_{e,\gamma} \in S$, where $g_{e,\gamma}$ is obtained from g by deleting all *green* coefficients and all *green* terms with respect to γ.

Lemma 7.6.4 *Let $f, f', p \in S$ and let γ be a condition. If $f \longrightarrow_p f'[\gamma]$ then*

$$f'_{e,\gamma} < f_{e,\gamma} \quad \textit{(in } S\textit{)}.$$

Proof: Let $f' = c \cdot f - d \cdot s * p$. By definition a non-*green* term t is removed from f in f'. Furthermore all terms $t' \in T(s * p)$ with $t' > t$ are coloured *green*. By the product proposition 3.2.5 and the properties of colourings, all non-*green* terms of $s * p$ are smaller than t. Since differences of green monomials gives green monomials, this shows, that all new non-*green* terms in f' are smaller than t. □

Lemma 7.6.5 *For any finite $F \subset S$, any condition γ that determines F and any $f \in S$ one can compute a tuple (g, c) such that*

1. *$c \in R$, $g \in S$ and γ colours c red.*
2. *$f \longrightarrow_F^* g[\gamma]$ and $cf - g \in \mathrm{ideal}_l(F)$ (*$\mathrm{ideal}_r(F)$, $\mathrm{ideal}_t(F)$*).*
3. *g is irreducible modulo F relative to γ.*

Proof: We give an algorithm which computes (g, c) in table 7.2.

Partial correctness follows from the definition of reduction.

Termination: Let $\{g_i\}_{i=0,1,\ldots}$ be the sequence of reduction polynomials with $g_0 = g$. Let $g_{i+1} = c_i \cdot g_i - d_i \cdot s_i * p_i$ be one step reduct of g_i. Then we have for the essential parts $g_{i+1,e,\gamma} < g_{i,e,\gamma}$. Since $<$ is a well-founded quasi-order on S the reduction sequence must be finite $\{g_i\}_{i=0,1,\ldots,k}$. □

To distinguish left and right reduction we will denote $NORMALFORM$ by LNF (for left reduction) and RNF (for right reduction).

7.7 Gröbner System

In this section we discuss 'trees with pairs of a condition and an ideal base at the nodes', such that the 'leaves consist of (preimages of) Gröbner bases'. The 'leaves' constitute the so called Gröbner system and the union over all ideal bases in a Gröbner system is a comprehensive Gröbner base. In this section let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric

Algorithm: $NORMALFORM(\gamma, f, F)$
Input: A condition γ, $f \in S$ and $F = \{f_1, \ldots, f_k\} \subseteq S$
such that γ determines F.
Output: A tuple (g, c) satisfying the conditions (1) – (3) of the lemma.
begin $D \leftarrow \mathrm{HT}_\gamma(F)$. $c \leftarrow 1$. $g \leftarrow f$.
while $\exists s \in D$ with $s \mid t$ for some $t \in T(g_{e,\gamma})$ **do**
Let $p \in F$ with $\mathrm{HT}_\gamma(p) = s$. Let $u \in T$ with $t = su$.
$c' \leftarrow \mathrm{coeff}(t, u * p)$. $d \leftarrow \mathrm{coeff}(t, g)$.
$g \leftarrow c' \cdot g - d \cdot u * p$.
$c \leftarrow c'c$. **end**.
return$((g, c))$.
end $NORMALFORM$.

Table 7.2: Algorithm: NORMALFORM

solvable polynomial ring over a ring $R = \mathbf{R}[u_1, \ldots, u_m]$ over a commutative Noetherian domain $\mathbf{R}$.

Recall that $R = \mathbf{R}[u_1, \ldots, u_m]$ arises from a ring $R' = \mathbf{R}[U_1, \ldots, U_m]$ in the indeterminates $U_1, \ldots, U_m$ such that $u_j = U_j + I$, $1 \leq j \leq m$, where I is a two-sided ideal in $\mathbf{R}[U_1, \ldots, U_m]$ such that $R = R'/I$. In the algorithms the computations in R will actually be performed in R'. So $S' = R'\{X_1, \ldots, X_n; Q\}$ is possibly not an associative ring, but we know, that if we specialize the U's to the u's or to some elements of a field $\mathbf{K}$, such that $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ is a solvable polynomial ring, then all parametric computations are justified.

Definition 7.7.1 *Let Δ be a case distinction. A* left (right, two-sided) Gröbner system *GS of an left (right, two-sided) ideal I of S for Δ is a finite set of pairs (γ, G) such that:*

1. *γ is a condition and G is a finite subset of I determined by γ.*
2. *$\Gamma = \{\gamma \ : \ (\gamma, G) \in GS\}$ is a cover of Δ.*
3. *For every $\pi \in$ c-spec$_\gamma$, $\sigma_\pi(G)$ is a left (right, two-sided) Gröbner base of* $\mathrm{ideal}_l(\sigma_\pi(I))$ *(* $\mathrm{ideal}_r(\sigma_\pi(I))$, $\mathrm{ideal}_t(\sigma_\pi(I))$ *) of $\mathbf{K}_\pi\{X_1, \ldots, X_n; Q\}$.*

Definition 7.7.2 *Let Δ be a case distinction. A* comprehensive left (right, two-sided) Gröbner base *G of a left (right, two-sided) ideal I for Δ is a finite subset of I such that for all $\pi \in \bigcup_{\delta \in \Delta}$ c-spec$_\delta$, $\sigma_\pi(G)$ is a left (right, two-sided) Gröbner base of the left (right, two-sided) ideal* $\mathrm{ideal}_{l,r,t}(\sigma_\pi(I))$. *In particular for $\Delta = \emptyset$, G is a comprehensive left (right, two-sided) Gröbner base of I. GS is then called a left (right, two-sided) Gröbner system of I.*

Proposition 7.7.3 *Any left (right, two-sided) Gröbner system GS of a left (right, two-sided) ideal I of S for Δ determines a comprehensive left (right, two-sided) Gröbner base G of I for Δ and vice versa in the following sense.*

1. *Let GS be a left (right, two-sided) Gröbner system of I for Δ. Let*

$$G' = \bigcup\{G \ : \ (\delta, G) \in GS\}.$$

Then G' is a comprehensive left (right, two-sided) Gröbner base of I for Δ

2. *Let G be a comprehensive left (right, two-sided) Gröbner base of I for Δ. Let*

$$\Gamma = \bigcup_{\delta \in \Delta} DETER(\delta, G), \quad GS = \{(\gamma, G) \ : \ \gamma \in \Gamma\}.$$

Then GS is a left (right, two-sided) Gröbner system of I for Δ. Moreover for any further left (right, two-sided) Gröbner system GS' of I for Δ, such that $(\delta, G') \in GS'$ implies $G' = G$, there exists $(\gamma, G) \in GS$ with c-spec$_\delta \subseteq$ c-spec$_\gamma$.

Proof: (1) Let $\Gamma = \{\gamma \ : \ (\gamma, G) \in GS\}$. Then Γ is a cover of Δ so $\bigcup\{\text{c-spec}_\gamma \ : \ \gamma \in \Gamma\} = \bigcup\{\text{c-spec}_\delta \ : \ \delta \in \Delta\} = \text{c-spec}_\Delta$. Now $G' \supseteq G$ is an extension of G so for any $\pi \in \text{c-spec}_\Delta$ also

$$\sigma_\pi(G) \subseteq \sigma_\pi(G') \subseteq \text{ideal}_{l,r,t}(\sigma_\pi(G)).$$

Since any extension of a Gröbner base is again a Gröbner base, $\sigma_\pi(G')$ is as desired.

(2) The first claim follows from the fact that Γ is by construction a cover of Δ. Let GS' be a further Gröbner system. Let $(\delta, G) \in GS'$ and let $\pi \in \text{c-spec}_\delta$. Let $(\gamma, G) \in GS$ with $\pi \in \text{c-spec}_\gamma$. Then both δ and γ determine G and so by definition of Γ we have c-spec$_\delta \subseteq$ c-spec$_\gamma$. $\square$

Using a comprehensive Gröbner base of an ideal I one can compute the equivalence relation $\sim_I$ on c-spec(R), which is defined by $\pi \sim_I \pi'$ iff $\text{HT}_\pi(I) = \text{HT}_{\pi'}(I)$.

Corollary 7.7.4 *Let G be a comprehensive Gröbner base for an ideal $I \subseteq S$ (that is $\Delta = \emptyset$) and let GS be a Gröbner system for G with case distinction Γ. Then for $\pi, \pi' \in$* c-spec(R)*: $\pi \sim_I \pi'$ iff there exist $\gamma, \delta \in \Gamma$ such that*

1. $\text{mult}(\text{HT}_\gamma(G)) = \text{mult}(\text{HT}_\delta(G))$ *and*

2. $\pi \in \text{c-spec}_\gamma$, $\pi' \in \text{c-spec}_\delta$.

Proof: For any $\gamma \in \Gamma$ and $\pi \in \text{c-spec}_\gamma$, $\text{HT}_\pi(I) = \text{mult}(\text{HT}_\gamma(G))$ holds. $\square$

Theorem 7.7.5 (Construction of Gröbner systems) *For any finite $F \subset S$ and any case distinction Δ one can construct a left (right, two-sided) Gröbner system GS of* $\text{ideal}_l(F)$ *(*$\text{ideal}_r(F)$, $\text{ideal}_t(F)$*) for Δ.*

Algorithm: $LGSYSTEM(\Delta, F)$
Input: A case distinction Δ and $F = \{f_1, \ldots, f_k\} \subseteq S$.
Output: A left Gröbner system GS of ideal$_l(F)$ for Δ.
begin $\Gamma \leftarrow \bigcup\{DETER(\delta, F) \ : \ \delta \in \Delta\}$.
$GS \leftarrow \{(\gamma, F) \ : \ \gamma \in \Gamma\}$.
$P \leftarrow \{(\gamma, F, f, g) \ : \ \gamma \in \Gamma, f, g \in F, f \neq g\}$.
while $P \neq \emptyset$ **do** Let $(\gamma, G, f, g) \in P$.
$P \leftarrow P \setminus \{(\gamma, G, f, g)\}$. $GS \leftarrow GS \setminus \{(\gamma, G)\}$.
$h \leftarrow \mathrm{LSP}(\gamma, f, g)$.
$(p, c) \leftarrow \mathrm{LNF}(\gamma, h, G)$.
$N \leftarrow \{(\alpha, p, c) \ : \ \alpha \in DETER(\gamma, \{p\})\}$.
while $N \neq \emptyset$ **do** Let $(\beta, p, c) \in N$.
$N \leftarrow N \setminus \{(\beta, p, c)\}$.
if $T_{green,\beta}(p) \neq T(p)$
then $P \leftarrow P \cup \{(\beta, G \cup \{p\}, f', p) \ : \ f' \in G\}$.
$GS \leftarrow GS \cup \{(\beta, G \cup \{p\})\}$
else $GS \leftarrow GS \cup \{(\beta, G)\}$ **end**.
end.
end.
$GS' \leftarrow GS$.
$GS \leftarrow \{(\gamma, G) \ : \ $ exists G'' and maximal γ, with $(\gamma, G'') \in GS'$,
and $G = \bigcup\{G' \ : \ (\beta, G') \in GS', \beta \subseteq \gamma\}\}$.
return(GS).
end $LGSYSTEM$.

Table 7.3: Algorithm: LGSYSTEM

Proof: We give algorithms which compute a left (right) GS and a two-sided GS. Note, that the computations on the coefficients take place in $\mathbf{R}[U_1, \ldots, U_m]$. Table 7.3 shows an algorithm for the computation of a left (right) GS.

Correctness: Upon termination for every pair $(\gamma, G) \in GS$ we have $G \subseteq \text{ideal}_{l,r}(F)$ and the conditions 1 and 2 of the definition 7.7.1 of a Gröbner system hold. To show condition 3, let $(\gamma, G) \in GS$ with $G = \bigcup\{G' \ : \ (\beta, G') \in GS', \beta \subseteq \gamma\}$. Then observe that for $f, g \in G$ with $f \neq g$, for $p \in S$ and for γ with $\pi \in \text{c-spec}_\gamma$ with

$$\text{LSP}(\gamma, f, g) \longrightarrow_G^* p[\gamma].$$

By construction of the left normal form, there exists $0 \neq c \in \mathbf{R}$ such that $(p, c) = \text{LNF}(\gamma, \text{LSP}(\gamma, f, g), G)$. The **if** condition in the algorithm assures that $T(p) = T_{green,\gamma}(p)$. So for every $\pi \in \text{c-spec}_\gamma$ by lemma 7.6.3

$$\text{LSP}(\sigma_\pi(f), \sigma_\pi(g)) \longrightarrow_{\sigma_\pi(G)}^* 0.$$

So by theorem 4.6.2(6) $\sigma_\pi(G)$ is a left (right) Gröbner base of

$$\text{ideal}_l(\sigma_\pi(\text{ideal}_l(F)) \quad (\ \text{ideal}_r(\sigma_\pi(\text{ideal}_r(F))\ )$$

and condition 3 holds.

Termination: The set of all pairs (γ, G) produced by the algorithm forms a tree. The successor of a pair (γ, G) is a pair (δ, G'), where δ is a successor of the condition γ and $G' = G$ or $G' = G \cup \{p\}$, with $(p, c) = \text{LNF}(\gamma, G, f, g)$ for some $f, g \in G$, $f \neq g$. Since $DETER(\gamma, \{p\})$ is finite, the tree of the pairs (γ, G) is finitely branching. If in a branch B a successor (δ, G') is equal to (δ, G), that is when no polynomial was added to G', then the corresponding set of pairs P has decreased. So there exists no infinite branch with the same G. If in a branch B a successor (δ, G') is equal to $(\delta, G \cup \{p\})$, then the δ head term $t = \text{HT}_\delta(p)$ is irreducible with respect to the δ head terms of G. Since δ is a successor of γ we have $\text{HT}_\delta(G) = \text{HT}_\gamma(G)$. So if a branch B is infinite, there exists an infinite sequence of head terms $\{t_i \ : \ t_i \in \text{HT}_\gamma(G), (\gamma, G) \in B\}$, such that $t_i \not| t_j$ for $i < j$. Such a sequence contradicts Dickson's lemma. So in the tree each branch is finite and since the tree is finitely branching the tree is finite by König's tree lemma.

Table 7.4 shows an algorithm for the computation of a two-sided GS.

Correctness: Upon termination for every pair $(\gamma, G) \in GS$ we have $G \subseteq \text{ideal}_t(F)$ and the conditions 1 and 2 of the definition 7.7.1 of a two-sided Gröbner system hold. To show condition 3, let $(\gamma, G) \in GS$ with $G = \bigcup\{G' \ : \ (\beta, G') \in GS', \beta \subseteq \gamma\}$. Then observe that for $f, g \in G$ with $f \neq g$, for $p \in S$ and for γ with $\pi \in \text{c-spec}_\gamma$ with

$$\text{LSP}(\gamma, f, g) \longrightarrow_G^* p[\gamma].$$

By construction of the left normal form, there exists $0 \neq c \in \mathbf{R}$ such that $(p, c) = \text{LNF}(\gamma, \text{LSP}(\gamma, f, g), G)$. The (second) **if** condition in the algorithm assures that $T(p) = T_{green,\gamma}(p)$. So for every $\pi \in \text{c-spec}_\gamma$ by lemma 7.6.3

$$\text{LSP}(\sigma_\pi(f), \sigma_\pi(g)) \longrightarrow_{\sigma_\pi(G)}^* 0.$$

Algorithm: $TSGSYSTEM(\Delta, F)$
Input: A case distinction Δ and $F = \{f_1, \ldots, f_k\} \subseteq S = R\{X_1, \ldots, X_n; Q\}$.
Output: A two-sided Gröbner system GS of $\text{ideal}_t(F)$ for Δ.
begin $\Gamma \leftarrow \bigcup\{DETER(\delta, F) \ : \ \delta \in \Delta\}$. $GS \leftarrow \{(\gamma, F) \ : \ \gamma \in \Gamma\}$.
$P \leftarrow \{(\gamma, F, f, g) \ : \ \gamma \in \Gamma, f, g \in F, f \neq g\}$.
$M \leftarrow \{(\gamma, f * X_i) \ : \ \gamma \in \Gamma, \ f \in F, \ 1 \leq i \leq n\}$.
while $M \neq \emptyset$ **do** Let $(\gamma, h) \in M$. $M \leftarrow M \setminus \{(\gamma, h)\}$.
$(p, c) \leftarrow \text{LNF}(\gamma, h, G)$. $N \leftarrow \{(\alpha, p, c) \ : \ \alpha \in DETER(\gamma, \{p\})\}$.
while $N \neq \emptyset$ **do** Let $(\beta, p, c) \in N$. $N \leftarrow N \setminus \{(\beta, p, c)\}$.
if $T_{green,\beta}(p) \neq T(p)$
then $P \leftarrow P \cup \{(\beta, G \cup \{p\}, f', p) \ : \ f' \in G\}$.
$GS \leftarrow GS \cup \{(\beta, G \cup \{p\})\}$
else $GS \leftarrow GS \cup \{(\beta, G)\}$ **end**.
end.
end.
while $P \neq \emptyset$ **do** Let $(\gamma, G, f, g) \in P$.
$P \leftarrow P \setminus \{(\gamma, G, f, g)\}$. $GS \leftarrow GS \setminus \{(\gamma, G)\}$.
$h \leftarrow \text{LSP}(\gamma, f, g)$. $(p, c) \leftarrow \text{LNF}(\gamma, h, G)$.
$N \leftarrow \{(\alpha, p, c) \ : \ \alpha \in DETER(\gamma, \{p\})\}$.
while $N \neq \emptyset$ **do** Let $(\beta, p, c) \in N$. $N \leftarrow N \setminus \{(\beta, p, c)\}$.
if $T_{green,\beta}(p) \neq T(p)$
then $G' \leftarrow G \cup \{p\}$. $P \leftarrow P \cup \{(\beta, G', f, p) \ : \ f \in G\}$.
$GS \leftarrow GS \cup \{(\beta, G')\}$. $i \leftarrow 0$.
while $i < n$ **do** $i \leftarrow i + 1$.
$(q, c') \leftarrow \text{LNF}(\beta, p * X_i, G')$.
$N' \leftarrow \{(\alpha, q, c') \ : \ \alpha \in DETER(\beta, \{q\})\}$.
while $N' \neq \emptyset$ **do** Let $(\alpha, q, c') \in N'$. $N' \leftarrow N' \setminus \{(\alpha, q, c')\}$.
if $T_{green,\alpha}(q) \neq T(q)$
then $P \leftarrow P \cup \{(\alpha, G' \cup \{q\}, f, q) \ : \ f \in G'\}$.
$GS \leftarrow GS \cup \{(\alpha, G' \cup \{q\})\}$
else $GS \leftarrow GS \cup \{(\alpha, G')\}$ **end**.
end.
end.
else $GS \leftarrow GS \cup \{(\beta, G)\}$ **end**.
end.
end.
$GS' \leftarrow GS$.
$GS \leftarrow \{(\gamma, G) \ : \ \text{exists } G'' \text{ and maximal } \gamma, \text{ with } (\gamma, G'') \in GS',$
and $G = \bigcup\{G' \ : \ (\beta, G') \in GS', \beta \subseteq \gamma\}\}$.
return(GS).
end $TSGSYSTEM$.

Table 7.4: Algorithm: TSGSYSTEM

Furthermore we have for any $p \in G$, $1 \leq i \leq n$ and for $h \in S$ with

$$p * X_i \longrightarrow_G^* h[\gamma].$$

The (first and third) **if** conditions in the algorithm assure that $T(h) = T_{green,\gamma}(h)$. So for every $\pi \in \text{c-spec}_\gamma$ by lemma 7.6.3

$$\sigma_\pi(p * X_i) \longrightarrow_{\sigma_\pi(G)}^* 0.$$

This shows by theorems 4.6.2(6) and 4.11.6(6) that $\sigma_\pi(G)$ is a two-sided Gröbner base of $\text{ideal}_t(\sigma_\pi(\text{ideal}_t(F))$ and condition 3 holds.

Termination: The set of all pairs (γ, G) produced by the algorithm forms a tree. The successor of a pair (γ, G) is a pair (δ, G'), where δ is a successor of the condition γ and $G' = G$ or $G' = G \cup \{p\}$, with $(p, c) = \text{LNF}(\gamma, \text{LSP}(\gamma, f, g), G)$ for some $f, g \in G$, $f \neq g$ or $(p, c) = \text{LNF}(\gamma, f * X_i, G)$ for some $f \in G$, $1 \leq i \leq n$. Since in either case $DETER(\gamma, \{p\})$ is finite, the tree of the pairs (γ, G) is finitely branching. If in a branch B a successor (δ, G') is equal to (δ, G), that is when no polynomial was added to G', then the corresponding set of pairs P has decreased. So there exists no infinite branch with the same G. If in a branch B a successor (δ, G') is equal to $(\delta, G \cup \{p\})$, then the δ head term $t = \text{HT}_\delta(p)$ is irreducible with respect to the δ head terms of G. Since δ is a successor of γ we have $\text{HT}_\delta(G) = \text{HT}_\gamma(G)$. So if a branch B is infinite, there exists an infinite sequence of head terms $\{t_i \ : \ t_i \in \text{HT}_\gamma(G), (\gamma, G) \in B\}$, such that $t_i \not| t_j$ for $i < j$. Such a sequence contradicts Dickson's lemma. So in the tree each branch is finite and since the tree is finitely branching the tree is finite by König's tree lemma. This completes the proof in all cases. □

Note that the last assignments in the algorithms $LGSYSTEM$ and $TSGSYSTEM$ can be omitted in case one is interested in a comprehensive Gröbner base only and not in the Gröbner system.

7.8 Parametric Ideal Membership

In this section let $S = R\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over a ring $R = \mathbf{R}[u_1, \ldots, u_m]$ over a commutative Noetherian domain $\mathbf{R}$. For a subset F in S, $\mathbf{a} \in \mathbf{R}^m$ let $F(\mathbf{a}, X_1, \ldots, X_n) = \{f(\mathbf{a}, X_1, \ldots, X_n) \ : \ f \in F\}$.

Theorem 7.8.1 (Parametric Ideal Membership) *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable polynomial ring over a ring $R = \mathbf{R}[U_1, \ldots, U_m]$ over a commutative Noetherian domain $\mathbf{R}$. Let F be a finite subset of S and let $p \in S$. Then one can construct a formula $\psi_{F,p}$, such that for all extension fields $\mathbf{K}'$ of $\mathbf{R}$ and all $\mathbf{a} \in \mathbf{K}'^m$:*

$$\mathbf{K}' \models \psi_{F,p}(\mathbf{a}) \Longleftrightarrow p(\mathbf{a}, X_1, \ldots, X_n) \in \text{ideal}_{l,r,t}(F(\mathbf{a}, X_1, \ldots, X_n)).$$

Here $\text{ideal}_{l,r,t}(F(\mathbf{a}, X_1, \ldots, X_n))$ *is taken in* $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q\}$.

Proof: By theorem 7.7.5 there exists a comprehensive left (right, two-sided) Gröbner base $G_{l,r,t}$ of $\text{ideal}_{l,r,t}(F)$. Collect all conditions under which p reduces to 'zero mod G', that means all conditions under which the normalform p' of p consists only of green terms. Let $\Gamma = DETER(\emptyset, G)$ and let

$$\Delta_{G,p} = \{\gamma \ : \ (p', c) = \text{LNF}(\gamma, p, G),\ T(p') = T_{green,\gamma}(p'),\ \gamma \in \Gamma\}.$$

For a condition δ define the conjunction of all its equalities and inequalities $\phi_\delta : \bigwedge_{\varphi\in\delta} \varphi$. Then define

$$\psi_{F,p}(U_1, \ldots, U_m) = \bigvee_{\delta\in\Delta_{G,p}} \phi_\delta(U_1, \ldots, U_m).$$

We claim, that $\psi_{F,p}$ has the desired properties. Let σ be the specialization of R, that maps U_i to a_i for $1 \le i \le m$, and let $\mathbf{a} = (a_1, \ldots, a_m)$.

"$\Longrightarrow$" Assume $\mathbf{K}' \models \psi_{F,p}(\mathbf{a})$, then $\mathbf{K}' \models \varphi_\delta(\mathbf{a})$ for some $\delta \in \Delta_{G,p}$. So $p \longrightarrow^*_G p'$ $[\delta]$ for some $p' \in S$ with $T(p') = T_{green,\delta}(p')$. Let $\pi \in \text{c-spec}_\delta$ such that σ extends σ_π, then $\bar\sigma(p') = \bar\sigma_\pi(p') = 0$. This shows $\bar\sigma(p) \in \text{ideal}_{l,r,t}(\sigma(G)) = \text{ideal}_{l,r,t}(\sigma(F))$ as claimed.

"$\Longleftarrow$" Assume $\bar\sigma(p) \in \text{ideal}_{l,r,t}(\sigma(F))$. Let $\gamma \in \Gamma$ and let $(p', c) = \text{LNF}(\gamma, p, G)$ $(= \text{RNF}(\gamma, p, G))$ such that there exists $\pi \in \text{c-spec}_\gamma$ such that σ extends σ_π. Then $\bar\sigma(p') \in \text{ideal}_{l,r,t}(\sigma(F))$ since $cp - p' \in \text{ideal}_{l,r,t}(\sigma(F))$ and $\sigma(c) \neq 0$. Now $T(p') = T_{green,\gamma}(p')$ and so $\gamma \in \Delta_{G,p}$. This shows $\phi_\gamma(a_1, \ldots, a_m)$ holds in $\mathbf{K}'$ and consequently $\psi_{F,p}(a_1, \ldots, a_m)$ holds in $\mathbf{K}'$ as claimed. □

The proof shows moreover, that for any $\mathbf{a} \in \mathbf{K}'^m$, such that for a fixed condition δ, $\phi_\delta(\mathbf{a})$ holds in $\mathbf{K}'$,

$$c\ p(\mathbf{a}, X) = \sum_{f\in F} g_f(\mathbf{a}, X) f(\mathbf{a}, X) h_f(\mathbf{a}, X)$$

(where $h_f = 1$ for $p \in \text{ideal}_l(F)$ and $g_f = 1$ for $p \in \text{ideal}_r(F)$) uniformly in the coefficients of the polynomials if $\mathbf{R}$ is commutative. The linear combination can be obtained from the left (right) reduction $p \longrightarrow^*_G p'$ $[\delta]$ and from the representation of the $g \in G$ by the $f \in F$.

The special case $p = 1$ is recorded in the following corollary.

Corollary 7.8.2 (Proper Ideal Test) *Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable polynomial ring over a ring $R = \mathbf{R}[U_1, \ldots, U_m]$ over a commutative Noetherian domain $\mathbf{R}$. Let F be a finite subset of S. Then one can construct a formula ψ_F, such that for all extension fields $\mathbf{K}'$ of $\mathbf{R}$ and all $\mathbf{a} \in \mathbf{K}'^m$:*

$$\mathbf{K}' \models \psi_F(\mathbf{a}) \Longleftrightarrow 1 \in \text{ideal}_{l,r,t}(F(\mathbf{a}, X_1, \ldots, X_n)).$$

Where $\text{ideal}_{l,r,t}(F(\mathbf{a}, X_1, \ldots, X_n))$ *is taken in* $S' = \mathbf{K}'\{X_1, \ldots, X_n; Q\}$.

Chapter 8

Nullstellensätze

In this chapter we discuss roots (or zeroes) of polynomials of a solvable polynomial ring. In contrast to the commutative case, a problem arises here, since the substitution of arbitrary elements for the variables of a polynomial will in general no more be a homomorphism of a solvable polynomial ring to a field. Tuples of elements, such that the substitution is a homomorphism are called *places* and are defined in the first section. Furthermore we summarize some of the important facts about Ore extensions and quotient fields of Ore extensions. It was shown by Dixmier, Lorenz and others that certain rings have the property that every prime ideal is completely prime. In particular there exist solvable polynomial rings with this property. Using these completely prime ideals we state a 'weak' theorem on roots based on the theory of Ore extensions over the rational numbers.

In the next part of the chapter we summarize the results of Cohn on free products of (skew) fields. Then we introduce some model theory: existentially complete structures, model complete structures, substructure complete structures, the amalgamation property, axiomatizability and quantifier elimination. Using this background and the results on comprehensive Gröbner bases we obtain 'stronger' theorems on roots. Finally we discuss existential varieties and close with some remarks on the 'Rabinowich trick'.

In this chapter let $R = \mathbf{K}[U_1, \ldots, U_k]$ be a (non-commutative Noetherian) domain over a (skew) field $\mathbf{K}$. Let $S = R\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over R in the variables $X_1, \ldots, X_n$ with commutator relations Q and Q'. Note, that two-sided ideals are some times only denoted by ideal(P) instead of ideal$_t(P)$ since we consider mostly two-sided ideals in this chapter. Furthermore recall that $\mathbf{Q}$ denotes the rational numbers. The characteristic of all fields we consider will be zero unless otherwise stated. So all fields are extensions of $\mathbf{Q}$, i.e. they are $\mathbf{Q}$-algebras.

8.1 Roots of Solvable Polynomials

In this section we define places and roots of polynomials of solvable polynomial rings.

Definition 8.1.1 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$ with commutator relations Q and Q'. Let $\mathbf{L}$ be an extension field of $\mathbf{K}$. A* **place** *$a = (a_1, \ldots, a_n) \in \mathbf{L}^n$ is a n-tuple of field elements $a_i \in \mathbf{L}$, $i = 1, \ldots, n$, which satisfy the following conditions:*

$$\begin{aligned} a_j a_i - c_{ij} a_i a_j - p_{ij}(a_1, \ldots, a_n) &= 0, \quad 1 \leq i \leq j \leq n \\ a_i b - c_{bi} b a_i - p_{bi}(a_1, \ldots, a_n) &= 0, \quad 1 \leq i \leq n, 0 \neq b \in \mathbf{K}. \end{aligned}$$

Where the c_{ij} and the p_{ij}, $1 \leq i \leq j \leq n$ are from the commutator relations Q of S and where the c_{bi} and the p_{bi}, $1 \leq i \leq n$, $0 \neq b \in \mathbf{K}$ are from the commutator relations Q' of S.

Lemma 8.1.2 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$ with commutator relations Q and Q'. The mapping $\phi_a : S \longrightarrow \mathbf{L}$, $X_i \mapsto a_i$, $1 \leq i \leq n$ with $\phi_{|\mathbf{K}} = \mathrm{id}_{\mathbf{K}}$ is a homomorphism if and only if $a = (a_1, \ldots, a_n)$ is a place.*

Proof: "$\Longrightarrow$" Let ϕ_a be a homomorphism. Then for $1 \leq i \leq j \leq n$ we have

$$\begin{aligned} \phi_a(X_j X_i) &= \phi_a(X_j)\phi_a(X_i) = a_j a_i \\ \phi_a(X_j X_i) &= \phi_a(c_{ij} X_i X_j + p_{ij}) = c_{ij}\phi_a(X_i X_j) + \phi_a(p_{ij}) \\ &= c_{ij} a_i a_j + p_{ij}(a_1, \ldots, a_n) \end{aligned}$$

and for $0 \neq b \in \mathbf{K}$ we have

$$\begin{aligned} \phi_a(X_i b) &= \phi_a(X_j)\phi_a(b) = a_i b \\ \phi_a(X_i b) &= \phi_a(c_{bi} b X_i + p_{bi}) = c_{bi}\phi_a(b X_i) + \phi_a(p_{bi}) \\ &= c_{bi} b a_i + p_{bi}(a_1, \ldots, a_n). \end{aligned}$$

This shows $a_j a_i - c_{ij} a_i a_j - p_{ij}(a_1, \ldots, a_n) = 0$ and $a_i b - c_{bi} b a_i - p_{bi}(a_1, \ldots, a_n) = 0$, so a is a place.

"$\Longleftarrow$" Let $(a_1, \ldots, a_n)$ be a place. Let $\hat{S} = \mathbf{K}\ll Y_1, \ldots, Y_n \gg$ be a free associative polynomial ring generated by $\mathbf{K}$ and the Y's. Define homomorphisms $\psi : \hat{S} \longrightarrow S$ with $Y_i \mapsto X_i$ and $\psi_{|\mathbf{K}} = \mathrm{id}_{|\mathbf{K}}$ and $\psi' : \hat{S} \longrightarrow \mathbf{L}$ with $Y_i \mapsto a_i$ and $\psi'_{|\mathbf{K}} = \mathrm{id}_{|\mathbf{K}}$.

$$\begin{array}{ccccc} & & \psi & & \\ \hat{S} & \longrightarrow & S & & \\ & \searrow & \downarrow & \phi_a & \\ & \psi' & \mathbf{L} & & \end{array}$$

Since a is a place and ψ' is a homomorphism we have $\psi'(Y_j Y_i - c_{ij} Y_i Y_j - p_{ij}(Y_1, \ldots, Y_n)) = a_j a_i - c_{ij} a_i a_j - p_{ij}(a_1, \ldots, a_n) = 0$ and for $0 \neq b \in \mathbf{K}$ $\psi'(Y_i b - c_{bi} b Y_i - p_{bi}(Y_1, \ldots, Y_n)) = a_i b - c_{bi} b a_i - p_{bi}(a_1, \ldots, a_n) = 0$. Since $\psi(Y_j Y_i - c_{ij} Y_i Y_j - p_{ij}(Y_1, \ldots, Y_n)) = X_j X_i - c_{ij} X_i X_j - p_{ij}(X_1, \ldots, X_n) = 0$ and for $0 \neq b \in \mathbf{K}$ $\psi'(Y_i b - c_{bi} b Y_i - p_{bi}(Y_1, \ldots, Y_n)) = X_i b - c_{bi} b X_i - p_{bi}(X_1, \ldots, X_n) = 0$ we see, that the Q and Q' in the variables Y, are in the

kernel of ψ. Since ψ is a homomorphism we can apply theorem 3.4.20, which shows that $Q \cup Q'$ (in the Y's) satisfies hypothesis (NoCg) from 3.4.18 and that $\ker(\psi) = \text{ideal}_t(Q \cup Q')$. Together we obtain that $\ker(\psi) \subseteq \ker(\psi')$. By the factor theorem for ring homomorphisms there exists a unique ϕ (which will be denoted by ϕ_a) with $\phi_a \circ \psi = \psi'$ and $\phi_a : S \longrightarrow \mathbf{L}$. By construction of ψ and ψ' we must have $\phi_a : X_i \mapsto a_i$, $1 \leq i \leq n$ and $\phi_{a|\mathbf{K}} = \text{id}_{\mathbf{K}}$. Which proves the lemma. $\square$

A place is defined relative to a given polynomial ring of solvable type S with commutator relations Q and Q'. ϕ_a is called 'evaluation morphism'. For $f \in S$ and a place $a \in \mathbf{L}^n$ we denote $\phi_a(f)$ by $f(a)$.

Definition 8.1.3 *Let* $\mathbf{L}$ *be an extension field of* $\mathbf{K}$ *and let* S *be a polynomial ring of solvable type. A* **root** *of a polynomial* $f \in S$ *is a* place $a = (a_1, \ldots, a_n) \in \mathbf{L}^n$ *for which:*

$$f(a) = 0.$$

A **root** *of a subset* $I \subseteq S$ *is a* place $a = (a_1, \ldots, a_n) \in \mathbf{L}^n$ *for which:*

$$f(a) = 0 \quad \text{for all} \quad f \in I.$$

With $N_{\mathbf{L}}(I)$ *we denote the set of roots of* I *in the extension field* $\mathbf{L}$ *of* $\mathbf{K}$. *If* $\mathbf{L}$ *is clear from the context we denote* $N_{\mathbf{L}}(I)$ *by* $N(I)$.

Lemma 8.1.4 *Let* $I = \text{ideal}(F)$ *be a two-sided ideal in* S *generated by* $F = \{f_1, \ldots, f_m\}$. *Let* $a \in \mathbf{L}^n$ *be a place such that* $f_i(a) = 0$ *for all* $f_i \in F$ *then* a *is a root of the ideal* I.

Proof: Since I is generated by F every polynomial $f \in I$ has a representation $f = \sum_{i=1}^{k} g_i f_i h_i$, with $g_i, h_i \in S$ for $i = 1, \ldots, k$. So $f(a) = \phi_a(\sum_{i=1}^{k} g_i f_i h_i) = \sum_{i=1}^{k} \phi_a(g_i) f_i(a) \phi_a(h_i) = \sum_{i=1}^{k} \phi_a(g_i) 0 \phi_a(h_i) = 0$ since a is a place, ϕ_a is a homomorphism and a is a root of each f_i, $i = 1, \ldots, k$. That is, a is a root of I. $\square$

Lemma 8.1.5 *Let* $I, J \subseteq S$ *be two-sided ideals. If* $I \subseteq J$ *then* $N(J) \subseteq N(I)$.

Proof: Since I is contained in J any $f \in I$ has a representation with respect to J: $f = \sum_{i=1}^{k} g_i f_i h_i$, with $f_i \in J$ and $g_i, h_i \in S$ for $i = 1, \ldots, k$. So $f(a) = 0$ since a is a place, ϕ_a is a homomorphism and a is a root of J whence of each f_i, $i = 1, \ldots, k$. That is, any root a of J is a root of I. $\square$

Remarks:

1. Not every $a = (0, \ldots, 0, a_i, 0, \ldots, 0) \in \mathbf{L}^n$ is a place. Let $S = \mathbf{Q}\{X_1, X_2; \{X_2X_1 = X_1X_2 + 1\}\}$. Then for $a = (0, a_2) \in \mathbf{Q}^2$ we have $a_2 0 - 0 a_2 - 1 = 1 \neq 0$. This shows that a is not a place.

2. Not every univariate polynomial need to have a root in some extension field. Let $S = \mathbf{Q}\{X_1, X_2; \{X_2X_1 = X_1X_2 + 1\}\}$ and let $X_1 = f(X_1) \in S$. Assume $a = (a_1, a_2) \in \mathbf{L}^2$, where $\mathbf{L}$ is an extension field of $\mathbf{Q}$, is a root of f. Then we have $f(a) = \phi_a(f) = \phi_a(X_1) = 0$ and consequently $a_2a_1 - a_1a_2 - 1 = \phi_a(X_2X_1 - X_1X_2 - 1) = \phi_a(X_2)\phi_a(X_1) - \phi_a(X_1)\phi_a(X_2) - \phi_a(1) = \phi_a(X_2)0 - 0\phi_a(X_2) - \phi_a(1) = 1 \neq 0$. Thus a cannot be a place.

Lemma 8.1.6 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring. Let $a \in \mathbf{L} \supseteq \mathbf{K}$ be a root of the univariate polynomial $0 \neq f(X_i) \in S$ and let $S' = \mathbf{L}\{X_1, \ldots, X_n; Q, \hat{Q}'\}$ be a solvable polynomial ring which extends S. Then f is left divisible by the linear polynomial $(X_i - a)$, i.e. there exists $0 \neq q \in \mathbf{L}[X_i]$ such that $f = q * (X_i - a)$.*

Proof: By left reduction with $P = \{X_i - a\}$ let $r \in S'$ with $f \longrightarrow_P^* r$. Then we have

$$f = \sum_{j=1,..,k} q_j * (X_i - a) + r = q * (X_i - a) + r,$$

with $q_j, q \in S'$ for $j = 1, \ldots, k$. Moreover $q, r \in \mathbf{L}[X_i]$ by lemma 3.2.4. Now $\mathrm{HT}(r)$ is irreducible wrt. $\mathrm{HT}(X_i - a) = \mathrm{HT}(X_i)$ and consequently $r \in \mathbf{L}$. Since a is a root of f we have $0 = \phi_a(f) = \phi_a(q)\phi_a(X_i - a) + \phi_a(r) = \phi_a(q)0 + \phi_a(r) = \phi_a(r)$. Since $r \in \mathbf{L}$ it follows from $\phi_a(r) = 0$ that $r = 0$. This shows that f is divisible by $(X_i - a)$. □

Lemma 8.1.7 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$ and let $f \in S$ be an univariate polynomial of degree d. If f can be written as product of d' linear polynomials and a polynomial q, such that q has no root in $\mathbf{K}$, then $d' \leq d$.*

Proof: By comparing the head terms of the product of the linear polynomials and the head term of f. □

Corollary 8.1.8 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$. If $0 \neq f \in S$ is an univariate polynomial of degree d, then f has at most d roots in some extension field $\mathbf{L}$ of $\mathbf{K}$ such that $\mathbf{L}\{X_1, \ldots, X_n; Q, \hat{Q}'\}$ is a solvable polynomial ring which extends S.*

Proof: For each root $a \in \mathbf{L}$ of $0 \neq f \in \mathbf{K}[X_i]$ the linear polynomial $X_i - a$ divides f. Since the degree of f is d, there can be at most d linear factors dividing f. □

Lemma 8.1.9 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring over a field $\mathbf{K}$. Let I be a two-sided ideal in S which contains an univariate polynomial $p_i(X_i)$ for each variable X_i, $i = 1, \ldots, n$. Then ideal I has only finitely many roots in $\mathbf{K}$.*

Proof: Each p_i has only finitely many roots by the previous lemma. Since the ideal generated by the p_i is contained in I, the roots of I are among the common roots of the p_i. □

8.2 Existence of Roots of Solvable Polynomials

In this section we will first discuss the construction of quotient fields for iterated Ore extensions. Then we show the existence of extension fields, in which proper (two-sided) ideal have roots. Finally we prove a 'weak' form of the Hilbert Nullstellensatz.

8.2.1 Quotient Fields

The main obstacle in non-commutative extension field theory is that prime ideals may not be completely prime ideals. This has the consequence that dividing a ring by a prime ideal does not lead to a ring without zero divisors. But a necessary condition for a ring to be embeddable in a field is that it has no zero divisors (i.e. it is a domain). To see that in general prime ideals need not be completely prime, consider the following example.

Example 8.2.1 *Let $R = \mathbf{F}[X; Y; \partial/\partial_X]$ be the Weyl algebra over a field $\mathbf{F}$ of characteristic $p > 0$. Let $G = \{X^p - 1, Y^p - 1\}$ and let $I = \mathrm{ideal}_t(G)$. Then one can show that I is a maximal ideal and so I is a prime ideal. But I is not completely prime, since $(X-1)^p = X^p - 1 \in I$, but $(X-1) \notin I$.*

Sufficient conditions for a domain to be embeddable in a (skew) field have been obtained by Ore. To state his results we need some preparations.

Definition 8.2.2 (Ore condition) *For a domain R the right (left)* Ore condition *holds, if for all nonzero $a, b \in R$ there exist $r, s \in R$ such that $0 \neq ar = bs$ ($0 \neq ra = sb$) hold. In other words each pair of nonzero elements of R has a nonzero right (left) common multiple.*

R is called a right (left) Ore domain if it is a domain and the right (left) Ore condition holds. R is called an Ore domain, if R is both a right and a left Ore domain.

Lemma 8.2.3 (Goldie, Lesieur-Croisot) *Let S be a (left / right) Noetherian domain. Then S is a (left / right) Ore domain.*

Proof: See [Goodearl, Warfield 1989](p 94). □ For the computation of left common multiples see 5.5.1.

Lemma 8.2.4 *Every solvable polynomial ring $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ over a field $\mathbf{K}$ is a (left / right) Ore domain. Moreover every solvable polynomial ring over a (left / right) Noetherian domain, which satisfies the extended axioms is a (left / right) Ore domain.*

Proof: First by the consequences of the product lemma 3.2.5 S is a domain. Since $\mathbf{K}$ is a field or S satisfies the extended axioms, by the Hilbert basis theorem 3.5.12 S is a (left / right) Noetherian ring. Then by the preceding lemma 8.2.3 S is a (left / right) Ore domain. □

Definition 8.2.5 *A subset X in a ring R is called a* strong multiplicative set *if $1 \in X$ and X is a multiplicative set.*

Let X be a strong multiplicative set in R. A ring $\mathbf{L}$ together with a homomorphism $\phi : R \longrightarrow \mathbf{L}$ is called a right ring of fractions for R with respect to X *if*

1. *$\phi(x)$ is a unit of $\mathbf{L}$ for all $x \in X$,*
2. *Each element of $\mathbf{L}$ has the form $\phi(r)\phi(x)^{-1}$ for some $r \in R$ and some $x \in X$.*
3. *$\ker(\phi) = \{r \in R : rx = 0$ for some $x \in X\}$.*

If $\ker(\phi) = \{0\}$, i.e. if there are no zero divisors in R, then ϕ is an embedding. In particular if R is a domain, then $X = R \setminus \{0\}$ is a strong multiplicative set. Then the right ring of fractions for R with respect to X is called a quotient field of R. *The quotient field of R (if it exists) is denoted by $Q(R)$.*

If the right ring of fractions $(\mathbf{L}, \phi)$ exists, then it is 'universal' and consequently it is unique up to isomorphism.

Theorem 8.2.6 *Let S be a (left / right) Ore domain. Then there exists a (unique) (left / right) quotient field $Q(S)$ of S.*

Proof: See [Goodearl, Warfield 1989](p 148). □

Theorem 8.2.7 *Let S be an Noetherian domain. Let I be a complete prime ideal in S. Then there exists the quotient field $Q(S/I)$ of S/I.*

Proof: Since S is a domain and I is completely prime, then S/I is a domain. Since S is Noetherian, also S/I is Noetherian, so the Ore condition also holds in S/I. Thus S/I is an Ore domain and therefore has a quotient field. □

The next proposition records the achievements which have been obtained so far to show under which conditions prime ideals are completely prime, and there is not much hope to improve the theorem. For counter examples see [Lorenz 1981].

Theorem 8.2.8 (Lie, Dixmier, Gabriel, Lorenz, Sigurdsson) *Let R be a commutative Noetherian $\mathbf{Q}$-algebra and $S = R[X_1, \delta_1] \ldots [X_n, \delta_n]$ be an iterated differential operator ring. Then every prime ideal of S is completely prime.*

Proof: See [Goodearl, Warfield 1989](p 160). □

As the example 8.2.1 of Weyl algebras over fields of positive characteristic shows, the theorem is false if $\mathbf{Q}$ being replaced by a field of characteristic $p > 0$.

Moreover the condition, that R is a commutative Noetherian $\mathbf{Q}$-algebra can not be replaced by the condition that R is a ring in which every prime ideal is completely prime.

The condition required on R is that in every extension field of R every prime ideal is completely prime, which is true only if R is an iterated differential operator ring over a commutative Noetherian $\mathbf{Q}$-algebra.

It is furthermore known that the theorem does not hold for an Ore extension $R[X;\alpha,\delta]$ where the automorphism α is arbitrary. It is required that α is the identity on R, that is $R[X;\delta]$ is an differential operator ring.

8.2.2 Extension Fields

As a consequence of theorem 8.2.8 we see that there exist solvable polynomial rings, such that every prime ideal is completely prime.

Lemma 8.2.9 *There exist a field* $\mathbf{K}$ *and commutator relations* Q *and* Q'*, such that*

1. $S = \mathbf{K}\{X_1,\ldots,X_n;Q,Q'\}$ *is a solvable polynomial ring*
2. *and every prime ideal of* S *is completely prime.*

In other words, the class of solvable polynomial rings in which every prime ideal is completely prime is non-empty.

Proof: By theorem 8.2.8 for $\mathbf{K} = \mathbf{Q} = R$ the iterated differential operator ring $S' = \mathbf{Q}[X_1,\delta_1]\ldots[X_n,\delta_n]$ has the property that every prime ideal is completely prime. By theorem 3.4.6 there exists a solvable polynomial ring $S = \mathbf{K}\{X_1,\ldots,X_n;Q,Q'\}$ of strictly monic lexicographical type which corresponds to S'. Furthermore an ideal in S is prime respectively completely prime if and only if the corresponding ideal in S' is so. □

Moreover we have a sufficient 'syntactic' criterion of solvable polynomial rings where prime ideals are completely prime:

Lemma 8.2.10 *Let* $\mathbf{Q} \subset \mathbf{K}$ *be a commutative field of characteristic zero. Let* Q *be a set of strictly monic lexicographical commutator relations and let* Q' *be a set of coefficient commutator relations, such that* $S = \mathbf{K}\{X_1,\ldots,X_n;Q,Q'\}$ *is a solvable polynomial ring of strictly monic lexicographical type, then every prime ideal of* S *is completely prime.*

Proof: Under this assumptions there exists by theorem 3.4.7 a corresponding iterated Ore extension S' of $\mathbf{Q}$. Since the assumptions of theorem 8.2.8 are fulfilled, every prime ideal of S' is completely prime. Consequently every prime ideal of S is completely prime. □

The next proposition shows that ideals I in solvable polynomial rings (where prime ideals are completely prime) have roots in some extension (skew) field of $\mathbf{K}$ if an only if I is proper.

Proposition 8.2.11 (Nullstellensatz) *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q\}$ be a solvable polynomial ring of strictly monic lexicographical type.*

1. *For every proper ideal I in S there exists a (skew) field extension $\mathbf{L}$ of $\mathbf{K}$ such that the set of roots $N_{\mathbf{L}}(I)$ is not empty.*
2. *Let I be an ideal in S such that there exists a (skew) field extension $\mathbf{L}$ of $\mathbf{K}$ such that $N_{\mathbf{L}}(I) \neq \emptyset$ then $1 \notin I$.*

Proof: (1) Let I be proper and let J be a prime ideal in S which contains I: $I \subseteq J$. J exists, since by lemma 2.2.4 every ideal is contained in a maximal ideal and by lemma 2.2.5 every maximal ideal is prime. Under the assumptions on Q, by lemma 8.2.10 every prime ideal of S is completely prime. Furthermore by lemma 8.2.4 S is an Ore domain, there exists a quotient field $\mathbf{L} = Q(S/J)$. Let $a_i = X_i + J$ for $1 \leq i \leq n$ and $a = (a_1, \ldots, a_n) \in \mathbf{L}^n$. Then a is a place since the commutator relations are inherited from S. Furthermore for every $f \in J$ we have

$$f(a) = \phi_a(f) = f(X + J) = f(X) + J = J$$

that is, $f(a) = 0$ in $\mathbf{L}^n$. This shows that a is a root of J and so of I, and thus proves (1).
(2) Let $a \in N(I)$, $a \in \mathbf{L}^n$. Assume $1 \in I$ then there exist $f_i \in I$ and $g_i, h_i \in S$ for $(1 \leq i \leq k)$ for some $k \in \mathbf{N}$ such that $1 = \sum_{i=1}^{k} g_i f_i h_i$. Since a is a root (in particular a place) the evaluation morphism yields:

$$1 = \phi_a(1) = \phi_a(\sum_{i=1}^{k} g_i f_i h_i) = \sum_{i=1}^{k} \phi_a(g_i) 0 \phi_a(h_i) = 0.$$

This is a contradiction and thus the assumption $1 \in I$ must have been wrong. So $1 \notin I$, which proves (2). □

8.2.3 Roots and Radical Ideals

Using the separation lemma of prime ideals and multiplicatively closed sets we obtain the following improved propositions.

Proposition 8.2.12 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring. Let $\mathbf{L}$ be an extension (skew) field of $\mathbf{K}$. Let I be an ideal in S and let $a \in \mathbf{L}^n$ be a root of I. Let $f \in S$ such that $f(a) \neq 0$ then $f^k \notin I$ for all $0 < k \in \mathbf{N}$.*

Proof: Assume for a contradiction that there exists $0 < k \in \mathbf{N}$ such that $f^k \in I$. Let I be generated by $\{f_1, \ldots, f_m\}$, then there exist $g_i, h_i \in S$ for $i = 1, \ldots m$ such that

$$f^k = \sum_{i=1}^{m} g_i f_i h_i.$$

Since a is a root, whence a place, the evaluation morphism yields: $\phi_a(f^k) = \phi_a(\sum_{i=1}^{m} g_i f_i h_i)$ $= \sum_{i=1}^{m} \phi_a(g_i) 0 \phi_a(h_i) = 0$. Since $\mathbf{L}$ is a field it follows that $\phi_a(f) = f(a) = 0$. This contradicts our assumption $f(a) \neq 0$ and thus proves the proposition. □

Proposition 8.2.13 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring of strictly monic lexicographical type. Let I be a proper ideal in S. Let $f \in S$ such that $f^k \notin I$ for all $0 < k \in \mathbf{N}$. Then there exists an extension (skew) field $\mathbf{L}$ of $\mathbf{K}$ and a root $a \in \mathbf{L}^n$ of I such that $f(a) \neq 0$.*

Proof: Under the assumptions on Q, by lemma 8.2.10 every prime ideal of S is completely prime. Let $M = \{f^k : 0 < k \in \mathbf{N}\}$, then M is multiplicatively closed. By assumption $M \cap I = \emptyset$ holds. So by the separation lemma 2.2.12 there exists a prime ideal J with $I \subseteq J$ and $M \cap J = \emptyset$. Again by assumption J is completely prime and so S/J is an Ore domain and there exists a quotient field $\mathbf{L} = Q(S/J)$. Let $a_i = X_i + J \in \mathbf{L}$ for $i = 1, \ldots, n$ and let $a = (a_1, \ldots, a_n) \in \mathbf{L}^n$. Then a is a root of I since $\phi_a(f_j) = f_j(a) = f_j(X + J) = f_j(X) + J = J$. But $0 \neq \phi_a(f) = f(a) = f(X + J) = f(X) + J \neq J$ since $f \notin I$. That is a is not a root of f and this proves the proposition. □

Combining this results with the characterization of radical ideals in rings where prime ideals are completely prime we obtain

Theorem 8.2.14 (Weak Hilbert Nullstellensatz) *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ be a solvable polynomial ring of strictly monic lexicographical type.*

1. *Let I be a proper (two-sided) ideal in S. Let $f \in S$ such that $f \notin \mathrm{rad}(I)$. Then there exists an extension (skew) field $\mathbf{L}$ of $\mathbf{K}$ and a root $a \in \mathbf{L}^n$ of I such that $f(a) \neq 0$.*
2. *Let $\mathbf{L}$ be an extension (skew) field of $\mathbf{K}$. Let I be an ideal in S and let $a \in \mathbf{L}^n$ be a root of I. Let $f \in S$ such that $f(a) \neq 0$ then $f \notin \mathrm{rad}(I)$.*

Proof: (1) From $f \notin \mathrm{rad}(I)$ it follows by lemma 2.2.16 that for all $0 < k \in \mathbf{N}$, $f^k \notin I$ holds. Then the claim follows by the preceding proposition 8.2.12.

(2) From $f \in \mathrm{rad}(I)$ it follows from lemma 2.2.15 that there exists $0 < k \in \mathbf{N}$ such that $f^k \in I$. But by the preceding proposition 8.2.13 it follows from $f(a) \neq 0$ that $f^k \notin I$ for all $0 < k \in \mathbf{N}$. So $f \in \mathrm{rad}(I)$ cannot hold. □

8.3 Coproducts and Free Products

In this section we will mainly record the results obtained by P. M. Cohn about so called free products of fields. To this end we need some preparations. Recall the definition of a category by its objects and morphisms.

Definition 8.3.1 *A* category *is a class $\mathbf{C}$ of objects such that*

1. *for every pair of objects X, Y of $\mathbf{C}$ there is a* set

$$\mathrm{Mor}_{\mathbf{C}}(X, Y),$$

called the set of morphisms from X to Y, *with* $\mathrm{Mor}_{\mathbf{C}}(X, Y)$ *and* $\mathrm{Mor}_{\mathbf{C}}(X', Y')$ *disjoint unless $X = X'$ and $Y = Y'$ in which case they coincide;*

2. *for any three objects X, Y, Z of $\mathbf{C}$ there is a mapping*

$$\mathrm{Mor}_{\mathbf{C}}(X,Y) \times \mathrm{Mor}_{\mathbf{C}}(Y,Z) \longrightarrow \mathrm{Mor}_{\mathbf{C}}(X,Z),$$

described by $(f,g) \mapsto f \circ g$, with the following properties:

(a) *for every object X there is a morphism*

$$id_X \in \mathrm{Mor}_{\mathbf{C}}(X,X)$$

which is the right identity under $\circ$ for the elements of $\mathrm{Mor}_{\mathbf{C}}(X,Y)$ and a left identity under $\circ$ for the elements of $\mathrm{Mor}_{\mathbf{C}}(Y,X)$;

(b) *$\circ$ is 'associative' in the sense, that when the composites*

$$h \circ (g \circ f) \text{ and } (h \circ g) \circ f$$

are defined they are equal.

Definition 8.3.2 *An object U of a category $\mathbf{C}$ is said to be an* initial object *if, for every object X of $\mathbf{C}$, the set of morphisms $\mathrm{Mor}_{\mathbf{C}}(U,X)$ is a singleton.*

Dually, an object U of a category $\mathbf{C}$ is said to be a terminal object *if, for every object X of $\mathbf{C}$, the set of morphisms $\mathrm{Mor}_{\mathbf{C}}(X,U)$ is a singleton.*

Definition 8.3.3 *Let $\{A_i\}_{i\in I}$ be a family of objects in a category $\mathbf{C}$. Define a category $\mathbf{D}$ as follows:*

1. *for the objects of $\mathbf{D}$ take the pairs $e = (E, \{f_i\}_{i\in I})$ consisting of an object E of $\mathbf{C}$ and a family $\{f_i\}_{i\in I}$ of morphisms $f_i : A_i \longrightarrow E$, and*

2. *for the set of morphisms of $\mathbf{D}$ $e \mapsto e'$ take those morphisms $\delta : E' \longrightarrow E$ of $\mathbf{C}$ such that the diagram*

$$\begin{array}{ccc} E & \xleftarrow{f_i} & A_i \\ & \nwarrow_{\delta} & \downarrow_{f_i'} \\ & & E' \end{array}$$

is commutative for every $i \in I$.

An initial object $(Q, \{q_i\}_{i\in I})$ in the category $\mathbf{D}$ (if it exists) is called a coproduct *of the family $\{A_i\}_{i\in I}$. In abuse of notation we also refer to Q itself as the coproduct of the $\{A_i\}_{i\in I}$ and we write*

$$Q = \bigcirc_{i\in I} A_i.$$

Theorem 8.3.4 *Since initial objects are unique up to composition by an isomorphism, the coproduct is unique in the sense that is has the following universal property. If* $(P, \{p_i\}_{i\in I})$ *and* $(Q, \{q_i\}_{i\in I})$ *are both coproducts of the family* $\{A_i\}_{i\in I}$*, then there exists a unique isomorphism* $\delta : Q \longrightarrow P$ *such that each of the diagrams*

$$\begin{array}{ccc} P & \longleftarrow_{p_i} & A_i \\ & \nwarrow_{\delta} & \downarrow_{q_i} \\ & & Q \end{array}$$

is commutative.

Proof: See [Blyth 1986](p 28). □

In other words if we have a situation with morphisms $f_i : A_i \longrightarrow X$ for some X in the category $\mathbf{C}$, then there exist unique $p_i : A_i \longrightarrow \bigcirc_{i\in I} A_i$ and a unique $\delta : \bigcirc_{i\in I} A_i \longrightarrow X$, such that $\delta \circ p_i = f_i$ for each $i \in I$.

In the sequel we will restrict our attention to the case $I = \{1, 2\}$. Then we have the following diagram

$$\begin{array}{ccccc} & & A_1 \bigcirc A_2 & & \\ & \nearrow_{p_1} & & \nwarrow_{p_2} & \\ A_1 & & \downarrow_{\delta} & & A_2. \\ & \searrow_{f_1} & & \swarrow_{f_2} & \\ & & X & & \end{array}$$

Definition 8.3.5 *Let* $\mathbf{C}$ *now be the category with coproducts. We consider the situation*

$$\begin{array}{ccccc} & & A_1 \bigcirc A_2 & & \\ & \nearrow_{p_1} & & \nwarrow_{p_2} & \\ A_1 & & & & A_2 \\ & \nwarrow_{f_1} & & \nearrow_{f_2} & \\ & & A & & \end{array}$$

where A, A_1, A_2 *are some objects.*

1. *The coproduct* $A_1 \bigcirc A_2$ *is called* faithful *if, whenever the* f_1, f_2 *are injective then also* p_1, p_2 *are injective.*

2. *The coproduct* $A_1 \bigcirc A_2$ *is called* separating *if,*

$$p_1(f_1(A)) = p_1(A_1) \cap p_2(A_2) = p_2(f_2(A))$$

Theorem 8.3.6 (Cohn) *The coproduct of (skew) fields* A_1*,* A_2 *over a common sub field* A *exists and is faithful and separating. It is called* free product *and is denoted by* $C = A_1 \bigcirc_A A_2$*.*

Proof: See [Cohn 1971], [Cohn 1977](p 98). □

8.4 Some Model Theory

In this section we recall some definitions from model theory and fix the notations used in the sequel.

8.4.1 Deduction and Models

Let L be a (first order) language. Let $\mathcal{M}$ denote a class of L-structures. Recall that for A '$\in$' $\mathcal{M}$ and a L-formula ϕ we say A is a model for ϕ if $A \models \phi$. Let ϕ be a formula and let Γ be a set of formulas, then we denote by $\Gamma \models \phi$ that for all L-structures A, with $A \models \Gamma$ also $A \models \phi$. In this case we say that ϕ is a semantic consequence of Γ.

Let L be a language. Let ϕ, ψ be formulas and let Γ be a set of formulas. Recall, that ϕ is deducible from ψ, $\psi \vdash \phi$, if ϕ can be produced from ψ by syntactic manipulations on ψ according to a set of certain *rules*. The rules used in classical first order logic are called Hilbert type calculus. $\Gamma \vdash \phi$ denotes that ϕ is deducible from a set of formulas Γ. Γ is called *consistent* if falsity (**false**) cannot be deduced from Γ.

Let ϕ, ψ be formulas and let Γ be a set of formulas. For Hilbert type calculus in first order logic the following theorems of Gödel hold.

Correctness: if $\Gamma \vdash \phi$ then $\Gamma \models \phi$,

Completeness: if $\Gamma \models \phi$ then $\Gamma \vdash \phi$.

And for sentences ϕ, ψ and a set of sentences Γ,

Deduction: if $\Gamma \cup \{\psi\} \vdash \phi$ then $\Gamma \vdash (\psi \longrightarrow \phi)$.

Note that '$\longrightarrow$' here denotes 'implies' and not 'reduction'; but it should always be clear from the context what is meant. Using the completeness theorem or more generally using ultraproducts one can derive the compactness theorem.

Theorem 8.4.1 (Compactness) *Let Γ be a set of formulas. Γ has a model if and only if every finite subset of Γ has a model.*

Let L be a language. Let ϕ be a formula and let Γ be a set of formulas. A *theory* $\mathcal{T}$ is a deductively closed subset of formulas of L, that is: $\mathcal{T} \vdash \phi \implies \phi \in \mathcal{T}$. Γ is an *axiom set* for $\mathcal{T}$ if $\mathcal{T} = \{\phi : \Gamma \vdash \phi\}$.

Let L be a language. Let ϕ be a formula and let Γ be a set of formulas. Let A be a L-structure.

$$\mathcal{M} = \mathrm{Mod}(\Gamma) = \{A \ : \ A \models \phi, \text{ for all } \phi \in \Gamma \ \}$$

denotes the class of all L-structures A which are models of Γ.

$$\mathcal{T} = \mathrm{Thy}(\mathcal{M}) = \{\phi \ : \ A \models \phi, \text{ for all } A \in \mathcal{M} \ \}$$

denotes the set of all L-formulas ϕ which hold in every $A \in \mathcal{M}$.

Definition 8.4.2 *Let L be a language and let $\mathcal{M}$ be a class of L-structures. Then $\mathcal{M}$ is* axiomatizable in L *if there exists a set of L-formulas Γ such that*

$$\mathcal{M} = \mathrm{Mod}(\Gamma).$$

The elements of Γ are called axioms. If there exists a finite set Γ of axioms for $\mathcal{M}$, we say $\mathcal{M}$ is elementary in L *or finitely axiomatizable in L.*

8.4.2 Classes of Structures with Completeness Properties

There are several notations of classes of structures with completeness properties:

1. complete classes,
2. model complete classes,
3. model companionable classes,
4. substructure complete classes,
5. existentially complete classes.

Complete classes occur 'rarely'. Only if the corresponding theory $\mathcal{T}$ is maximal in the sense, that for every L-sentence ϕ either $\mathcal{T} \vdash \phi$ or $\mathcal{T} \vdash \neg\phi$ then the class of structures is complete. Model complete classes occur more 'frequently', e.g. the class of algebraically closed fields. We will not define model companionable classes, since in our cases of interest, the classes of structures have the amalgamation property, in which case this class has further properties. Classes of structures which are substructure complete occur for model complete classes of structures for which the class of substructures has moreover the amalgamation property. The class of these structures then allows elimination of quantifiers. Existentially complete classes of structures exists whenever the respective class is inductive (that is it is closed under unions of chains). The relevant definitions will be made more precise in the sequel.

Definition 8.4.3 *A class $\mathcal{M}$ of L-structures is* complete *if for all L-sentences ϕ and all $A \in \mathcal{M}$*

either $A \models \phi$ or $A \models \neg\phi$.

A theory $\mathcal{T}$ is complete *if* $\mathrm{Mod}(\mathcal{T})$ *is complete.*

For the further definitions we need to introduce the notion of elementary equivalent structures.

Definition 8.4.4 *Two L-structures A and B are called* elementary equivalent *(notation $A \equiv B$) if for all L-sentences ϕ*

$A \models \phi$ *if and only if* $B \models \phi$.

Two L-structures A and B are called elementary equivalent wrt. a common substructure *C (notation $A \equiv_C B$) if for all L-formulas $\phi(X_1, \ldots, X_n)$ and $c_1, \ldots, c_n \in C$*

$A \models \phi(c_1, \ldots, c_n)$ *if and only if* $B \models \phi(c_1, \ldots, c_n)$.

Consequently, a class $\mathcal{M}$ of L-structures is complete if and only if for any $A, B \in \mathcal{M}$, A and B are elementary equivalent.

Definition 8.4.5 *Let A and B be two L-structures. Then A is called* elementary substructure *of B (and B is called* elementary extension *of A) (notation $A \prec B$) if $A \sqsubseteq B$ and for $a_1, \ldots, a_n \in A$, and for all L-formulas $\phi(X_1, \ldots, X_n)$*

$A \models \phi(a_1, \ldots, a_n)$ *if and only if* $B \models \phi(a_1, \ldots, a_n)$.

Model complete classes are defined by the property that every substructure of a structure of the class is an elementary substructure.

Definition 8.4.6 *A class $\mathcal{M}$ of L-structures is* model complete *if for A, $B \in \mathcal{M}$ with $A \sqsubseteq B$ then*

$A \prec B$.

A theory $\mathcal{T}$ is called model complete if $\mathrm{Mod}(\mathcal{T})$ *is model complete.*

Definition 8.4.7 *A class $\mathcal{M}$ of L-structures is* substructure complete *if for A, $B \in \mathcal{M}$ with a common substructure C*

$A \equiv_C B$.

A theory $\mathcal{T}$ is called substructure complete if $\mathrm{Mod}(\mathcal{T})$ *is substructure complete.*

Lemma 8.4.8 *If a class of L-structures $\mathcal{M}$ is substructure complete, then $\mathcal{M}$ is model complete.*

Proof: Let $A, B \in \mathcal{M}$ with $A \sqsubseteq B$. Then A is a common substructure of A and B and since $\mathcal{M}$ is substructure complete $A \equiv_A B$. That is $A \equiv B$, which shows $A \prec B$. □

We will later define existentially complete fields, here is first the general definition of existentially complete structures. Let $\phi_\exists$ denote existential L-formulas, that is $\phi_\exists$ has the form $\exists X_1 \ldots \exists X_k \psi(X_1, \ldots, X_k)$ with ψ quantifier free.

Definition 8.4.9 *Let $A \sqsubseteq B$ be L-structures. A is called* existentially complete *in B if for all existential formulas $\phi_\exists(Y_1, \ldots, Y_l)$, $a_1, \ldots, a_l \in A$*

$$\text{whenever } B \models \phi_\exists(a_1, \ldots, a_l) \text{ then also } A \models \phi_\exists(a_1, \ldots, a_l).$$

If $\mathcal{M}$ is a class of L-structures, and $A \in \mathcal{M}$ is existentially complete in every $B \in \mathcal{M}$, with $A \sqsubseteq B$, then A is existentially complete in $\mathcal{M}$.

Definition 8.4.10 *Call a totally ordered (sub-)set a chain. Then a class $\mathcal{M}$ of L-structures is called* inductive *if it is closed under unions of chains. That means, that for every chain $A_1 \sqsubseteq A_2 \sqsubseteq \ldots$ of structures $A_i \in \mathcal{M}$*

$$A = \bigcup A_i \quad \in \mathcal{M}.$$

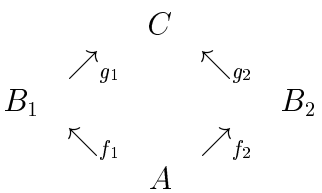
Proposition 8.4.11 *Let $\mathcal{M}$ be an inductive class of L-structures, then each $A \in \mathcal{M}$ is contained in some existentially complete structure $E \in \mathcal{M}$.*

Proof: See [Cohn 1981](p 327) or [Hirschfeld, Wheeler 1975]. □

We denote by $\mathrm{EC}(\mathcal{M})$ the class of existentially complete structures of $\mathcal{M}$. (So $\mathrm{EC}(\mathcal{M}) \subseteq \mathcal{M}$.) For a theory let $\mathrm{EC}(\mathcal{T}) = \mathrm{EC}(\mathrm{Mod}(\mathcal{T}))$. Note that even for a theory $\mathcal{T}$, $\mathrm{Thy}(\mathrm{EC}(\mathcal{T}))$ need not be non-empty.

8.4.3 Amalgamation Property

Definition 8.4.12 *Let $\mathcal{M}$ be a class of L-structures. $\mathcal{M}$ has the* amalgamation property *if for any B_1, $B_2 \in \mathcal{M}$ with a common substructure $A \in \mathcal{M}$ there exists $C \in \mathcal{M}$ and embeddings g_1, g_2 of B_1, B_2 into C,*



such that $g_1(a) = g_2(a)$ for all $a \in A$. C is called an amalgam of B_1 and B_2. A theory $\mathcal{T}$ has the amalgamation property if $\mathrm{Mod}(\mathcal{T})$ *has the amalgamation property.*

Theorem 8.4.13 (Cohn) *The class of (skew) fields has the amalgamation property. More precisely for any (skew) fields B_1 and B_2 the free product over A*

$$C = B_1 \bigcirc_A B_1$$

is an amalgam of B_1 and B_2.

Proof: Let $C = B_1 \bigcirc_A B_1$ be the free product of B_1 and B_2 over A. Let A be a common substructure of the B_i and let $f_i : A \longrightarrow B_i$ be the embeddings of A into B_i $(i = 1, 2)$. Since the free product is faithful the homomorphisms $g_i : B_i \longrightarrow C$ are embeddings of B_i into C $(i = 1, 2)$. Since the free product is separating we have $g_1(f_1(A)) = g_1(B_1) \cap g_2(B_2) = g_2(f_2(A))$. So if we identify A with $f_i(A)$ in B_i we have $g_1(a) = g_2(a)$ for all $a \in A$. This shows that the free product C is an amalgam of B_1 and B_2 over A. □

The relation between model completeness and substructure completeness is as follows

Theorem 8.4.14 *An axiomatizable class of L-structures $\mathcal{M}$ is substructure complete, if and only if $\mathcal{M}$ is model complete and the class of substructures of $\mathcal{M}$ has the amalgamation property.*

Proof: Assume $\mathcal{M}$ is model complete and has the amalgamation property. Let $A, B, C \in \mathcal{M}$ such that C is a common substructure of A and B. By the amalgamation property there exists D in $\mathcal{M}$ which is a common extension of A and B. Since $\mathcal{M}$ is model complete, we have $A \prec D$ and $B \prec D$. By this we have for $c_1, \ldots, c_n \in C$ and for all ϕ

$$A \models \phi(c_1, \ldots, c_n) \iff D \models \phi(c_1, \ldots, c_n) \iff B \models \phi(c_1, \ldots, c_n).$$

This shows $A \equiv_C B$ and $\mathcal{M}$ is substructure complete.

Assume $\mathcal{M}$ is substructure complete, then we have already shown, that $\mathcal{M}$ is model complete. Let $A, B, C \in \mathcal{M}$, such that C is a common substructure of A and B. The existence of a common extension of A and B follows then by arguments involving Robinsons 'model consistency lemma' [Robinson 1974](p. 112) on so called 'diagrams' of A and B over C and by compactness, which we will not present here. □

For existentially complete structures with amalgamation property we note:

Lemma 8.4.15 (Lefschetz Principle) *Let $\mathcal{M}$ be an inductive class of L-structures which has the amalgamation property. Let $A, B_1, B_2 \in \mathcal{M}$ with $B_1, B_2 \in \mathrm{EC}(\mathcal{M})$ and let $a_1, \ldots, a_n \in A$. Then for all existential formulas $\phi_\exists(Y_1, \ldots, Y_l)$,*

$$B_1 \models \phi_\exists(a_1, \ldots, a_l) \text{ if and only if } B_2 \models \phi_\exists(a_1, \ldots, a_l).$$

Proof: By the amalgamation property let $C \in \mathcal{M}$ be a common extension of B_1 and B_2. Then since $B_1 \subseteq C$ we have $C \models \phi_\exists(a_1, \ldots, a_l)$. Now $B_2 \subseteq C$ and B_2 is existentially complete and since $\phi_\exists(a_1, \ldots, a_l)$ is defined over A and holds in C we have $B_2 \models \phi_\exists(a_1, \ldots, a_l)$. □

8.4.4 Quantifier Elimination

Definition 8.4.16 *Let $\mathcal{M}$ be a class of L-structures. Then $\mathcal{M}$ allows* quantifier elimination *if for every formula $\psi(Y_1, \ldots, Y_l)$ there exists a formula $\phi(Y_1, \ldots, Y_l)$ which is quantifier free (or equal to* **true** *or* **false** *if L does not contain constants) and*

$$\mathcal{M} \models \psi(Y_1, \ldots, Y_l) \longleftrightarrow \phi(Y_1, \ldots, Y_l).$$

Theorem 8.4.17 *Let $\mathcal{M}$ be an axiomatizable class of L-structures. Then $\mathcal{M}$ allows quantifier elimination, if and only if $\mathcal{M}$ is substructure complete.*

Proof: See [Weispfenning 1983] theorem 2.6. □

Let $\mathcal{M}$ be a class of L-structures. If the class $\mathrm{EC}(\mathcal{M})$ is closed under substructures and is axiomatizable and has the amalgamation property then $\mathrm{EC}(\mathcal{M})$ is substructure complete. In case of the class $\mathcal{M}$ of (skew) fields $\mathbf{L}$ which are $\mathbf{K}$-algebras it is known, that $\mathrm{EC}(\mathcal{M})$ is not axiomatizable, see e.g. [Hirschfeld, Wheeler 1975] (p 133).

8.4.5 Polynomials as Terms

Let R be a ring, let V be a set of variables and let L_R be the language $L_R = (\emptyset, \{+, -, \cdot\}, \sigma, R \cup \{0, 1\}, V)$. Let $X \subseteq V$ be a distinguished set of variables. Then every polynomial of the polynomial ring $R\langle X\rangle$ corresponds to a term from $\mathtt{Tm}(L_R, X)$. On the other hand, if we identify terms with the same 'meaning', every equivalence class of terms corresponds to a polynomial.

In this sense we will identify polynomials with terms and we will consider polynomials as constituents of first order L_R formulas. If ψ is an L_R formula for some ring (or structure) R, then we say that ψ is defined over R.

8.4.6 Notes on the Nullstellensätze

There are many flavours of Nullstellensätze in the literature. In order to make the notation of 'weak', 'normal' and 'strong' Nullstellensätze more precise we consider the following cases:

1. 'pure' existence of roots in some extension field if the considered ideal is proper,
2. existence of roots in existentially complete fields, for proper ideals in polynomial rings over an existentially complete field,
3. existence of roots of proper ideals in *one* existentially complete field implies the existence of roots in *all* existentially complete fields,
4. given a bound on the degrees of the generating polynomials (and their number) then there exist degree bounds on the polynomials required to represent 1 as element of the ideal.

Additionally a similar case distinction can be considered for the question of roots of ideals, which are not roots of some other polynomial.

To solve 1) above one requires information on the class of algebraic structures considered, e.g. primeness of ideals, embeddability conditions into fields. To solve 2) the only important thing to know is that the considered class of algebraic structures, is inductive. And this in turn is true, whenever the class can be axiomatized by $\forall\exists$ formulas. To solve 3) it must be known whether the subclass of existentially complete structures has the amalgamation property or not. To solve 4) one must even know that the subclass of existentially complete structures allows quantifier elimination. This together with compactness arguments establishes the degree bounds.

There are many criterions to establish the respective requirements. To establish these results for the class of Q-complete fields we use Gröbner bases and comprehensive Gröbner base methods in the proofs.

8.5 Existentially Complete Fields

In this section we summarize the results of Cohn, Hirschfeld and Wheeler about existentially complete 'free' skew fields. The first result states the existence of existentially complete fields and the second result states a Nullstellensatz relative to the existence of d-radicals. The problem is that such d-radicals are hard to characterize and difficult to find. Furthermore, since the free non-commutative polynomial ring $P = \mathbf{K}\langle X_1, \ldots, X_n\rangle$ over a field $\mathbf{K}$ is non Noetherian, ideals may not be finitely generated. Even worse, by a result of [Hirschfeld, Wheeler 1975], the class of existentially complete skew fields is *not* axiomatizable. The definition of consistence of a formula and existentially complete structures adapted for (skew) fields reads as follows:

Definition 8.5.1 *Let* $\mathbf{K}$ *be a (skew) field. Let* $\exists X_1 \ldots \exists X_k \psi(X_1, \ldots, X_k)$ *denote existential formulas which are defined over* $\mathbf{K}$ *(that is* $\psi \in L_{\mathbf{K}}$*) and* ψ *quantifier free. The formula* ψ *is said to be* consistent *if there exists a field* $\mathbf{L}$, $\mathbf{K} \subseteq \mathbf{L}$ *and* $a \in \mathbf{L}^k$ *with* $\mathbf{L} \models \psi(a)$. $\mathbf{K}$ *is called* existentially complete *if*

> *for all extension fields* $\mathbf{E}$ *of* $\mathbf{K}$ *and* $a \in \mathbf{E}^k$ *with* $\mathbf{E} \models \psi(a)$ *follows that there exists* $b \in \mathbf{K}^k$ *with* $\mathbf{K} \models \psi(b)$.

Theorem 8.5.2 (Cohn) *Let* $\mathbf{K}$ *be a skew field. Then there exists an existentially complete field* $\mathbf{E}$*, which contains* $\mathbf{K}$ *and in which every consistent existential formula over* $\mathbf{K}$ *is valid in* $\mathbf{E}$.

Proof: See [Cohn 1977](p 133). □

Definition 8.5.3 (Hirschfeld, Wheeler) *Let* $\mathbf{R}$ *be an algebra over* $\mathbf{K}$. *An ideal* I *in* $\mathbf{R}$ *is called a* d-prime ideal *if* $\mathbf{R}/I$ *can be embedded into a skew field extension of* $\mathbf{K}$ *by*

an algebra homomorphism. The d-radical *of an ideal I is the intersection of all d-prime ideals which contain I. The d-radical is denoted by*

$$\text{d-rad}(I) = \bigcap_{I \subseteq J_i} J_i$$

with J_i d-prime ideals.

Theorem 8.5.4 (Hirschfeld, Wheeler) *Let $\mathbf{E}$ be an existentially complete skew field over $\mathbf{K}$. Let $P = \mathbf{E}\langle X_1, \ldots, X_n\rangle$ be a non-commutative polynomial ring over $\mathbf{E}$. Let I be an ideal in P and let $f \in P$.*

1. *If f shares all roots of I in every skew field extension of $\mathbf{E}$ then f is in the d-radical of I. Moreover if I is finitely generated then if f shares all roots of I in $\mathbf{E}$ then f is in the d-radical of I.*

2. *Conversely if f is in the d-radical of I, then every root of I in E is also a root of f.*

Proof: See [Hirschfeld, Wheeler 1975](p 225). Let d-rad(I) denote the d-radical of an ideal I.

(1) Assume f is not d-rad(I). Then there exists a d-prime ideal J which includes I but not f. Since J is d-prime, P/J can be embedded into a quotient field $Q(P/J)$. Let $\phi : P/J \longrightarrow \mathbf{E}' = Q(P/J)$ denote the embedding homomorphism. Now $\mathbf{E}$ is isomorphic to $\phi(\mathbf{E})$ and therefore $\mathbf{E}'$ can be regarded as an extension field of $\mathbf{E}$. Since $f \notin J$ we have $\phi(f) \neq 0$ in $\mathbf{E}'$ but for every $f \in J$ we have $\phi(f) = 0$ in $\mathbf{E}'$. That is, there exists a root in $\mathbf{E}'^n$ of I which is not a root of f, contradicting our assumption. This proves the first claim.

If I is finitely generated by $\{f_1, \ldots, f_l\}$ then $\mathbf{E}'$ satisfies

$$\exists X_1 \ldots \exists X_n \left(\left(\bigwedge_{1 \leq i \leq l} f_i(X_1, \ldots, X_n) = 0 \right) \wedge \neg (f(X_1, \ldots, X_n) = 0) \right).$$

Since $\mathbf{E}$ was existentially complete, $\mathbf{E}$ must satisfy this sentence also. This proves that there is a root of I in $\mathbf{E}^n$ which is not a root of f.

(2) Assume $f \in$ d-rad(I). Let $\mathbf{E}'$ be a (skew) field extension of $\mathbf{K}$ which extends $\mathbf{E}$, and let $a \in \mathbf{E}'^n$ be a root of I. Let $\phi_a : P \longrightarrow \mathbf{E}'$ be the evaluation morphism. Because $\mathbf{E}'$ is a domain, the kernel of ϕ_a is a d-prime ideal in P which contains I. Since $f \in$ d-rad(I), f is in the kernel of ϕ_a. This shows $0 = \phi_a(f) = f(a)$ and a is therefore also a root of f. □

8.6 Q-existentially complete fields

In this section we consider a variant of existentially complete fields that arise from the study of zeroes of polynomials from solvable polynomial rings. Note that from now on

we assume that for a solvable polynomial ring $S = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ the variables commute with the coefficients. As usual we indicate this by omitting Q' from the definition of $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$. Furthermore we assume the field $\mathbf{K}$ to be a commutative $\mathbf{Q}$-algebra. This restriction is necessary, since we have to define finite formulas, which state, that some elements are a place in an extension field.

Definition 8.6.1 *Let $\mathbf{K}$ be a commutative field or a commutative Noetherian domain (compare definition 8.7.1). Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring. Let $\exists X_1 \ldots \exists X_n \psi(X_1, \ldots, X_n)$ be an existential formula with ψ defined over $\mathbf{K}$ (that is $\psi \in L_{\mathbf{K}}$) and ψ quantifier free. From the polynomials of Q define a formula* $\mathrm{place}_Q(X_1, \ldots, X_n)$ *by:*

$$\bigwedge_{1 \le i \le j \le n} X_j X_i = c_{ij} X_i X_j + p_{ij}(X_1, \ldots, X_n)$$
$$\wedge \ \forall Y \left(\mathrm{in}\mathbf{K}(Y) \longrightarrow \bigwedge_{1 \le i \le n} Y X_i = X_i Y \right)$$

where $\mathrm{in}\mathbf{K}(Y)$ *is a new unary predicate which is interpreted by the set* $\mathbf{K}$. *An* Q-existential formula *over* $\mathbf{K}$ *is an existential formula of the form*

$$\exists X_1 \ldots \exists X_n \left(\psi(X_1, \ldots, X_n) \wedge \mathrm{place}_Q(X_1, \ldots, X_n) \right)$$

with ψ quantifier free. We denote Q-existential formulas by

$$\exists X_1 \ldots \exists X_n \psi_Q(X_1, \ldots, X_n).$$

An Q-existential formula is called Q-algebraic formula *over* $\mathbf{K}$*, if ψ contains no negated atomic formulas.*

We also speak of Q-formulas when we mean Q-algebraic or Q-existential formulas.

Definition 8.6.2 *Let $\mathbf{K}$ be a commutative field. $\mathbf{K} \subseteq \mathbf{E}$ a skew field extension. Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring with commutator relations Q. Let $\mathbf{L}$ be a commutative extension field of $\mathbf{K}$ such that $\mathbf{E}$ is an extension field of $\mathbf{L}$ and $S' = \mathbf{L}\{X_1, \ldots, X_n; Q\}$ is an extension ring of S. Let $\exists X_1 \ldots \exists X_k \psi_Q(X_1, \ldots, X_k)$ denote Q-existential (Q-algebraic) formulas which are defined over $\mathbf{L}$.*

Then $(\mathbf{E}, \mathbf{L})$ is called Q-existentially (Q-algebraically) complete *if for all Q-existential (Q-algebraic) formulas which are defined over $\mathbf{L}$ the following holds*

> *whenever $\mathbf{E} \subseteq \mathbf{E}'$ is an extension skew field of $\mathbf{E}$ and $a \in \mathbf{E}'^k$ with $\mathbf{E}' \models \psi_Q(a)$ then there exists $b \in \mathbf{E}^k$ with $\mathbf{E} \models \psi_Q(b)$.*

Note, that an Q-existentially complete field is Q-algebraically complete. We also speak of Q-complete fields when we mean Q-algebraically or Q-existentially complete fields.

Lemma 8.6.3 *Let* $\mathbf{K} \subset \mathbf{E}$ *and let* $\mathbf{E}$ *be existentially complete and let* Q *be a set of commutator relations of a solvable polynomial ring* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$. *Then* $(\mathbf{E}, \mathbf{K})$ *is Q-existentially complete. Hence there exist Q-existentially complete extension fields of* $\mathbf{K}$ *for every* Q.

Proof: Every Q-existential formula ψ_Q defined over $\mathbf{K}$ is in particular an existential formula over $\mathbf{K}$. So ψ_Q is defined over $\mathbf{E}$ and since $\mathbf{E}$ is existentially complete, by theorem 8.5.2, every consistent existential formula is valid in $\mathbf{E}$. This shows that $(\mathbf{E}, \mathbf{K})$ is also Q-existentially complete. □

Of course one may obtain Q-existentially complete extension fields also directly as follows.

Proposition 8.6.4 *Let* $\mathbf{K}$ *be a commutative field and let* $\mathbf{E}$ *be a skew field extension of* $\mathbf{K}$. *Let* Q *be a set of commutator relations of a solvable polynomial ring* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$.

1. *Then there exists an Q-existentially (Q-algebraically) complete field* $(\mathbf{E}', \mathbf{L})$, *which is an extension of* $\mathbf{E}$ *and in which every consistent Q-existential (Q-algebraic) formula defined over* $\mathbf{L}$ *with* $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{E}$ *is valid in* $\mathbf{E}'$.

2. *Whenever* $(\mathbf{E}', \mathbf{L})$ *is an Q-existentially (Q-algebraically) complete extension field of* $\mathbf{E}$, *then every consistent Q-existential (Q-algebraic) formula defined over* $\mathbf{L}$ *with* $\mathbf{K} \subseteq \mathbf{L} \subseteq \mathbf{E}$ *is valid in* $\mathbf{E}'$.

Proof: (1) Let $\{C_\lambda\}_{\lambda \in \Lambda}$ be the family of all consistent Q-existential (Q-algebraic) formulas defined over a fixed commutative extension field $\mathbf{L} \subseteq \mathbf{E}$ of $\mathbf{K}$. For every λ let $\mathbf{E}_\lambda$ be a skew field extension of $\mathbf{E}$ in which C_λ is valid. Let $\mathbf{H} = \bigcirc_{\mathbf{K}} \mathbf{E}_\lambda$ be the free product of the fields $\mathbf{E}_\lambda$. Then every consistent Q-existential (Q-algebraic) formula defined over $\mathbf{L}$ is valid in $\mathbf{H}$ and by the properties of the free product $\mathbf{L}$ is a subfield of $\mathbf{H}$ and $\mathbf{H}$ is an extension of $\mathbf{E}$. This shows that $(\mathbf{H}, \mathbf{L})$ is a Q-existentially (Q-algebraically) complete extension field of $\mathbf{E}$.

(2) Let ϕ_Q be a consistent Q-existential (Q-algebraic) formula defined over the commutative extension field $\mathbf{L}$ of $\mathbf{K}$ and let $\mathbf{E}$ be a skew field extension of $\mathbf{K}$ and $\mathbf{L}$. Then there exists a skew field extension $\mathbf{H}'$ of $\mathbf{E}$ and $\mathbf{L}$, such that ϕ_Q is valid in $\mathbf{H}'$. Let $(\mathbf{E}', \mathbf{L})$ be an Q-existentially (Q-algebraically) complete extension field of $\mathbf{E}$ and $\mathbf{L}$. Let $\mathbf{H} = \mathbf{E}' \bigcirc_{\mathbf{L}} \mathbf{H}''$, then ϕ_Q is also valid in $\mathbf{H}$ and since $\mathbf{H}$ is an extension field of $\mathbf{E}'$, which was Q-existentially (Q-algebraically) complete it is also valid in $\mathbf{E}'$. □

Theorem 8.6.5 (Hilbert Nullstellensatz) *Let* $\mathbf{K} \subseteq \mathbf{L}$ *be a commutative extension field of* $\mathbf{K}$. *Let* $S' = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring, with commutator relations* Q, *of strictly monic lexicographical type. Let* $S = \mathbf{L}\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring extension of* S'. *Let* I *be an ideal in* S *and let* $f \in S$.

1. *If* f *shares all roots of* I *in some Q-existentially complete extension field* $(\mathbf{E}, \mathbf{L})$ *then* f *is in the complete prime radical of* I.

2. *Conversely if f is in the complete prime radical of I, then every root of I in every (Q-existentially complete) extension field $(\mathbf{E}, \mathbf{L})$ is also a root of f.*

Proof: (1) Assume f is not in the complete prime radical of I. Then $1 \notin I$ and there exists a prime ideal J of S, which includes I but not f. Under the assumptions on Q, by lemma 8.2.10 every prime ideal of S and S' is completely prime, so J is a complete prime ideal. Since S is Noetherian, S/J is an Ore domain and since $1 \notin J$ it can be embedded into a quotient field $Q(S/J)$. Let $\phi : S/J \longrightarrow \mathbf{E}' = Q(S/J)$ denote the embedding homomorphism. Now $\mathbf{L}$ is isomorphic to $\phi(\mathbf{L})$ and therefore $\mathbf{E}'$ can be regarded as an extension field of $\mathbf{L}$. Since $f \notin J$ we have $\phi(f) \neq 0$ in $\mathbf{E}'$ but for every $f \in J$ we have $\phi(f) = 0$ in $\mathbf{E}'$. Since S is Noetherian, every ideal is finitely generated, let I be generated by $\{f_1, \ldots, f_l\}$, say. Then $\mathbf{E}'$ satisfies

$$\exists X_1 \ldots \exists X_n \quad \Big(\quad \Big(\bigwedge_{1 \leq i \leq l} f_i(X_1, \ldots, X_n) = 0 \Big) \\ \wedge \neg (f(X_1, \ldots, X_n) = 0) \\ \wedge \operatorname{place}_Q(X_1, \ldots, X_n) \Big).$$

Since $(\mathbf{E}, \mathbf{L})$ was Q-existentially complete, $\mathbf{E}$ must satisfy this sentence also. This proves that there is a root of I in $\mathbf{E}^n$ which is not a root of f.

(2) Assume $f \in \text{c-rad}(I)$. Let $(\mathbf{E}, \mathbf{L})$ be a (Q-existentially complete) extension field and let $a \in \mathbf{E}^n$ be a root of I. Let $\phi_a : S \longrightarrow \mathbf{E}$ be the evaluation morphism. Because $\mathbf{E}$ is a domain, the kernel of ϕ_a is a complete prime ideal J in S. Furthermore J contains I and since $f \in \text{c-rad}(I)$, f is in J. This shows $0 = \phi_a(f) = f(a)$ and a is therefore also a root of f. □

8.7 Comprehensive Gröbner Bases and Q-complete Fields

We are now going to show, that the class of Q-algebraically complete fields is axiomatizable and allows elimination of existential quantifiers. To prove this we have to find a formula ψ, to express the fact that another formula ϕ is consistent. Such formulas can be constructed by means of the parametric ideal membership test 7.8.2 using comprehensive Gröbner bases.

Recall some notation from chapter 7. Let $S = R\{X_1, \ldots, X_n; Q\}$ be a parametric solvable polynomial ring over a ring $R = \mathbf{R}[u_1, \ldots, u_m]$ over a commutative Noetherian domain $\mathbf{R}$.

$$R = \mathbf{R}[u_1, \ldots, u_m] \qquad (*)$$

arises from a ring $R' = \mathbf{R}[U_1, \ldots, U_m]$ in the indeterminates $U_1, \ldots, U_m$ such that $u_j = U_j + I$, $1 \leq j \leq m$, where I is a two-sided ideal in $\mathbf{R}[U_1, \ldots, U_m]$ such that $R = R'/I$.

So $S' = R'\{X_1, \ldots, X_n; Q\}$ is possibly not an associative ring, but we know, that if we specialize the U's to the u's in R or to some elements of a field $\mathbf{K}$, such that $S = R\{X_1, \ldots, X_n; Q\}$ respectively $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ is a solvable polynomial ring, then all arguments are justified.

Let $F = \{f_1, \ldots, f_m\} \subset S$ be a set of polynomials with coefficients in $U_1, \ldots, U_k$. To indicate the dependence on the parameters the polynomials are also denoted by $f(U_1, \ldots, U_k, X_1, \ldots, X_n)$ respectively by $F(U_1, \ldots, U_k, X_1, \ldots, X_n)$. For a specialization of the $U_i \mapsto a_i$, where the a_i's are from commutative extension field of $\mathbf{K}$ we denote by $f(a_1, \ldots, a_k, X_1, \ldots, X_n)$ respectively by $F(a_1, \ldots, a_k, X_1, \ldots, X_n)$ the polynomials under this specialization.

In this section let $\mathbf{K} = \mathbf{Q}$ the field of rational numbers.

Definition 8.7.1 *Let $R = \mathbf{K}[u_1, \ldots, u_k]$ be as in $(*)$ and let $S = R\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring with commutator relations Q. Let $F = \{f_1, \ldots, f_m\} \subset S$, $m \in \mathbf{N}$, be a finite subset of S and let $f \in S$. Let*

$$\exists X_1 \ldots \exists X_n \psi(U_1, \ldots, U_k, X_1 \ldots, X_n)$$

be an Q-algebraic formula with ψ quantifier free. ψ is a boolean combination (without negations) of polynomial equations and a place_Q *condition. Taking the disjunctive normal form and moving the existential quantifiers inside the disjunction we may assume that $\psi = \psi_{FQ}$ is defined by a single conjunction of polynomial equations*

$$\mathrm{place}_Q(X_1, \ldots, X_n) \wedge \bigwedge_{1 \leq i \leq m} f_i(X_1, \ldots, X_n) = 0.$$

Let

$$\exists X_1 \ldots \exists X_n \psi(U_1, \ldots, U_k, X_1 \ldots, X_n)$$

be an Q-existential formula with ψ quantifier free. ψ is a boolean combination (including negations) of polynomial equations and a place_Q *condition. Taking the disjunctive normal form and moving the existential quantifiers inside the disjunction we may assume that $\psi = \psi_{FfQ}$ is defined by a single conjunction of polynomial equations and a single polynomial inequality (by forming the product over all polynomials of the conjunction of inequalities)*

$$\mathrm{place}_Q(X_1, \ldots, X_n) \wedge \left(\bigwedge_{1 \leq i \leq m} f_i(X_1, \ldots, X_n) = 0 \right) \wedge \neg(f(X_1, \ldots, X_n) = 0).$$

Let $G = \{g_1, \ldots, g_l\}$, $l \in \mathbf{N}$ be a comprehensive Gröbner base of $\mathrm{ideal}_t(F)$*. By the parametric ideal membership proposition 7.8.1 there exists a quantifier free formula in $U_1, \ldots, U_k$ which holds under all specializations of the U_i's if $f \in \mathrm{ideal}_t(F)$ under the same specializations. This quantifier free formula*

$$\chi_{FfQ}(U_1, \ldots, U_k)$$

is defined by

$$\bigvee_{\delta \in \Delta_{G,f}} \phi_\delta(U_1, \ldots, U_k)$$

where ϕ_δ *is* $\bigwedge_{\varphi \in \delta} \varphi$ *in the notation of the parametric ideal membership proposition 7.8.1. Furthermore define the (infinite) formula*

$$\chi^*_{FfQ}(U_1, \ldots, U_k)$$

by

$$\bigvee_{\ell \in \mathbf{N}} \chi_{Ff^\ell Q}(U_1, \ldots, U_k).$$

Theorem 8.7.2 *Let* $R = \mathbf{K}[u_1, \ldots, u_k]$ *be as* $(*)$ *and let* $S = R\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring with commutator relations* Q *of strictly monic lexicographical type. Let* $F = \{f_1, \ldots, f_m\} \subset S$ *be a finite set of polynomials and let* $f \in S$.

For F *and* Q *let* $\exists X_1 \ldots \exists X_n \psi_{FQ}(U_1, \ldots, U_k, X_1 \ldots X_n)$ *be an* Q*-algebraic formula and let* $\chi_{F1Q}(U_1, \ldots, U_k)$ *be the quantifier free formula as defined before in 8.7.1. Then for all* Q*-algebraically complete extensions fields* $(\mathbf{E}, \mathbf{L})$ *of* $\mathbf{K}$ *and specializations of the* U_i*'s in* $\mathbf{L}$

$$\mathbf{E} \models \neg\chi_{F1Q} \longleftrightarrow \exists X_1 \ldots \exists X_n \psi_{FQ}$$

For F, f *and* Q *let* $\exists X_1 \ldots \exists X_n \psi_{FfQ}(U_1, \ldots, U_k, X_1 \ldots X_n)$ *be an* Q*-existential formula and let* $\chi^*_{FfQ}(U_1, \ldots, U_k)$ *be the infinite quantifier free formula as defined before in 8.7.1. Then for all* Q*-existentially complete extensions fields* $(\mathbf{E}, \mathbf{L})$ *of* $\mathbf{K}$ *and specializations of the* U_i*'s in* $\mathbf{L}$

$$\mathbf{E} \models \neg\chi^*_{FfQ} \longleftrightarrow \exists X_1 \ldots \exists X_n \psi_{FfQ}$$

Proof: Let $a_1, \ldots, a_k \in \mathbf{L}$. Under the assumptions on the commutator relations Q, by the Nullstellensatz 8.6.5, $1 \notin \text{ideal}_t(F(a_1, \ldots, a_k, X_1 \ldots X_n)) \iff \mathbf{E} \models \exists X_1 \ldots \exists X_n \psi_{FQ}(a_1, \ldots, a_k, X_1 \ldots X_n)$. Then by the parametric proper ideal test 7.8.2 $1 \notin \text{ideal}_t(F(a_1, \ldots, a_k, X_1 \ldots X_n)) \iff \mathbf{E} \models \neg\chi_{F1Q}(a_1, \ldots, a_k)$.

And similarly for the existential case: Again under the assumptions on the commutator relations Q, by the Nullstellensatz 8.6.5, $f \notin \text{c-rad}(\text{ideal}_t(F(a_1, \ldots, a_k, X_1 \ldots X_n))) \iff \mathbf{E} \models \exists X_1 \ldots \exists X_n \psi_{FfQ}(a_1, \ldots, a_k, X_1 \ldots X_n)$. Then by the parametric ideal membership test 7.8.1 $f \notin \text{c-rad}(\text{ideal}_t(F(a_1, \ldots, a_k, X_1 \ldots X_n))) \iff \{f(a_1, \ldots, a_k, X_1 \ldots X_n)^\ell : \ell \in \mathbf{N}\} \cap \text{ideal}_t(F(a_1, \ldots, a_k, X_1 \ldots X_n)) = \emptyset \iff \mathbf{E} \models \bigwedge_{\ell \in \mathbf{N}} \neg\chi_{Ff^\ell Q}(a_1, \ldots, a_k) \iff \mathbf{E} \models \neg\chi^*_{FfQ}(a_1, \ldots, a_k)$. □

Another consequence of the parametric ideal membership test 7.8.2 is the existence of bounds on the (total) degrees of polynomials h_i, g_i representing f in the ideal generated by F, $f = \sum h_i * f_i * g_i$. In particular, there exists such bounds for the polynomial $f = 1$.

Theorem 8.7.3 *Let $d, m, d', n \in \mathbf{N}$. Then there exists a bound $D \in \mathbf{N}$*

$$D = D(d, m, d', n)$$

such that for all solvable polynomial rings $S = \mathbf{L}\{X_1, \ldots, X_n; Q\}$ over $\mathbf{L}$, where $\mathbf{K} \subseteq \mathbf{L}$ is a commutative extension field of $\mathbf{K}$ with commutator relations Q of strictly monic lexicographical type, such that for every commutator polynomial p_{ij} in Q $\deg(p_{ij}) \leq d'$, for $1 \leq i < j \leq n$ and every finite subset $F = \{f_1, \ldots, f_m\}$ of S, with $\deg(f_i) \leq d$, for $1 \leq i \leq m$ and every polynomial $f \in S$ with $\deg(f) \leq d$ the following holds

$$f \in \mathrm{ideal}_t(F)$$

if and only if there exist polynomials $g_i, h_i \in S$, with $\deg(g_i * f_i * h_i) \leq D$ for $1 \leq i \leq m$, with

$$f = \sum_{1 \leq i \leq m} g_i * f_i * h_i.$$

Proof: Let k be a bound for the number of coefficients of $m+1$ polynomials in n variables of degree $\leq d$ (e.g. $(m+1)(d+1)^n$) and the number of coefficients of the commutator polynomials of strictly monic lexicographical type such that for p_{ij} in Q $\deg(p_{ij}) \leq d'$, for $1 \leq i < j \leq n$. Let $R = \mathbf{K}[u_1, \ldots, u_k]$ be as $(*)$ and let $S = R\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring with commutator relations Q of strictly monic lexicographical type. Let $F_{dm} = \{f_1, \ldots, f_m\}$ together with f be the general system of polynomials of degree d with indeterminate coefficients $U_1, \ldots, U_k$ in some arbitrary but fixed order.

The claim that there exist polynomials h_i, g_i with total degrees less than or equal to some constant $c \in \mathbf{N}$ can be formulated as existential sentence $\varphi_c(c_1, \ldots, c_k)$, where $c_1, \ldots, c_k \in \mathbf{L}$ are the coefficients of F_{dm} and f

$$\exists b_1, \ldots, b_k, d_1, \ldots, d_k \phi_c(b_1, \ldots, b_k, c_1, \ldots, c_k, d_1, \ldots, d_k),$$

over the coefficients b_j, c_j, d_j, $(1 \leq j \leq k)$, of the polynomials h_i, f_i, f and g_i respectively. Where ϕ_c can be determined (using the parametric product lemma 7.1.2) by comparing the coefficients of the monomials in the equation $f = \sum_{i=1}^{m} h_i * f_i * g_i$. Furthermore by the ideal membership test 7.8.1 there exists a quantifier free formula $\chi_{FfQ} = \chi_{FfQdm}$, such that for all extension fields $\mathbf{E}$ of $\mathbf{L}$ and all coefficients $c_j \in \mathbf{L}$, $\mathbf{E} \models \chi_{FfQdm}(c_1, \ldots, c_k) \Longleftrightarrow f \in \mathrm{ideal}_t(F(c_1, \ldots, c_k, X_1, \ldots, X_n))$. Assume that for all $c \in \mathbf{N}$, $\varphi_c(c_1, \ldots, c_k)$ does not hold, then

$$\chi_{FfQdm}(c_1, \ldots, c_k) \wedge \bigwedge_{c \in \mathbf{N}} \neg \varphi_c(c_1, \ldots, c_k),$$

is contradictory. By a corollary to the compactness theorem this holds if and only if it holds for a finite set of φ_c's $\chi_{FfQdm}(c_1, \ldots, c_k) \wedge \bigwedge_{0 \leq c \leq c'} \neg \varphi_c(c_1, \ldots, c_k)$. So it follows that

$$\Phi_F \models \chi_{FfQdm}(c_1, \ldots, c_k) \longrightarrow \bigvee_{0 \leq c \leq c'} \varphi_c(c_1, \ldots, c_k).$$

holds, where Φ_F denotes the axioms for commutative fields. If $\varphi_{c^*}(c_1, \ldots, c_k)$ holds for $0 \leq c^* \leq c'$, then $f \in I$ and $\varphi_{c''}(c_1, \ldots, c_k)$ also holds for all $c^* \leq c'' \in \mathbf{N}$. Finally we observe, that the constant c' does not depend on the particular $\mathbf{L}$ but it depends only on n, m, d' and d, so we let $D(d, m, d', n) = c'$ and end the proof. $\square$

Corollary 8.7.4 *Let* $\mathbf{E}$ *be an extension field of* $\mathbf{Q}$*, and let* Q *be a fixed set of commutator relations of strictly monic lexicographical type of a solvable polynomial ring* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$*. For* $d, m \in \mathbf{N}$ *let* $\exists X_1 \ldots \exists X_n \psi_{FQdm}$ *be the general* Q*-algebraic formula for a set of general polynomials with degrees* $\leq d$ *in indeterminate coefficients* $U_1, \ldots, U_k$ *and let* Ψ_{Qdm} *be the formula*

$$\begin{aligned} \forall U_1, \ldots, \forall U_{k(d)} \quad & \Big(\Big(\bigwedge_{1 \leq i \leq k(d)} \mathrm{in}\mathbf{L}(U_i) \Big) \longrightarrow \\ & \Big(\neg \chi_{F1Qdm}(U_1, \ldots, U_k) \longrightarrow \\ & \exists X_1 \ldots \exists X_n \psi_{FQdm}(U_1, \ldots, U_k, X_1, \ldots, X_n) \Big) \Big). \end{aligned}$$

Then $(\mathbf{E}, \mathbf{L})$ *is algebraically* Q*-complete if and only if for all* $d, m \in \mathbf{N}$

$$\mathbf{E} \models \Psi_{Qdm}.$$

Proof: Assume $(\mathbf{E}, \mathbf{L})$ is Q-algebraically complete and let $a_1, \ldots a_k \in \mathbf{E}$. Then the condition $\bigwedge_{1 \leq i \leq k(d)} \mathrm{in}\mathbf{L}(U_i)$ ensures that the whole formula is defined over the commutative extension field $\mathbf{L}$ of $\mathbf{K}$. Now if $\neg \chi_{F1Qdm}(a_1, \ldots, a_k)$ holds, it implies the consistence of the formula $\exists X_1 \ldots \exists X_n \psi_{FQdm}(a_1, \ldots, a_k, X_1, \ldots, X_n)$. So $\exists X_1 \ldots \exists X_n \psi_{FQdm}$ is a consistent Q-algebraic formula defined over $\mathbf{L} \subseteq \mathbf{E}$ which extends $\mathbf{Q}$. Since $(\mathbf{E}, \mathbf{L})$ is Q-algebraically complete Ψ_{Qdm} is valid in $\mathbf{E}$ for all $d, m \in \mathbf{N}$.

Assume $\mathbf{E} \models \Psi_{Qdm}$ for all $d, m \in \mathbf{N}$. Let $\mathbf{Q} \subseteq \mathbf{L} \subseteq \mathbf{E}$. Let $a_1, \ldots, a_l \in \mathbf{L}$ and let $\exists X_1 \ldots \exists X_n \psi'_Q(a_1, \ldots, a_l, X_1, \ldots, X_n)$ be a consistent Q-algebraic formula defined over $\mathbf{L}$, such that all elements of $\mathbf{L}$ in ψ'_Q are among $a_1, \ldots, a_l$, which is a conjunction of polynomial equations and a place_Q condition. Let $d, m \in \mathbf{N}$ and $k \in \mathbf{N}$ with $l \leq k$ such that F is the general system of polynomials in indeterminate coefficients $U_1, \ldots, U_k$ such that the formula $\psi'_Q(a_1, \ldots, a_l, X_1, \ldots, X_n)$ is equal to $\psi_{FQdm}(a_1, \ldots, a_k, X_1, \ldots, X_n)$. Since ψ'_Q is consistent $\neg \chi_{F1Qdm}(a_1, \ldots, a_k)$ implies $\exists X_1 \ldots \exists X_n \psi_{FQdm}(a_1, \ldots, a_k, X_1, \ldots, X_n)$. Now by assumption $\mathbf{E} \models \Psi_{Qdm}$ which shows, that $\mathbf{E} \models \exists X_1 \ldots \exists X_n \psi'_Q(a_1, \ldots, a_k, X_1, \ldots, X_n)$, i.e. $(\mathbf{E}, \mathbf{L})$ is Q-algebraically complete. □

8.8 Axiomatizability and Quantifier Elimination

We are now ready to state that the class of Q-algebraically complete fields is axiomatizable.

Corollary 8.8.1 *Let* $L = (0, 1, +, -, \cdot, *)$ *be the language of solvable polynomial rings. Let* Q *be a fixed set of commutator relations of strictly monic lexicographical type of a solvable polynomial ring over* $\mathbf{Q}$*. Then the class* $\mathcal{S}$ *of* Q*-algebraically complete fields is axiomatizable in* L*.*

Proof: Let Φ_F be the axioms of commutative fields of characteristic zero with a fixed commutative extension field $\mathbf{L}$ described by the predicate 'in$\mathbf{L}$'. Let Q be the commutator relations of a solvable polynomial ring as defined in 3.2.1. For each $d, m \in \mathbf{N}$ let $\Psi_{dm} = \Psi_{Qdm}$ be the formula as defined in the previous proposition 8.7.4. Let $\Phi = \{\Psi_{dm} : d, m \in \mathbf{N}\}$. Then $\Phi^* = \Phi_F \cup \Phi$ is an (enumerable) set of axioms. Now by theorem 8.7.4 we have $(\mathbf{E}, \mathbf{L}) \in \mathcal{S} \Longleftrightarrow \mathbf{E} \models \Phi^*$. This shows that $\mathcal{S}$ is axiomatizable by Φ^*. □

We proved actually more than was needed for axiomatizability. The comprehensive Gröbner bases provide moreover a means for quantifier elimination.

Corollary 8.8.2 *Let $L = (0, 1, +, -, \cdot, *)$ be the language of solvable polynomial rings. Let Q be a fixed set of commutator relations of strictly monic lexicographical type of a solvable polynomial ring over $\mathbf{Q}$. Then the class $\mathcal{S}$ of Q-algebraically complete fields allows elimination of existential quantifiers in Q-algebraic formulas.*

Proof: Let $\exists X_1 \ldots \exists X_n \psi_{FQ}$ be an Q-algebraic formula with ψ_{FQ} quantifier free. Let χ_{F1Q} be the corresponding quantifier free formula as defined before in 8.7.1. Then by theorem 8.7.2 in an Q-algebraically complete field $(\mathbf{E}, \mathbf{L})$ we have

$$\mathbf{E} \models \exists X_1 \ldots \exists X_n \psi_{FQ} \longleftrightarrow \chi_{F1Q}.$$

This shows that $\mathcal{S}$ allows elimination of existential quantifiers. □

The case of universal quantifiers would require that $\forall X \phi \longleftrightarrow \neg \exists X \neg \phi$ can be used. This however introduces negations in the formulas. In the theory of (skew) fields for formulas (polynomials) f: $\neg(f = 0) \longleftrightarrow \exists X(fX - 1 = 0)$ holds, so negation can be reformulated by an existential formula. In our setting it would be necessary to define some commutator relation for X. Since X is intended to be an inverse of f: f^{-1}. So we must have

$$X * X_i = X_i X + (f(X_1, \ldots, X_n)^{-1} * X_i - f(X_1, \ldots, X_n)^{-1} * X_i)$$

for $1 \leq i \leq n$. But it is in general not true, that this defines commutator relations for a solvable polynomial ring (see also section 8.11). The general case could then be handled by induction on the number of alternating quantifier blocks.

8.9 Strong Theorems on Roots

In this section, we state some stronger versions on theorems on roots using the Lefschetz principle, which is a consequence of the amalgamation property. Then we summarize the theorems on roots.

Theorem 8.9.1 (Strong Algebraic Nullstellensatz) *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring of strictly monic lexicographical type. Let I be a proper two-sided ideal in S. Then the following are equivalent*

1. *There exists some Q-algebraically complete field* $(\mathbf{E}, \mathbf{L})$ *over* $\mathbf{K}$ *and there exist* $a_1, \ldots, a_n \in \mathbf{E}$ *such that* $(a_1, \ldots, a_n)$ *is a root of* I.

2. *In all Q-algebraically complete fields* $(\mathbf{E}, \mathbf{L})$ *over* $\mathbf{K}$ *there exist* $a_1, \ldots, a_n \in \mathbf{E}$ *such that* $(a_1, \ldots, a_n)$ *is a root of* I.

Proof: It suffices to show (1) $\Rightarrow$ (2): Let $(\mathbf{E}, \mathbf{L})$ be some Q-algebraically complete field over $\mathbf{K}$ and let $a_1, \ldots, a_n \in \mathbf{E}$ such that $(a_1, \ldots, a_n)$ is a root of I. Let $I = \mathrm{ideal}_t(f_1, \ldots, f_m)$. Let $b_1, \ldots, b_k \in \mathbf{L}$ be the coefficients of the polynomials $f_1, \ldots, f_m$ in $\mathbf{L} \subseteq \mathbf{E}$ of $\mathbf{K}$. Replace the $b_1, \ldots, b_k$ by new indeterminates $U_1, \ldots, U_k$ and let the resulting Q-algebraic formula $\Psi_{FQ}(U_1, \ldots, U_k)$ be

$$\exists X_1 \ldots \exists X_n \psi_{FQ}(U_1, \ldots, U_k, X_1, \ldots, X_n).$$

Now by assumption $\mathbf{E} \models \Psi_{FQ}(b_1, \ldots, b_k)$. Let $(\mathbf{E}', \mathbf{L})$ be another Q-algebraically complete field over $\mathbf{K}$. Then by the Lefschetz principle also $\mathbf{E}' \models \Psi_{FQ}(b_1, \ldots, b_k)$. This shows that there exist $a_1, \ldots, a_n \in \mathbf{E}'$ such that $(a_1, \ldots, a_n)$ is a root of I. $\square$

Theorem 8.9.2 (Strong Existential Nullstellensatz) *Let* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring of strictly monic lexicographical type. Let* I *be a proper two-sided ideal in* S *and let* $0 \neq f \in S$. *Then the following are equivalent*

1. *There exists some Q-existentially complete field* $(\mathbf{E}, \mathbf{L})$ *over* $\mathbf{K}$ *such that all roots* $(a_1, \ldots, a_n)$ *of* I *in* $\mathbf{E}^n$ *are not roots of* f.

2. *In all Q-existentially complete fields* $(\mathbf{E}, \mathbf{L})$ *over* $\mathbf{K}$ *all roots* $(a_1, \ldots, a_n)$ *of* I *in* $\mathbf{E}^n$ *are not roots of* f.

Proof: It suffices to show (1) $\Rightarrow$ (2): Let $(\mathbf{E}, \mathbf{L})$ be some Q-existentially complete field over $\mathbf{K}$ and let $a_1, \ldots, a_n \in \mathbf{E}$ such that $(a_1, \ldots, a_n)$ is a root of I which is not a root of f. Let $I = \mathrm{ideal}_t(f_1, \ldots, f_m)$. Let $b_1, \ldots, b_k \in \mathbf{L}$ be the coefficients of the polynomials $f, f_1, \ldots, f_m$ in $\mathbf{L} \subseteq \mathbf{E}$ of $\mathbf{K}$. Replace the $b_1, \ldots, b_k$ by new indeterminates $U_1, \ldots, U_k$ and let the resulting Q-existential formula $\Psi_{FfQ}(U_1, \ldots, U_k)$, containing $\neg(f = 0)$, be

$$\exists X_1 \ldots \exists X_n \psi_{FfQ}(U_1, \ldots, U_k, X_1, \ldots, X_n).$$

By assumption $\mathbf{E} \models \Psi_{FfQ}(b_1, \ldots, b_k)$. Let $(\mathbf{E}', \mathbf{L})$ be another Q-existentially complete field over $\mathbf{K}$. Then by the Lefschetz principle also $\mathbf{E}' \models \Psi_{FfQ}(b_1, \ldots, b_k)$. This shows that all roots $(a_1, \ldots, a_n)$ of I in $\mathbf{E}'^n$ are not roots of f. $\square$

The last two theorems summarize the results on the Hilbert Nullstellensatz in algebraic and existential extension fields compatible with solvable polynomial rings with commutator relations Q.

Theorem 8.9.3 *Let* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring over* $\mathbf{K} = \mathbf{Q}$, *with fixed commutator relations* Q *of strictly monic lexicographical type. Let* F *be a finite subset of* S. *Then the following are equivalent*

1. $1 \notin \text{ideal}_t(F)$.
2. $\text{ideal}_t(F)$ *has a common zero in some extension field of* $\mathbf{K}$.
3. $\text{ideal}_t(F)$ *has a common zero in all Q-algebraically complete extension fields of* $\mathbf{K}$.
4. $\text{ideal}_t(F)$ *has a common zero in some Q-algebraically complete extension field of* $\mathbf{K}$.

Proof: The equivalence between 1 and 2 follows by proposition 8.2.11. The equivalence between 1 and 3 follows by theorem 8.6.5. The equivalence between 3 and 4 follows by theorem 8.9.1. □

Theorem 8.9.4 *Let* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring over* $\mathbf{K} = \mathbf{Q}$, *with fixed commutator relations* Q *of strictly monic lexicographical type. Let* F *be a finite subset of* S *and let* $f \in S$. *Then the following are equivalent*

1. $f \notin \text{c-rad}(\text{ideal}_t(F))$.
2. $\text{ideal}_t(F)$ *has a common zero in some extension field of* $\mathbf{K}$, *which is not a zero of* f.
3. $\text{ideal}_t(F)$ *has a common zero in all Q-existentially complete extension fields of* $\mathbf{K}$, *which is not a zero of* f.
4. $\text{ideal}_t(F)$ *has a common zero in some Q-existentially complete extension field of* $\mathbf{K}$, *which is not a zero of* f.

Proof: The equivalence between 1 and 2 follows by proposition 8.2.14. The equivalence between 1 and 3 follows by theorem 8.6.5. The equivalence between 3 and 4 follows by theorem 8.9.2. □

8.10 Q-existential Varieties

In this section we discuss the relation between semiprime ideals (radical ideals, cf. 2.2.13) and varieties of roots of these ideals. Using this results it makes sense to define a topology (the so called Zariski topology) on the set of complete prime ideals c-spec(S). The radical ideals form the closed sets and correspond one to one to the varieties of roots of ideals.

Definition 8.10.1 *Let* $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ *be a solvable polynomial ring with commutator relations* Q *of strictly monic lexicographical type. Let* $\mathbf{E}$ *be an extension field of* $\mathbf{K}$ *and let* $\mathbf{L}$ *be a fixed commutative extension field of* $\mathbf{K}$ *with* $\mathbf{K} \subset \mathbf{L} \subset \mathbf{E}$. *For a subset* A *of* S *define a subset* V *of* $\mathbf{E}^n$ *by*

$$V = \mathcal{V}(A, \mathbf{E}, Q) = \{(a_1, \ldots, a_n) = a \in \mathbf{E}^n : f(a) = 0 \text{ for all } f \in A \text{ and } \text{place}_Q(a)\}$$

$\mathcal{V}(A, \mathbf{E}, Q)$ *is called the* Q-variety *of* A *over* $(\mathbf{E}, \mathbf{L})$. *If* $V' = \mathcal{V}(A, \mathbf{E}, Q)$ *for some subset* V' *of* $\mathbf{E}^n$ *and some subset* A *of* S *then* V' *is called a variety. If* $\mathbf{E}$ *and* Q *is clear from the context we will simply write* $\mathcal{V}(A)$ *for* $\mathcal{V}(A, \mathbf{E}, Q)$.

Definition 8.10.2 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring with commutator relations Q of strictly monic lexicographical type. Let $\mathbf{E}$ be an extension field of $\mathbf{K}$ and let $\mathbf{L}$ be a fixed commutative extension field of $\mathbf{K}$ with $\mathbf{K} \subset \mathbf{L} \subset \mathbf{E}$.*

For a subset V of Q-places of $\mathbf{E}^n$ define a subset A of S by

$$A = \{f \in S : f(a) = 0 \text{ for all } a \in V\}.$$

Then A is an ideal in S and it is denoted by $A = \text{ideal}(V)$.

Proof: Since the elements of V are Q-places, the evaluation ϕ_a for $a \in V$ is a homomorphism. For all $a \in V$ and for $f, g \in A$ and $h \in S$ we have $\phi_a(f - g) = \phi_a(f) - \phi_a(g) = 0$ and $\phi_a(hf) = \phi_a(h)\phi_a(f) = 0$. This shows that $f - g \in A$ and $hf \in A$ and A is indeed an ideal. □

In analogy to Hirschfeld and Wheeler we get:

Theorem 8.10.3 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring with commutator relations Q of strictly monic lexicographical type. Let $(\mathbf{E}, \mathbf{L})$ be an Q-existentially complete extension field of $\mathbf{K}$ where $\mathbf{L}$ be a fixed commutative extension field of $\mathbf{K}$ with $\mathbf{K} \subset \mathbf{L} \subset \mathbf{E}$.*

1. *Two semiprime ideals in S are distinct if and only if they have different Q-varieties in $\mathbf{E}^n$.*

2. *If V is a Q-variety in $\mathbf{E}^n$ then $\text{ideal}(V)$ is semiprime in S.*

Proof: (1) "$\Longrightarrow$" Let I and J be two distinct semiprime ideals in S. Without loss of generality assume that there exists $f \in I$ which is not in J. Since J is semiprime and $f \notin J = \text{c-rad}(J)$ by theorem 8.6.5 there exists a root a of J in $\mathbf{E}^n$ which is not a root of f. That is $a \in \mathcal{V}(J)$ and $a \notin \mathcal{V}(I)$ which proves one direction.

"$\Longleftarrow$" Let $\mathcal{V}(J)$ and $\mathcal{V}(I)$ be distinct varieties. Without loss of generality assume that there exists $a \in \mathcal{V}(J)$ and $a \notin \mathcal{V}(I)$. Let $f \in I$, then $f(a) \neq 0$. By theorem 8.6.5 we have $f \notin \text{c-rad}(J)$ and since $J = \text{c-rad}(J)$ we have $f \notin J$ which proves the other direction.

(2) Let V be a variety in $\mathbf{E}^n$ and let $A = \text{ideal}(V)$, $A \subseteq S$. Assume there is a polynomial $f \in S$ such that $f \notin A$. Then there exists a place $a \in \mathbf{E}^n$ such that $a \in V$ but $f(a) \neq 0$. Since $f(a) \neq 0$ we have by theorem 8.6.5 that $f \notin \text{c-rad}(A)$. This shows $A = \text{c-rad}(A)$ and proves the claim. □

8.11 Rabinowitch Trick

Let R be a commutative polynomial ring and let I be an ideal in R and let $f \in R$. Then the so called Rabinowitch trick, known form *commutative* ideal theory, states that

there exists $k \in \mathbf{N}$ such that $f^k \in \text{ideal}(I)$
$\iff f \in \text{rad}(I)$
$\iff 1 \in \text{ideal}(\{1 - Zf\} \cup I)$,

where Z is a new variable and $k \in \mathbf{N}$. This trick has the great advantage, that the test whether some power of a polynomial f lies in the ideal I, can be reduced to the question whether 1 is in the ideal generated by I and the polynomial $1 - Zf$. Although for practical purposes a new variable must be adjoined to the ring and the proper ideal test 'computation' must be done in this bigger ring. But also for theoretical reasons this trick is fortunate, since it allows the elimination of negated formulas. These aspects are discussed in the next two subsections.

8.11.1 Existential and Algebraic Completeness

In commutative and in free non-commutative *field* theory some element $a \neq 0$ if and only if a is invertible. So negated atomic formulas are logically equivalent to an existential formula introducing a new variable and a positive atomic formula:

$$\neg(\phi_1(X) = \phi_2(X)) \Longleftrightarrow \exists U \ (\phi_1(X)U = \phi_2(X)U + 1),$$

where ϕ_1, ϕ_2 denote terms in the language of fields. By this equivalence it is clear that existentially completeness is the same as algebraically completeness.

However in case of the solvable polynomial rings this equivalence seems not to hold in general. To see the problems let $\phi_2(X)$ be 0 and let $\phi_1(X)$ be the polynomial $f(X)$. Consider

$$\neg(f(X) = 0) \stackrel{?}{\Longleftrightarrow} \exists U \ (f(X)U = 1) \wedge \text{place}_{Q1}(X, U).$$

In the theory of solvable polynomial rings we *must* specify commutator relations for the new variable U. In the quotient field of S (S is a Noetherian domain) they can be defined as:

$$\begin{aligned} U * X_i &= X_i U + (f(X)^{-1} * X_i - X_i * f(X)^{-1}) \\ U * X_i &= X_i U + g_i(X) \end{aligned}$$

for $g_i \in Q(S)$ for $i = 1, \ldots, n$. In $Q(S)$ the elements g_i are quotients of polynomials from S: $g_i(X) = \frac{p_i(X)}{q_i(X)}$, where the q_i are left fractions. Using syzygy construction (e.g. using Gröbner bases) the $g_i(X) = f(X)^{-1} * X_i - X_i * f(X)^{-1}$ can be constructed together with the $p_i(X)$ and the $q_i(X)$. So $\text{place}_{Q1}(X, U)$ takes the form

$$\begin{aligned} \text{place}_Q(X) \wedge \exists U_1, \ldots, U_n \quad & \Big(\bigwedge_{i=1,\ldots,n} (q_i(X)U_i = p_i(X) \\ & \wedge U * X_i = X_i U + U_i) \\ & \wedge \text{place}_{Q2}(U_1, \ldots, U_n) \Big). \end{aligned}$$

But here again we need to specify commutator relations for the U_i:

$$\begin{aligned} U_i * X_j &= X_j U_i + (g_i(X)^{-1} * X_j - X_j * g_i(X)^{-1}) \\ U_i * X_j &= X_j U_i + g_{ji}(X) \end{aligned}$$

for $g_{ji} \in Q(S)$ for $j, i = 1, \ldots, n$. Let $g_{ji}(X) = \frac{p_{ji}(X)}{q_{ji}(X)}$, then we have for $\text{place}_{Q2}(U_1, \ldots, U_n)$

$$\exists U_{11}, \ldots, U_{nn} \, (\bigwedge_{i,j=1,\ldots,n} (q_{ji}(X)U_{ji} = p_{ji}(X) \wedge U_j * X_i = X_i U_j + U_{ji}) \wedge \text{place}_{Q3}(U_{ij})).$$

At this point it is clear that the construction of such a formula is in general an infinite process. Thus for solvable polynomial rings we have proved a weaker form of the the general results from [Bacsich 1973] (where only finitely many quantifiers are required) in the following proposition.

Proposition 8.11.1 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over a field $\mathbf{K}$ with commutator relations Q. Let $f \in S$, then one can construct an infinite positive formula Ψ, with infinitely many quantifieres, such that*

$$\exists X_1 \ldots \exists X_n \neg (f(X_1, \ldots, X_n) = 0) \Longleftrightarrow \exists X_1 \ldots \exists X_n \Psi(X_1, \ldots, X_n).$$

$\Psi(X_1, \ldots, X_n)$ is defined as

$$\begin{aligned} \exists U, U_1, \ldots, U_n, U_{11}, \ldots, U_{nn}, \ldots \quad & (f(X_1, \ldots, X_n)U = 1) \wedge \text{place}_Q(X_1, \ldots, X_n) \wedge \\ & \Big(\bigwedge_{i=1,\ldots,n} (q_i(X_1, \ldots, X_n)U_i = p_i(X_1, \ldots, X_n) \\ & \qquad \wedge U * X_i = X_i U + U_i) \wedge \\ & (\bigwedge_{i,j=1,\ldots,n} (q_{ji}(X_1, \ldots, X_n)U_{ji} = p_{ji}(X_1, \ldots, X_n) \\ & \wedge U_j * X_i = X_i U_j + U_{ji}) \wedge \ldots) \Big). \end{aligned}$$

8.11.2 Using the Quotient Field

Another possibility to exploit the Rabinowich trick could be to determine $1 \in I + (1 - Zf)$ not in S but in the in the quotient field $Q(S)$ of S.

Proposition 8.11.2 *Let $S = \mathbf{K}\{X_1, \ldots, X_n; Q\}$ be a solvable polynomial ring over a commutative field $\mathbf{K}$ with commutator relations Q of strictly monic lexicographical type. Let $\mathbf{L}$ be an extension field of $\mathbf{K}$. Let I be a two-sided ideal in S generated by $f_1, \ldots, f_k$ and let $0 \neq f \in S$. Let $f' = f^{-1}$ be the inverse of f in $Q(S)$ (that is $f'f = 1$). Let Z be a new variable and define an Ore extension of $Q(S)$ by*

$$S' = Q(S)\{Z; \{ZX_i = X_i Z + (f'X_i - X_i f'), \ i = 1, \ldots, n\}\}.$$

Then the following conditions are equivalent

1. *there exists a root* $a \in \mathbf{L}^n$ *of* I *which is not a root of* f,

2. $1 \notin J = I + (1 - Zf)$, *where* J *is an ideal in* S'.

Proof: $1 \Longrightarrow 2$: Assume $1 \in J$, then we have $1 = \sum_{i=1}^{k} g_i f_i h_i + g(1 - Zf)h$, where $g_i, h_i, g, h \in S'$. Let a be a root of I, that is of every f_i such that $f(a) \neq 0$. Then also $f'(a) \neq 0$ and so define $a' = (a_1, \ldots, a_n, f'(a))$. By construction of S' we have that a' is a place and the evaluation morphism yields: $\phi_{a'}(1 - Zf) = 1 - f'(a)f(a) = 1 - 1 = 0$. So we get $1 = \phi_{a'}(\sum_{i=1}^{k} g_i f_i h_i + g(1 - Zf)h) = 0 + \phi_{a'}(g)0\phi_{a'}(h) = 0$, a contradiction. So the assumption must have been false, which proves $1 \notin J$.

$2 \Longrightarrow 1$: Let $1 \notin J$ and let $a \in \mathbf{L}^n$ be a root of J. Under the assumptions on Q and the extended Q, by lemma 8.2.10 every prime ideal of S' is completely prime. So there exists a root $a' \in \mathbf{L}^{n+1}$ of J. Let $a' = (a_1, \ldots, a_n, a_{n+1}) = (a, a_{n+1})$. So $f_i(a') = 0$ since the f_i do not depend on Z. Now a' is also a root of $1 - Zf$, that is $0 = \phi_{a'}(1 - Zf) = 1 - \phi_{a'}(Z)\phi_{a'}(f)$. That is $\phi_{a'}(f)$ is invertible in $\mathbf{L}$ and so it is nonzero. This proves $f(a') \neq 0$ and so the proposition. $\square$

Appendix A

Generalizations of Solvable Rings

In this chapter we discuss the requirements for more general solvable polynomial rings, where the condition that the head term of the polynomials under the $*$-product is equal to the head term of the commutative product is released. Prominent structures in this class are Grassmann (exterior) algebras. However not much positive results have been achieved with this concept.

In the first section the generalized axioms are presented and it is shown, that the $*$-product of two polynomials is again a polynomial which is smaller or equal to the respective commutative product. Next some implications for the associativity of the $*$-product and the example of exterior algebra is discussed. Finally we try to define a suitable (left) reduction relation for this rings. To ensure, that enough head terms for reduction are present, we define so called saturated polynomial sets. However the saturation process is in general infinite. Only if the set of terms is finite or the commutator relations have certain shape the saturation is finite.

A.1 Generalized Axioms

In this section we first state the axioms of the $*$-product for elements of T and $\mathbf{K}$ and then we extent the $*$-product to arbitrary elements of $\mathbf{R}$. Note, that the notation of the commutator relations is slightly different: in 3.2.1 we write $X_i * a = c_{ai} a X_i + p_{ai}$ but here in A.1.1 we write $X_i * a = c_{ai} X_i + p_{ai}$. So e.g. the condition $c_{ai} = 1$ is here expressed as $c_{ai} = a$.

Axioms A.1.1 *For a fixed term order $<_T$, $(\mathbf{R}, *)$ is called a solvable polynomial ring if the following axioms for $*$ are satisfied:*

1. $(\mathbf{R}, 0, 1, +, -, *, <)$ *is an associative ring with* 1 *and with admissible term order* $<$.
2. (a) *For all* $a, b \in \mathbf{K}$, $t \in T(X_1, \ldots, X_n)$, $a * b * t = abt$.
   (b) *For all* $1 \leq i < n$, $s \in T(X_1, \ldots, X_i)$, $t \in T(X_{i+1}, \ldots, X_n)$, $s * t = st$.

3. *For all* $1 \leq i \leq j \leq n$ *there exist* $c_{ij} \in \mathbf{K}$ *and* $p_{ij} \in \mathbf{R}$, $p_{ij} <_T X_iX_j$ *with* $p_{ii} = 0$ *if* $c_{ii} \neq 0$, *such that*
$$X_j * X_i = c_{ij}X_iX_j + p_{ij}.$$

4. *For all* $1 \leq i \leq n$ *and all* $a \in \mathbf{K}$ *there exist* $c_{ai} \in \mathbf{K}$ *and* $p_{ai} \in \mathbf{K}$, *with* $c_{0i} = 0$, $c_{1i} = 1$, $p_{0i} = 0$, $p_{1i} = 0$, *such that*
$$X_i * a = c_{ai}X_i + p_{ai}.$$

5. *For all* $1 \leq i \leq n$, *all* $0 \leq e, d \in \mathbf{N}$ *such that* $c_{ii} \neq 0$, *there exist* $0 \neq c_{ied} \in \mathbf{K}$, *such that*
$$X_i^e * X_i^d = c_{ied}X_i^{e+d}.$$

Any admissible order satisfying condition (3) will be called $*$-*compatible*. $*$ will denote the new multiplication, the (non-commutative) multiplication in $\mathbf{K}$ and the commutative multiplication in $\mathbf{K}[X_1, \ldots, X_n]$ will be denoted by $\cdot$ or juxtaposition of elements. Solvable polynomial rings will be denoted by $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$, or if Q denotes the set of commutator relations of axiom A.1.1(3), and if Q' denotes the set of commutator relations of axiom A.1.1(4), by $\mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$.

In the following lemma properties of univariate polynomials are considered.

Lemma A.1.2 *Let* $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$ *be a solvable polynomial ring. Let* $c_{ii} \neq 0$, *for some* $1 \leq i \leq n$, *let* $f \in \mathbf{K}[X_i]$, *let* $t \in T(X_1, \ldots, X_i)$, $t = t'X_i^e$, $s \in T(X_i, \ldots, X_n)$, $s = X_i^d s'$.

1. *For* $0 \leq m \in \mathbf{N}$ *there exist* $0 \neq c, c' \in \mathbf{K}$ *such that* $X_i^m = cX_i * X_i^{m-1} = c'X_i^{m-1} * X_i$.
2. $f * X_i \in \mathbf{K}[X_i]$ *and* $\mathrm{HT}(f * X_i) = \mathrm{HT}(fX_i)$.
3. *For* $e \geq 1$, $d \geq 1$ *there exists* $0 \neq c, c' \in \mathbf{K}$ *such that* $s = cX_i * (X_i^{d-1}s') = cX_i * v$ *and* $t = (t'c'X_i^{e-1}) * X_i = u * X_i$.

Proof: (1) By axiom A.1.1(5) there exists $0 \neq c_{i,1,m-1} \in \mathbf{K}$ such that $X_i * X_i^{m-1} = c_{i,1,m-1}X_i^m$. Let $0 \neq c \in \mathbf{K}$ such that $cc_{i,1,m-1} = 1$ then $X_i^m = cX_i * X_i^{m-1}$ as claimed. To prove the second equation let also by axiom A.1.1(5) $0 \neq c_{i,m-1,1} \in \mathbf{K}$ such that $X_i^{m-1} * X_i = c_{i,m-1,1}X_i^m$. Let $0 \neq c' \in \mathbf{K}$ such that $c'c_{i,m-1,1} = 1$ then $X_i^m = cX_i^{m-1} * X_i$ as desired.

(2) By induction on degree f. Let $f = b \in \mathbf{K}$, then by A.1.1(2,a) $b * X_i = bX_i$. Let $f = bX_i^e + f'$, then $f * X_i = (bX_i^e + f') * X_i = b(X_i^e * X_i) + f' * X_i$. By induction assumption $h' = f' * X_i \in \mathbf{K}[X_i]$ and by axiom A.1.1(5) $X_i^e * X_i = c_{i,e,1}X_i^{e+1}$. So $f * X_i = bc_{i,e,1}X_i^{e+1} + h'$ as claimed. Furthermore $bc_{i,e,1} \neq 0$ since $\mathbf{K}$ is a field, i. e. $\mathrm{HT}(f * X_i) = X_i^{e+1} = \mathrm{HT}(fX_i)$.

(3) By (1) we have $s = X_i^e s' = (cX_i * X_i^{e-1})s' = cX_i * (X_i^{e-1}s') = cX_i * v$. Again by (1) we have $t = t'X_i^e = t'(c'X_i^{e-1} * X_i) = (t'c'X_i^{e-1}) * X_i = u * X_i$. □

The next lemma deals with products of polynomials and elements of the coefficient ring. Note: The statement of the following two lemmas is somewhat unlucky, since the proofs seem to be cyclic. However the proof of A.1.3(2) relies only on A.1.4(1), which does not depend on A.1.3.

Lemma A.1.3 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, let $f \in \mathbf{K}[X_i, \ldots, X_j]$, for $1 \leq i \leq j \leq n$ and let $a \in \mathbf{K}$.*

1. *Then $a * f = af$.*
2. *If $c_{ak} \neq 0$, when $a \neq 0$, for $1 \leq k \leq n$ and $a \in \mathbf{K}$, then there exists $c \in \mathbf{K}$ ($c \neq 0$ iff $a \neq 0$) and $h \in \mathbf{K}[X_i, \ldots, X_j]$, $h < f$ such that $f * a = cf + h$.*
3. *In any case $f * a \in \mathbf{K}[X_i, \ldots, X_j]$ and $\mathrm{HT}(f * a) \leq \mathrm{HT}(f)$.*

Proof: By Noetherian induction on f with respect to the quasiorder $<$ on $\mathbf{R}$ induced by $<$ on T.

(1) Let $f = b \in \mathbf{K}$, then by A.1.1(2,a) $a * b = ab$. For $f = bt + f'$, $bt = \mathrm{HM}(f)$ we get $a * f = a * (bt + f') = a * bt + a * f'$. By induction assumption and A.1.1(2,a) this is equal to $abt + af' = af$.

(2) Let $f = b \in \mathbf{K}$, then by A.1.1(2,a) $b * a = ba$ and if $a \neq 0$ then let $c_0 \in \mathbf{K}$ with $c_0 b = ba$ and let $h = 0$. For $f = bt + f'$, $bt = \mathrm{HM}(f)$ we get $f * a = (bt + f') * a = bt * a + f' * a$. By induction assumption $f' * a = c'f' + h'$.

For the first term let $1 \leq k \leq j$ maximal such that $e \geq 0$ and let $t = t'X_k^{e+1} = u * X_k = t'c_0 X_k^e * X_k$ by lemma A.1.2(3) (eventually $c = 1$ and $e = 0$). By A.1.1(4) for $X_k * a = c_{ak}X_k + p_{ak}$ we have $bt * a = b(u * X_k) * a = bu * (X_k * a) = bu * (c_{ak}X_k + p_{ak}) = b(u * c_{ak})X_k + b(u * p_{ak}) = bt'c_0(X_k^e * c_{ak})X_k + bt'c_0(X_k^e * p_{ak})$.

By twofold application of the induction assumption to $X_k^e * c_{ak} = c_1 X_k^e + p_1$ and $X_k^e * p_{ak} = c_2 X_k^e + p_2$ we get $bt * a = b(t' * c_0 c_1 X_k^e + t'c_0 p_1)X_k + b(t' * c_0 c_2 X_k^e + t'c_0 p_2)$. Taking c_1', c_2' such that $c_1' c_0 = c_0 c_1$ and $c_2' = c_0 c_2$ we obtain $bt * a = b(t' * c_1')c_0 X_k^e * X_k + bt' * c_0 p_1 * X_k + b(t' * c_2')X_k^e + bt' * c_0 p_2$.

Using $c_0 X_k^e * X_k = X_k^{e+1}$, induction assumption on $t' * c_1' = c_3 t' + p_3$ and $t' * c_2' = c_4 t' + p_4$, furthermore taking into account that since $p_1 \in \mathbf{K}[X_k]$ and by induction assumption $g_1 = bt' * c_0 p_1 \in \mathbf{K}[X_i, \ldots, X_k]$ we have by lemma A.1.2(2) $g_1 * X_k \in \mathbf{K}[X_i, \ldots, X_k]$. By the same arguments since $p_2 \in \mathbf{K}[X_k]$, $g_2 = bt' * c_0 p_2 \in \mathbf{K}[X_i, \ldots, X_k]$. So the second and fourth summand can be combined to $h_1 = g_1 * X_k + g_2$, and we get $bt * a = b(c_3 t' + p_3)X_k^{e+1} + b(c_4 t' + p_4)X_k^e + h_1$.

Now $t' * X_k^{e+1} = t'X_k^{e+1} = t$ and $t' * X_k^e = t'X_k^e$ by A.1.1(2,b), and again $bp_3 \in \mathbf{K}[X_i, \ldots, X_{k-1}]$, $bp_4 \in \mathbf{K}[X_i, \ldots, X_{k-1}]$ and using lemma A.1.4(1) on $bp_3 * X_k^{e+1}$ and $bp_4 * X_k^e$ the head term becomes $bt * a = bc_3 t + h_2$, where h_2 denotes the sum of the remaining parts. Finally taking $c \in \mathbf{K}$ such that $cb = bc_3$ and with $h = h_2 + h' + (c' - c)f'$, we arrive at $f * a = bt * a + c'f' + h' = cbt + h_2 + c'f' + h' = cf + h$.

(3) In the proof of (2) it may happen, that for some $1 \leq i \leq n$ and some $a \in \mathbf{K}$, $c_{ai} = 0$ and so in the product $X_i * a = 0 + p_{ai}$ the head term vanishes. As a consequence some terms in $f * a$ (probably the head term) may vanish, but the remaining terms are still less than the head term of f and are still in $\mathbf{K}[X_i, \ldots, X_j]$. □

The next lemma considers products of polynomials and terms from disjoint sets of variables.

Lemma A.1.4 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, let $0 \leq i \leq n-1$ and let $f \in \mathbf{K}[X_1, \ldots, X_i]$, $X_j \in \mathbf{R}$ for $(1 \leq j \leq n)$, $t \in T(X_{i+1}, \ldots, X_n)$, $g \in \mathbf{K}[X_{i+1}, \ldots, X_n]$.*

1. *Then $f * t = ft$.*
2. *If $c_{aj} = a$, $p_{aj} = 0$, for $1 \leq j \leq n$ and $a \in \mathbf{K}$, then*
$$f * g = fg.$$
3. *If $c_{ak} \neq 0$ when $a \neq 0$, for $1 \leq k \leq n$ and $a \in \mathbf{K}$, then there exists $c \in \mathbf{K}$ ($c \neq 0$ iff $g \neq 0$) and $h \in \mathbf{K}[X_1, \ldots, X_i]$, $h < \mathrm{HT}(fg)$, such that*
$$f * g = cfg + h.$$
4. *In any case $f * g \in \mathbf{K}[X_1, \ldots, X_n]$ and $\mathrm{HT}(f * g) \leq \mathrm{HT}(fg)$.*

Proof: (1) follows by Noetherian induction on f using axioms A.1.1(2,a,b). Let $f = b \in \mathbf{K}$, then by A.1.1(2,a) $f * t = a * t = at$. Let $f = bt' + f'$, $bt' = \mathrm{HM}(f)$, then $f * t = (bt' + f') * t = bt' * t + f' * t$. Then by A.1.1(2,b) we have $t' * t = t't$. So $f * t = bt't + f' * t = bt't + f't = ft$ by induction assumption on $f' * t$.

(2) follows by Noetherian induction on g: Let $g = a \in \mathbf{K}$, then by lemma A.1.3(2) $f * g = f * a = af$ under the assumptions of (2). Let $g = at + g'$, with $at = \mathrm{HM}(g)$, then $f * g = f * (at + g') = f * at + f * g'$. By (1), the assumptions of (2) and lemma A.1.3(2), the first product gives $f * at = af * t = aft$. $f * g'$ is handled by induction assumption, so we have $f * g = aft + fg' = fg$.

We prove (3) by Noetherian induction on g. Let $g = b \in \mathbf{K}$, then by lemma A.1.3(2): $f * b = cf + h$. Let $g = bt + g'$, $bt = \mathrm{HM}(g)$, then $f * g = f * (bt + g') = (f * b) * t + f * g'$. Again by lemma A.1.3(2): $f * b = c'f + h'$, where $h' \in \mathbf{K}[X_1, \ldots, X_i]$, and we obtain $(c'f + h') * t + f * g' = c'f * t + h' * t + f * g'$. Now by (1): $f * t = ft$, $h' * t = h't$ and $f * g' = c''fg' + h''$ by induction assumption. So $f * g = c'ft + h't + c''fg' + h'' = cfg + h$.

(4) In the proof of (3) it may happen, that for some f and some $b \in \mathbf{K}$, $f * b < \mathrm{HT}(f)$ by A.1.3(3). As a consequence some terms in $f * g$ (probably the head term) may vanish, but the remaining terms are still less than the head term of ft and are still in $\mathbf{K}[X_1, \ldots, X_n]$. □

The following lemma treats products of polynomials under the condition that the product of the head terms does not vanish. But this is condition is not used for the proof, that no product vanishes is only the worst case that can happen. See also the following proposition A.1.6.

Proposition A.1.5 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, and let $f, g \in \mathbf{R}$. Furthermore let $c_{aj} \neq 0$ when $a \neq 0$, for $1 \leq j \leq n$ and $a \in \mathbf{K}$ and let $c_{ij} \neq 0$, $1 \leq i \leq j \leq n$. Then there exists an $h \in \mathbf{R}$ and $c \in \mathbf{K}$, ($c \neq 0$ iff $g \neq 0$), such that*

$$f * g = c \cdot f \cdot g + h$$

and $h <_T \mathrm{HT}(fg)$. Moreover, c and h are uniquely determined by f and g.

Proof: The proof is adapted from [Kandri-Rody, Weispfenning 1988] lemma 1.4. Uniqueness: Let $f * g = cfg + h = c'fg + h'$. Since $h, h' < \mathrm{HT}(fg)$, $\mathrm{HT}(fg)$ cannot be cancelled by some term in h or h', so $c = c'$ and from this follows $h = h'$.

Existence: Follows by Noetherian induction on fg with respect to $<$. Let $f = a \in \mathbf{K}$, then by lemma A.1.3(1): $a * g = ag + 0$. Let $g = b \in \mathbf{K}$, then by lemma A.1.3(2): $f * b = cbf + h$.

For the general case let $f = as + f'$, $g = bt + g'$ with $as = \mathrm{HM}(f)$, $bt = \mathrm{HM}(g)$. Then by distributivity of $*$ and 3 times induction assumption we get

$$f * g = as * bt + as * g' + f' * bt + f' * g' = as * bt + d_1 asg' + d_2 f'bt + d_3 f'g' + h',$$

where $d_1, d_2, d_3 \in \mathbf{K}$, $h' \in \mathbf{R}$, $h' < st = \mathrm{HT}(fg)$. When we have proved that

$$as * bt \quad = \quad cabst + h'', \tag{A.1}$$

with $c \in \mathbf{K}$ and $h'' < st = \mathrm{HT}(fg)$, we can set $d_i' = d_i - c$, $h = h'' + d_1' asg' + d_2' f'bt + d_3' f'g' + h'$ and the claim $f * g = cfg + h$ follows.

It remains to show, that equation (A.1) holds. Assume, that $s \in T(X_h, \ldots, X_j)$ and $t \in T(X_i, \ldots, X_k)$ with h, i maximal and j, k minimal with $1 \leq h \leq j \leq n$, $1 \leq i \leq k \leq n$. We distinguish 4 cases:

Case $j \leq i$: If $j < i$ we can apply lemma A.1.4(3) to obtain $as * bt = cabst + h''$, with $h'' \in \mathbf{K}[X_h, \ldots, X_j]$.

If $i = j$ let $s = s'X_i^e$, $t = X_i^d t'$, with $e > 0$ and $d > 0$. Lemma A.1.3(2) applied to $s * b$ gives $c_3 bs + h_1$, $h_1 < s$. Then $as * bt = a(c_3 bs + h_1) * t = ac_3 bs * t + h_1 * t = ac_3 bs'(X_i^e * X_i^d)t' + h_2$. Where by induction assumption on $h_1 * t = h_2 < st$.

By axiom A.1.1(5) under the assumptions of the lemma we have $X_i^e * X_i^d = c_4 X_i^{e+d}$, $c_4 \neq 0$ and by lemma A.1.3(2) we have $s' * c_4 = c_5 s' + h_3$, $h_3 < s'$ so $as * bt = ac_3 b(s' * c_4)X_i^{e+d} * t' + h_2 = ac_3 b(c_5 s' + h_3)X_i^{e+d} * t' + h_2 = ac_3 bc_5 s' * X_i^{e+d} * t' + ac_3 bh_3 * X_i^{e+d} * t' + h_2 = cabs' * X_i^{e+d} * t' + h''$. Where $c \in \mathbf{K}$ such that $cab = ac_3 bc_5$ and by induction assumption $h'' = ac_3 bh_3 * X_i^{e+d} * t' + h_2$, $h'' < st$.

Now axiom A.1.1(2,b) can be applied to both products in $s' * X_i^{e+d} * t' = st$, and so $as * bt = cabst + h''$.

Case $h \leq i$**:** Let $s = X_h^{e+1}s'' = c_1X_h * X_h^e s'' = c_1X_h * s'$ by lemma A.1.2(3) with $e \geq 0$ (eventually $c_1 = 1$ and $e = 0$).

Now $s' < s$ and by induction assumption let $s' * bt = c_2bs't + h_2$. We get $as * bt = ac_1X_h*(s'*bt) = ac_1X_h*(c_2bs't+h_2) = ac_1(X_h*c_2b)s't+ac_1X_h*h_2$. Since $h_2 < s't$, induction assumption can be applied to the last summand giving $ac_1X_h * h_2 = h_3$ with $h_3 < X_hs't = st$.

By axiom A.1.1(4) there exist $c_3, p_3 \in \mathbf{K}$ with $X_hc_2b = c_3X_h + p_3$. Let $c_4 \in \mathbf{K}$ such that $c_4ab = ac_1c_3$ and let $p_4 = ac_1p_3$ then $as * bt = a(c_1c_3X_h + c_1p_3)s't + h_3 = c_4ab(X_h*s't)+p_4*s't+h_3 = c_4abX_h*(X_h^{e+d}s''t')+p_4s't+h_3 = c_4ab(X_h*X_h^{e+d})*s''t'+h'' = c_4abc_5(X_h^{e+1+d} * s''t') + h'' = cabst + h''$. Using axiom A.1.1(2,a) for products with coefficients, $c_1X_h * s' = s$, $c \in \mathbf{K}$ with $ca = ac_4$ and $h'' = p_4s't + h_3 < st$.

Furthermore using that the (commutative) term $s't$ can be written as $X_h^{e+d}s''t' = X_h^{e+d} * s''t'$ by axiom A.1.1(2,b), ($d \geq 0$ the degree of X_k in t) and using that by axiom A.1.1(5) $X_h*X_h^{e+d} = c_5X_h^{e+1+d}$ and again by axiom A.1.1(2,b) $X_h^{e+1+d}*s''t' = X_h^{e+1+d}s''t' = st$. Finally taking $c \in \mathbf{K}$ such that $cab = c_4abc_5$.

Case $j \leq k$**:** Let $t = t'X_k^{e+1} = u * X_k = t'c_1X_k^e * X_k$ by lemma A.1.2(3) with $e \geq 0$ (eventually $c_1 = 1$ and $e = 0$).

Now $t' < t$ and by induction assumption let $s * bt' = c_2bst' + h_2$. We get $as * bt = a(s*bt')c_1X_k^e*X_k = a(c_2bst'+h_2)c_1X_k^e*X_k = a(c_2bst'*c_1X_k^e)*X_k+(h_2*c_1X_k^e)*X_k$

Since $h_2 < st'$ we can apply induction assumption on both products in the second summand yielding $h_4 = (h_2 * c_1X_k^e) * X_k < st'X_h^{e+1} = st$. Furthermore we can apply induction assumption to $st' * c_1X_k^e = c_3c_1st'X_k^e + h_3$, since $st'X_k^e < st$.

This gives $as * bt = ac_2b(c_3c_1st'X_k^e + h_3) * X_k + h_4 = ac_2bc_3c_1(st'X_k^e) * X_k + ac_2bh_3 * X_k + h_4$ Again the second summand can be handled by induction assumption since $h_3 < st'X_k^e < st$, let $h_5 = ac_2bh_3 * X_k + h_4 < st$.

Now use, that the (commutative) term $st'X_k^e$ can be written as $s't'X_k^{e+d} = s't'*X_k^{e+d}$ by axiom A.1.1(2,b), ($d \geq 0$ the degree of X_k in s). Furthermore by axiom A.1.1(5) we have $X_k^{e+d}*X_k = c_4X_k^{e+1+d}$ thus $as*bt = ac_2bc_3c_1s't'*c_4X_k^{e+1+d}+h_5 = c_5ab(s't'*c_4)X_k^{e+1+d} + h_5$, using $c_5ab = ac_2bc_3c_1$.

With lemma A.1.3(2) $s't' * c_4 = c_6c_4s't' + h_6$, where h_6 is a polynomial in the same variables as $s't'$, and $h_6 < s't'$, we get $as * bt = c_5ab(c_6c_4s't' + h_6)X_k^{e+1+d} + h_5 = c_5abc_6c_4s't' * X_k^{e+1+d} + h_6 * X_k^{e+1+d} + h_5$, By axiom A.1.1(2,b) $s't' * X_k^{e+1+d} = s't'X_k^{e+1+d} = st$ and by lemma A.1.4(3) $h_6 * X_k^{e+1+d} = h_6X_k^{e+1+d} = h_7 < st$. With $cab = c_5abc_6c_4$ we get $as * bt = cabst + h_7 + h_5 = cabst + h''$, where $h'' = h_7 + h_5$.

Case $i < h$ & $k < j$**:** We use again lemma A.1.2(3) to split s and t: $s = s''X_j^{e+1} = u * X_j = s''c_1X_j^e * X_j$, $t = X_i^{d+1}t'' = c_2X_i * X_i^et'' = c_2X_i * t'$, with $e \geq 0$ and $d \geq 0$.

Lemma A.1.3(2) applied to $s * bc_2$ gives $c_3bs + h_1$, $h_1 < s$. We obtain $as * bt = a(s * bc_2)X_i*t' = a(c_3bs+h_1)*X_i*t' = c_4ab(s*X_i)*t'+ah_1*X_i*t' = c_4ab(s''c_1X_j^e)*(X_j*X_i)*t'+h_2$. Where we used two times induction assumption on $ah_1*X_i*t' = h_2 < st$ and $c_4 \in \mathbf{K}$ with $c_4ab = ac_3b$.

By axiom A.1.1(3) let $X_j * X_i = c_{ij}X_iX_j + p_{ij}$ so the first summand becomes $as * bt = c_4ab(s''c_1X_j^e) * (c_{ij}X_iX_j + p_{ij}) * t' + h_2 = c_4abs''c_1(X_j^e * c_{ij}) * X_iX_j * t' + c_4ab(s''c_1X_j^e) * p_{ij} * t' + h_2$.

For the first summand A.1.3(2) can be used to obtain $X_j^e * c_{ij} = c_5X_j^e + h_3$, $h_3 < X_j^e$. The second summand can be handled by induction assumption and combined with h_2 to form $h_4 = c_4ab(s''c_1X_j^e) * p_{ij} * t' + h_2 < st$, so: $as * bt = c_4abs''c_1(c_5X_j^e + h_3) * X_iX_j * t' + h_4 = c_4ab(s''c_1c_5)X_j^e * X_iX_j * t' + c_4abs''c_1 * h_3 * X_iX_j * t' + h_4$.

Using A.1.3(2) for $s''c_1c_5 = c_6s'' + h_5$, $h_5 < s''$ and application of 3 times induction assumption to the second summand and combination with h_4 giving $h_6 = c_4abs''c_1 * h_3 * X_iX_j * t' + h_4 < st$, we obtain $as * bt = c_4ab(c_6s'' + h_5)X_j^e * X_iX_j * t' + h_6 = c_4abc_6(s''X_j^e * X_i) * (X_j * t') + c_4abh_5X_j^e * X_iX_j * t' + h_6$.

From now on let $s''X_j^e = s'$ by axiom A.1.1(2,b). Since $s'X_i < s'X_jX_i \leq st$ and $X_jt' < X_jX_it' \leq st$ induction assumption can be applied to the first and last product of the first summand: $s' * X_i = c_8X_is' + h_8$, $h_8 < s'X_i$ and $X_j * t' = c_9t'X_j + h_9$, $h_9 < X_jt'$. For the second summand we use again induction assumption $h_7 = c_4abh_5X_j^e * X_iX_j * t' + h_6 < st$. So we get $as * bt = c_7ab(c_8X_is' + h_8) * (c_9t'X_j + h_9) + h_7 = c_7ab(c_8(X_is' * c_9)t'X_j + c_8X_is' * h_9 + h_8 * c_9t'X_j + h_8 * h_9) + h_7 = c_7abc_8(X_is' * c_9)t'X_j + h_{10}$. Using several induction assumptions and simplifications on the second to fourth summand, such that $h_{10} = c_7ab(c_8X_is' * h_9 + h_8 * c_9t'X_j + h_8 * h_9) + h_7$, $h_{10} < st$.

Using lemma A.1.3(2) we can write $X_is' * c_9 = c_9X_is' + h_{11}$, $h_{11} < X_is'$. With further simplifications we get: $as * bt = c_7abc_8(c_9X_is' + h_{11})t'X_j + h_{10} = c_7abc_8c_9(X_is') * (t'X_j) + c_7abc_8h_{11} * t'X_j + h_{10} = c_{10}abX_i(s' * t')X_j + h_{12}$. Using $h_{12} = c_7abc_8h_{11} * t'X_j + h_{10} < st$, and $c_{10} \in \mathbf{K}$ such that $c_{10}ab = c_7abc_8c_9$.

Since $s't' < st$ we can apply induction assumption to the middle product $s' * t' = c_{11}s't' + h_{13}$, so $as * bt = c_{10}abX_i(c_{11}s't' + h_{13})X_j = c_{10}ab(X_ic_{11})s't'X_j + c_{10}abX_i * h_{13} * X_j + h_{12} = c_{10}ab(c_{12}X_i + h_{14})(s't')X_j + c_{10}abX_i * h_{13} * X_j + h_{12} = c_{10}abc_{12}X_i * (s't') * X_j + c_{10}ab * h_{14} * (s't') * X_j + h_{15} = c_{13}abX_i * (s't') * X_j + h_{15}$, using induction assumptions on the second summands, $X_ic_{11} = c_{12}X_i + h_{14}$, coefficient products and collecting the rests in $h_{15} < st$.

Now by the hypothesis of this case, $s't' \in T(X_i, \ldots, X_j)$ and we can write $s't' = X_i^ds''t''X_j^e = X_i^d * s''t'' * X_j^e$ using axiom A.1.1(2,b). By axiom A.1.1(5) let $X_i * X_i^d = c_{14}X_i^{d+1}$ and $X_j * X_j^e = c_{15}X_j^{e+1}$.

So $as * bt = c_{13}abc_{14}X_i^{d+1} * s''t'' * c_{15}X_j^{e+1} + h_{15} = c_{16}ab(X_i^{d+1}s''t'' * c_{15}) * X_j^{e+1} + h_{15} = c_{16}ab(c_{17}X_i^{d+1}s''t'' + h_{16}) * X_j^{e+1} + h_{15} = c_{16}abc_{17}X_i^{d+1}s''t'' * X_j^{e+1} + c_{16}abh_{16} * X_j^{e+1} + h_{15} = cabX_i^{d+1}s''t''X_j^{e+1} + h''$.

By axiom A.1.1(2,b) we can write $X_i^{d+1} * s''t'' = X_i^{d+1}s''t''$. Furthermore we use lemma A.1.3(2) on $(X_i^{d+1}s''t'') * c_{15} = c_{17}(X_i^{d+1}s''t'') + h_{16}$ and induction assumption on the second summand such that $h'' = c_{16}abh_{16} * X_j^{e+1} + h_{15}$, $h'' < st$. Finally again by axiom A.1.1(2,b) $X_i^{d+1}s''t'' * X_j^{e+1} = X_i^{d+1}s''t''X_j^{e+1} = st$ and with $c \in \mathbf{K}$ such that $cab = c_{16}abc_{17}$ we obtain $as * bt = cabst + h''$ as desired.

So in all cases we have proved (A.1) and so the lemma. □

The next lemma shows that in any case the $*$-product of two (commutative) polynomials is again a (commutative) polynomial.

Proposition A.1.6 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, and let $f, g \in \mathbf{R}$. Then there exists an $h \in \mathbf{R}$*

$$f * g = h$$

and $h \leq \mathrm{HT}(fg)$, precisely $\mathrm{HT}(f * g) = \mathrm{HT}(fg)$ or $\mathrm{HT}(f * g) < \mathrm{HT}(fg)$. Moreover, h is uniquely determined by f and g.

Proof: In the proof of proposition A.1.5 it may happen, that for some $1 \leq i \leq j \leq n$: $c_{ij} = 0$ or for some $1 \leq i \leq n$, $a \in \mathbf{K}$: $c_{aj} = 0$ As a consequence some terms in $f * g$ (probably the head term) may vanish, but the remaining terms are still less than the head term of fg and are still in $\mathbf{K}[X_1, \ldots, X_n]$. If the product of the head terms does not vanish, then obviously $\mathrm{HT}(f * g) = \mathrm{HT}(fg)$, otherwise $\mathrm{HT}(f * g) = \mathrm{HT}(h) < \mathrm{HT}(fg)$. □

The last lemmas of this section deal with the $*$-product and the quasi-order $<$.

Lemma A.1.7 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n\}$ be a solvable polynomial ring, let $<_T$ be a $*$-compatible admissible term order, and let $f, g \in \mathbf{R}$. Furthermore let $c_{aj} \neq 0$ when $a \neq 0$, for $1 \leq j \leq n$ and $a \in \mathbf{K}$ and let $c_{ij} \neq 0$ $1 \leq i \leq j \leq n$. Then*

1. $\mathrm{HT}(f * g) = \mathrm{HT}(f)\mathrm{HT}(g) = \mathrm{HT}(fg) = \mathrm{HT}(g)\mathrm{HT}(f) = \mathrm{HT}(g * f)$,
2. $\mathrm{HM}(f * g) = c\mathrm{HM}(f)\mathrm{HM}(g)$,
3. *For $h \in \mathbf{R}$,* $\mathrm{HT}(f) < \mathrm{HT}(g)$ *implies* $\mathrm{HT}(f*h) < \mathrm{HT}(g*h)$ *and* $\mathrm{HT}(h*f) < \mathrm{HT}(h*g)$.

Proof: (1) The assumptions of proposition A.1.5 are fulfilled, so $f * g = cfg + h$ with $h < fg$, and we have $\mathrm{HT}(f * g) = \mathrm{HT}(cfg) = \mathrm{HT}(fg) = \mathrm{HT}(f)\mathrm{HT}(g)$ and similarly $\mathrm{HT}(g * f) = \mathrm{HT}(c'gf) = \mathrm{HT}(gf) = \mathrm{HT}(fg)$.

(2) As in (1) $\mathrm{HM}(f * g) = \mathrm{HM}(cfg) = c\mathrm{HM}(fg) = c\mathrm{HM}(f)\mathrm{HM}(g)$.

(3) If $\mathrm{HT}(f) < \mathrm{HT}(g)$, then by (1) and since $<$ is admissible, we have $\mathrm{HT}(f * h) = \mathrm{HT}(f)\mathrm{HT}(h) < \mathrm{HT}(g)\mathrm{HT}(h) = \mathrm{HT}(g * h)$ and $\mathrm{HT}(h * f) = \mathrm{HT}(h)\mathrm{HT}(f) < \mathrm{HT}(h)\mathrm{HT}(g) = \mathrm{HT}(h * g)$. □

A.2 Associativity and Order

The axioms A.1.1(2,3,4,5) do not guarantee the associativity of the $*$-product. So axiom A.1.1(1) imposes some restrictions on the values of the c_{ai}, p_{ai}, c_{ij} and the coefficients of the p_{ij}. These restrictions can be stated as a set of equations between these elements.

Also the admissibility of the order $<$ imposes restrictions on the values of the c_{ai}, p_{ai}, c_{ij} and the coefficients of the p_{ij}.

Consider $\mathbf{R}$ as a $\mathbf{K}$ bi-module generated by the elements of T. Besides the restrictions mentioned in lemmas 3.3.2 and 3.3.3 we note the following.

Lemma A.2.1 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring, satisfying axioms A.1.1(2,3,4,5). If $<$ is an admissible quasi-order on $\mathbf{R}$, then if for some $1 \leq i \leq j \leq n$*

$$c_{ij} = 0 \implies c_{ik}X_iX_k + p_{ik} <_T p_{ij},$$

for all $1 \leq k < j$.

Proof: Let $X_k < X_j$ so we must have $X_i * X_k < X_i * X_j$, i. e. $c_{ik}X_iX_k + p_{ik} <_T c_{ij}X_iX_j + p_{ij} = p_{ij}$. □

Lemma A.2.2 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring, satisfying axioms A.1.1(2,3,4,5). If $<$ is an admissible quasi-order on $\mathbf{R}$, then if for some $1 \leq j \leq n$ and some $0 \neq a \in \mathbf{K}$*

$$c_{aj} = 0 \implies c_{bi} = 0 \text{ and } p_{bi} = 0$$

for all $1 \leq i \leq j$ and all $0 \neq b \in \mathbf{K}$.

Proof: Write $a = bc$ for any $b \in \mathbf{K}$, $0 \neq c \in \mathbf{K}$, then $X_j * a = p_{aj}$ and $X_i * a = X_i * bc = c_{bi}X_ic + p_{bi}c$. From $X_i < X_j$ follows $c_{bi}X_ic + p_{bi}c < p_{aj}$. So $c_{bi} = 0$ and $p_{bi} = 0$ for all $1 \leq i \leq j$ and all $0 \neq b \in \mathbf{K}$. □

A.3 Examples and Applications

In addition to the algebraic structures which satisfy the axioms A.1.1 the extended set of axioms A.1.1 is satisfied by Clifford and Grassmann algebras.

A.3.1 Clifford and Grassmann Algebras

Let $\Lambda(V)$ be a Grassmann algebra of a vector space V over a field $\mathbf{K}$, with basis $X_1, \ldots, X_n$. Define the commutator relations by $c_{ij} = -1$, $p_{ij} = 0$, $c_{ii} = 0$, $p_{ii} = 0$, $1 \leq i < j \leq n$, and $c_{ai} = a$ and $p_{ai} = 0$ $1 \leq i \leq n$, $a \in \mathbf{K}$. Then $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ satisfies the axioms A.1.1.

More generally let $C(V)$ be a Clifford algebra of a vector space V over a field $\mathbf{K}$, with basis $X_1, \ldots, X_n$, determined by the quadratic form

$$Q(X_1, \ldots, X_n) = \sum_{1 \leq i \leq n} q_i X_i^2 + \sum_{1 \leq i < j \leq n} q_{ij} X_i X_j,$$

$q_i, q_{ij} \in \mathbf{K}$ Define the commutator relations by $c_{ij} = -1$, $p_{ij} = q_{ij}$, $c_{ii} = 0$, $p_{ii} = q_i$, $1 \leq i < j \leq n$, and $c_{ai} = a$ and $p_{ai} = 0$ $1 \leq i \leq n$, $a \in \mathbf{K}$. Then $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q, Q'\}$ satisfies the axioms A.1.1.

A.4 Reduction Relations and Saturation

We define non-constructive, constructive and saturated reduction relations. Assume in this section all $c_{ai} \neq 0$ for $a \neq 0$, $a \in \mathbf{K}$ for c_{ai} as in axiom A.1.1(4).

A.4.1 Non-commutative Division

A few remarks on the relation between commutative and non-commutative division are in order.

Lemma A.4.1 *Let $p \in \mathbf{R}$ and let $i \in \{1, \ldots, n\}$. If $\mathrm{HT}(X_i * p) = X_i \mathrm{HT}(p)$ then for all $k \in \mathbf{N}$*

$$\mathrm{HT}(X_i^k * p) = X_i^k \mathrm{HT}(p).$$

Proof: By induction on k: $k = 0$: $\mathrm{HT}(X_i^0 * p) = \mathrm{HT}(p) = X_i^0 \mathrm{HT}(p)$. $k = 1$: by assumption.

$k > 0$: We have $\mathrm{HT}(X_i^k * p) = \mathrm{HT}(cX_i * (X_i^{k-1} * p))$ by lemma A.1.4 and associativity of $*$. And $\mathrm{HT}(cX_i * \mathrm{HT}(X_i^{k-1} * p)) = \mathrm{HT}(cX_i * (X_i^{k-1} \mathrm{HT}(p)))$ by induction assumption. Now let $\mathrm{HT}(p) = u_1 X_i^e u_2$ such that $u_1 \in T(X_1, \ldots, X_{i-1})$ and $u_2 \in T(X_{i+1}, \ldots, X_n)$. Then $X_i^{k-1} \mathrm{HT}(p) = u_1 X_i^{e+k-1} u_2$ and $\mathrm{HT}(cX_i * (X_i^{k-1} \mathrm{HT}(p)) = \mathrm{HT}(cX_i * (u_1 X_i^{e+k-1} u_2)$. By assumption we have $\mathrm{HT}(X_i * (u_1 X_i^e u_2)) = X_i u_1 X_i^e u_2$, which requires $\mathrm{HT}(X_i * u_1) = X_i u_1$ to hold. So $\mathrm{HT}(cX_i * (u_1 X_i^{e+k-1} u_2) = \mathrm{HT}(cu_1 X_i * X_i^{e+k-1} u_2)$ and by lemma A.4.1 the head term is equal to $\mathrm{HT}(cu_1 X_i^{e+k} u_2)$. This shows $\mathrm{HT}(X_i^k * p) = X_i^k \mathrm{HT}(p)$ and proves the lemma. □

Lemma A.4.2 *Let $p \in \mathbf{R}$ and let $J = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$, with $i_j < i_{j'}$ when $j < j'$. If $\mathrm{HT}(X_{i_l} * p) = X_{i_l} \mathrm{HT}(p)$ for all $1 \leq l \leq k$ then for all $u \in T(X_{i_1}, \ldots, X_{i_k})$*

$$\mathrm{HT}(u * p) = u \mathrm{HT}(p).$$

Proof: By induction on $|J|$ using the previous lemma A.4.1. □

A.4.2 Non-constructive Reduction Relations

Our first attempt to define suitable reduction relations is as follows:

Definition A.4.3 (Left Reduction) *Let $p \in \mathbf{R}$, $t \in T$. $\longrightarrow_{t,p} \subseteq \mathbf{R} \times \mathbf{R}$ denotes a* left reduction relation *iff*

> *for $f, f' \in \mathbf{R}$, $t \in T(f)$ with $f \longrightarrow_{t,p} f'$, there exists $u \in T$, $a_u \in \mathbf{K}$ such that $t = \mathrm{HT}(u * p)$, $\mathrm{coeff}(t, f) = a_u * \mathrm{coeff}(t, u * p)$ and*
>
> $$f' = f - a_u * u * p.$$

By construction $t \notin T(f')$. If for certain f, t no such u exists, then t in $T(f)$ is called irreducible.

The definition requires that a suitable $u \in T$ exists for t to be reducible, but in certain situations there might be no constructive method to determine such an u. A trivial but important consequence of the definition is:

Lemma A.4.4 *Let $t, u \in T$, $p \in \mathbf{R}$ such that $t = HT(u * p)$. Then*

$$u * p \longrightarrow_{t,p} 0.$$

In such a case we write $u * p \longrightarrow_p 0$ for short.

Proof: Since $t = HT(u * p)$ there exists $u \in T$ as desired. Let $a_u = 1$ then also $a_u \in \mathbf{K}$ exists with $\text{coeff}(t, u * p) = a_u * \text{coeff}(t, u * p)$. So $u * p \longrightarrow_{t,p} u * p - 1 * u * p = 0$. □

In other words, expressions which look reducible are in fact reducible (with respect to this definition).

A.4.3 Constructive Reduction Relations

To find a constructive definition of reduction one might try only head term reductions:

Definition A.4.5 (Left Head Term Reduction) *Let $p \in \mathbf{R}$, $t \in T$. $\longrightarrow_{t,p} \subseteq \mathbf{R} \times \mathbf{R}$ denotes a* left head term reduction relation *iff*

> *for $f, f' \in \mathbf{R}$, $t \in T(f)$ with $f \longrightarrow_{t,p} f'$, there exists $u \in T$, $a_u \in \mathbf{K}$ such that $t = u \cdot \text{HT}(p) = \text{HT}(u * p)$, $\text{coeff}(t, f) = a_u * \text{coeff}(t, u * p)$ and*
>
> $$f' = f - a_u * u * p.$$

By construction $t \notin T(f')$. If for certain f, t no such u exists, then t in $T(f)$ is called irreducible.

This definition requires that

1. $\text{HT}(p)$ divides t in the commutative sense and
2. the head term of $u * p$ is equal to t.

Now (1) is constructive by comparing exponents of powers of X_i in t and in $\text{HT}(p)$ (which also determines u) and (2) can be tested constructively by proposition A.1.5. Unfortunately it may happen, that for certain $u \in T$, $u * p$ is irreducible with respect to p. Precisely this is the case when $\text{HT}(u * p) < u \cdot \text{HT}(p)$. One way out could be to define reductions only with respect to a (finite) set of polynomials:

Definition A.4.6 (Left Head Term Reduction wrt. P) *Let $P \subset \mathbf{R}$, P finite, $t \in T$, $p \in P$. $\longrightarrow_{t,P} \subseteq \mathbf{R} \times \mathbf{R}$ denotes a* left head term reduction relation wrt. P *iff*

$$\begin{aligned}&\text{for } f, f' \in \mathbf{R},\ t \in T(f) \text{ with } f \longrightarrow_{t,P} f', \text{ there exists } u \in T,\ p' \in P,\ a_u \in \mathbf{K}\\ &\text{such that } t = u \cdot \mathrm{HT}(p') = \mathrm{HT}(u * p'),\ \mathrm{coeff}(t, f) = a_u * \mathrm{coeff}(t, u * p') \text{ and}\end{aligned}$$

$$f' = f - a_u * u * p'.$$

By construction $t \notin T(f')$. If for certain t, f no such u and p' exists, then t in $T(f)$ is called irreducible.

This definition requires that there exists a $p' \in P$ such that

1. $\mathrm{HT}(p')$ divides t in the commutative sense and
2. the head term of $u * p'$ is equal to t.

Now (1) is constructive by comparing exponents of powers of X_i in t and in $\mathrm{HT}(p')$ for all $p' \in P$ (which also determines u) and (2) can be tested constructively by proposition A.1.5. But it still may happen, that for certain $u \in T$, $p \in P$, $u * p$ is irreducible with respect to P. Again this is the case when $P = \{p\}$ and $\mathrm{HT}(u * p) < u \cdot \mathrm{HT}(p)$. This shows, that we need some closure of P, such that such anomalies can not occur.

A.4.4 Saturated Polynomial Sets

The condition on P to improve reducibility is defined as follows:

Definition A.4.7 (Left Head Term Saturation) *Let $P \subset \mathbf{R}$. For $k \in \mathbf{N}$ define*

$$\begin{aligned}P_0 &= P,\\ \bar{P}_0 &= P,\\ P_{k+1} &= \{X_i * p \neq 0 \mid p \in P_k, 1 \leq i \leq n, \text{ for no } p' \in \bar{P}_k, \text{ there exists } u' \in T,\\ &\quad \text{such that } \mathrm{HT}(X_i * p) = u'\mathrm{HT}(p') = \mathrm{HT}(u' * p')\},\\ \bar{P}_{k+1} &= \bar{P}_k \cup P_k,\\ \hat{P} &= \bigcup_{k \in \mathbf{N}} P_k.\end{aligned}$$

$\hat{P}$ is called a left head term saturated closure *of P. P is called left head term saturated, iff $\hat{P} = P$.*

If no confusion arises we will simply speak of P being saturated, when P is a left head term saturated set. Unfortunately it may happen, that even for finite P, $\hat{P}$ is infinite. But there are several classes of solvable polynomial rings (depending on the type of commutator relations), where $\hat{P}$ is finite when P is finite. First this is true in the 'classical' case, where the head terms behave like in commutative polynomial rings:

Lemma A.4.8 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring. If for all commutator relations in Q and Q', $c_{ij} \neq 0$, for $1 \leq i \leq j \leq n$, (and all $c_{ai} \neq 0$, for $1 \leq i \leq n$ and $0 \neq a \in \mathbf{K}$) then any $P \subset \mathbf{R}$ is left head term saturated. In particular for finite P, $\hat{P}$ is finite.*

Proof: For $f \in P$ let $t = \mathrm{HT}(f)$. By proposition A.1.5 under the assumptions of the lemma we have $\mathrm{HT}(X_i * t) = X_i t$. So t divides $\mathrm{HT}(X_i * t)$ and consequently $P = \hat{P}$, i.e. P is left head term saturated. □

A second class, in case of the inverse lexicographical term order on T, is characterized by the following lemma. For $1 \leq i \leq n$ define $\deg_i(P)$ to be the maximal degree of X_i in any head term of polynomials in P and $\deg_i(p)$ to be the degree of X_i in the head term of p.

Lemma A.4.9 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring and let $<_T$ be the inverse lexicographical term order (admissible for Q). (Furthermore for all commutator relations in Q' let $c_{ai} \neq 0$, for $1 \leq i \leq n$ and $0 \neq a \in \mathbf{K}$.)*

If for all commutator relations in Q, either $c_{ij} \neq 0$, for $1 \leq i \leq j \leq n$, or if $c_{ij} = 0$, for some $1 \leq i \leq j \leq n$ then $p_{ij} <_T X_i$, then for any finite $P \subset \mathbf{R}$ the left head term saturated closure $\hat{P}$ is finite.

Proof: Let P be a finite subset of $\mathbf{R}$. Let $\hat{P} = \bigcup_{k \in \mathbf{N}} P_k$ a saturation of P. We show that there exists $k_0 \in \mathbf{N}$ such that $P_{k_0} = \emptyset$. For $k \in \mathbf{N}$ let $J_k = \{i \mid c_{ij} = 0, \text{ and } \deg_i(P_k) > 0, 1 \leq i \leq j \leq n\}$. Let $l = 0$, $k_l = 0$ and let $s_l = \max\{|J_k|, k > k_l\}$.

If $s_l = 0$ we have for $k > k_l$ that $J_k = \emptyset$ and by lemma A.4.2 $P_k = \hat{P_k}$, so $P_{k+1} = \emptyset$ and $k_0 = k_l + 1$.

For $s_l > 0$, $k > k_l$ let $J_k \neq \emptyset$ and let $i' \in J_k$, be maximal among all $i \in J_k$. Let $m = \deg_{i'}(P_k)$ and $k' = k + m$. Then $\deg_{i'}(P_{k'}) = 0$ since the head terms of polynomials in $P_{k'}$ are free of $X_{i'}$. Recall that polynomials in $P_{k'}$ are formed from polynomials of P_k by multiplication of variables X_i $(1 \leq i \leq n)$. So either the head terms are equal to the commutative head terms and the polynomials do not appear in $P_{k'}$ or the head term vanishes and by assumption on the commutator relation the variable $X_{i'}$ disappears in the head term. So $|J_{k'}| < s_l$ and also for all $k'' > k'$ we have $|J_{k''}| < s_l$ since no more head terms involving $X_{i'}$ are introduced by the assumption on the commutator relations. So $s_{k'} = \max\{|J_k|, k > k'\} < s_l$ and so there exists $k_0 \geq k'$ such that $P_{k_0} = \emptyset$. □

A third class, in case of a total degree term order on T, can be characterized as follows.

Lemma A.4.10 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring and let $<_T$ be the total degree inverse lexicographical term order (admissible for Q). (Furthermore for all commutator relations in Q' let $c_{ai} \neq 0$, for $1 \leq i \leq n$ and $0 \neq a \in \mathbf{K}$.)*

If for all commutator relations in Q, either $c_{ij} \neq 0$, for $1 \leq i \leq j \leq n$, or if $c_{ij} = 0$, for some $1 \leq i \leq j \leq n$ then $p_{ij} = \sum_{k=1}^{n} a_k X_k$ then for any finite $P \subset \mathbf{R}$ the left head term saturated closure $\hat{P}$ is finite.

Proof: Let $1 \leq i \leq j \leq n$ such that $c_{ij} = 0$, then p_{ij} is a linear combination of linear polynomials. By this $\deg(X_j * X_i) = 1$ and consequently

$$\deg(\mathrm{HT}(X_j * p)) = \deg(\mathrm{HT}(p)).$$

Now let m be the maximal degree of the polynomials in P. Then also m is the maximal degree of the polynomials in $\hat{P}$. But the set $\{u \in T \mid \deg(u) \leq m\}$ is finite, and so $\hat{P}$ must be finite too. □

In particular $\hat{P}$ for Grassmann algebras is finite (which is true anyway since the number of terms is equal to 2^n and this is finite). One may ask, if there is a decision procedure or at least a characterization of P such that $\hat{P}$ is finite. A necessary condition on P if $\hat{P}$ is infinite is as follows. However it is not known if the condition is sufficient to prove $\hat{P}$ to be infinite.

Lemma A.4.11 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring and let $<_T$ be an admissible term order. (Furthermore for all commutator relations in Q' let $c_{ai} \neq 0$, for $1 \leq i \leq n$ and $0 \neq a \in \mathbf{K}$.) Let $P \subset \mathbf{R}$ be a finite subset of $\mathbf{R}$, $\hat{P} = \bigcup_{k \in \mathbf{N}} P_k$ the left head term saturated closure of P. If $\hat{P}$ is infinite then the following condition holds:*

> *there exists a $k_0 \in \mathbf{N}$, such that $P_{k_0} \neq \emptyset$ and for all polynomials $p \in P_{k_0}$ there exists $p' \in P'$ such that $\mathrm{HT}(p) = u\mathrm{HT}(p')$ ($u \in T$), and $\mathrm{HT}(p) \neq \mathrm{HT}(u * p')$.*

Proof: Let $\hat{P}$ be infinite. By Dickson's Lemma there exists a (finite) subset P^* of $\hat{P}$, such that for all $p \in \hat{P}$ there exists a $p' \in P^*$ such that $\mathrm{HT}(p) = u\mathrm{HT}(p')$ for some $u \in T$. Trivially $u\mathrm{HT}(p') \neq \mathrm{HT}(u * p')$ since otherwise $p \notin \hat{P}$. Since P^* is finite, there exists $k_0 \in \mathbf{N}$ with $P^* \subseteq P' = \bigcup_{0 \leq k \leq k_0} P_k$. This shows that the condition holds. □

To define a reduction relation a lemma of the following kind is required. However it is false, and there seems to be no condition on the variables, such that it can be made valid.

Lemma A.4.12 *Let $\mathbf{R} = \mathbf{K}\{X_1, \ldots, X_n; Q; Q'\}$ be a solvable polynomial ring and let $<_T$ be an admissible term order. (Furthermore for all commutator relations in Q' let $c_{ai} \neq 0$, for $1 \leq i \leq n$ and $0 \neq a \in \mathbf{K}$.) Let $P \subset \mathbf{R}$ be a finite left head term saturated subset of $\mathbf{R}$.*

For $u \in T$, $p \in P$, there exist $u' \in T$, $p' \in P$, such that

$$\mathrm{HT}(u * p) = u'\mathrm{HT}(p') = \mathrm{HT}(u' * p').$$

One condition to make it valid, could be to assume that the $u' \in T$ with $\mathrm{HT}(u * p) = u'\mathrm{HT}(p') = \mathrm{HT}(u' * p')$ have the property:

$$\mathrm{HT}(X_i * u') = X_i u', \quad 1 \leq i \leq n.$$

This means nearly, that u' is not only required to commute with the head term of p', but also with any variable.

A.4.5 Saturated Reduction Relations

Given such a lemma we could define a suitable reduction:

Definition A.4.13 (Saturated Reduction) *Let $P \subset \mathbf{R}$, P finite and left head term saturated, $t \in T$, $p \in P$. $\longrightarrow_{t,P} \subseteq \mathbf{R} \times \mathbf{R}$ denotes a* saturated reduction relation *iff*

> *for $f, f' \in \mathbf{R}$, $t \in T(f)$ with $f \longrightarrow_{t,P} f'$, there exists $u \in T$, $p' \in P$, $a_u \in \mathbf{K}$ such that $t = u \cdot \mathrm{HT}(p') = \mathrm{HT}(u * p')$, for no $1 \neq w$ with $u = vw$, $w * p' \in P$, $\mathrm{coeff}(t, f) = a_u * \mathrm{coeff}(t, u * p')$ and*
>
> $$f' = f - a_u * u * p'.$$

By construction $t \notin T(f')$. If for certain t, f no such u and p' exists, then t in $T(f)$ is called irreducible.

In order to make this definition to work for a completion procedure, the following lemma is required.

Lemma A.4.14 *Let $P \subset \mathbf{R}$, P left head term saturated, $u \in T$ and $p \in P$, $t = \mathrm{HT}(u * p)$. Then $u * p \longrightarrow_{t,P} f$, for $f \in R$, $f < \mathrm{HT}(u * p)$.*

Proof: By lemma A.4.12. □

Without such a lemma, there is no chance to obtain a meaningful reduction relation.

A.4.6 Saturated Representation

If such lemmas hold then we could also define suitable polynomial representations, so called saturated representations.

Definition A.4.15 (Saturated representation) *Let $P \subset \mathbf{R}$, $f \in I_l(P)$. A representation*

$$f = \sum_{i=1}^{k} c_i s_i * p_i,$$

with $c_i \in \mathbf{K}$, $s_i \in T$, $p_i \in P$ for all $1 \leq i \leq k$ is called a saturated representation wrt. *P iff for all $1 \leq i \leq k$ the following condition is satisfied:*

$$\mathrm{HT}(s_i * p_i) = s_i * \mathrm{HT}(p_i) = s_i \mathrm{HT}(p_i).$$

Lemma A.4.16 *Let $f \in \mathbf{R}$, $P \subset \mathbf{R}$, P finite left head term saturated and fix an admissible term order on T. If $f \in I_l(P)$, then there exists a saturated representation for f.*

Proof: Recall that $f \in I_l(P)$ iff $f = \sum_{i=1}^{k} c_i s_i * p_i$, where $c_i \in \mathbf{K}$, $s_i \in T$ and $p_i \in P$ for $1 \leq i \leq k'$. Let $t \in T$ with $t = \max_{i=0}^{k}\{s_i\mathrm{HT}(p_i) \mid s_i * \mathrm{HT}(p_i) < s_i\mathrm{HT}(p_i)\}$ where the maximum is taken with respect to the term order on T. Let $J_t = \{j \mid 1 \leq j \leq k, s_j\mathrm{HT}(p_j) = t\}$. To establish the condition $\mathrm{HT}(s_i * p_i) = s_i * \mathrm{HT}(p_i) = s_i\mathrm{HT}(p_i)$ for $1 \leq i \leq k$, we modify the given representation by noetherian induction on t and for fixed t by induction on $|J_t|$.

Case $t = 1$ and $|J_t|$ arbitrary. Since $t = 1 = \mathrm{HT}(1 * 1) = 1 \cdot \mathrm{HT}(1)$, we have $|J_t| = \emptyset$ and the condition is satisfied.

Case $t > 1$ and $|J_t| = \emptyset$. then the condition is satisfied. Case $t > 1$ and $|J_t| > 1$. Assume the claim is true for all $t' < t$ with arbitrary $J_{t'}$ and for all J'_t with $|J'_t| < |J_t|$. Let $j \in J_t$, $J'_t = J_t \setminus \{j\}$. Since P is left head term saturated, by A.4.12 there exists $s \in T$, $p \in P$, such that $\mathrm{HT}(s_j * p_j) = s * \mathrm{HT}(p) = s\mathrm{HT}(p) = v < t$. Now let $h = c_j s_j * p_j - cs * p$, where $0 \neq c \in \mathbf{K}$ such that $\mathrm{coeff}(v, c_j s_j * p_j) = c\ \mathrm{coeff}(s * p)$.

Since $h < v < t$, by induction assumption h has a representation $h = \sum_{l=1}^{k'} c'_l s'_l * p'_l$, with $\mathrm{HT}(s'_l * p'_l) = s'_l * \mathrm{HT}(p'_l) = s'_l\mathrm{HT}(p'_l)$, where $k' \in \mathbf{N}$ and for $1 \leq l' \leq k'$ $c'_l \in \mathbf{K}$, $s'_l \in T$, $p'_l \in P$. By this $c_j s_j * p_j = h + cs * p$ has a representation of the required form. And so

$$f = \sum_{i=1, i\neq j}^{k} c_i s_i * p_i + \sum_{l=1}^{k'} c'_l s'_l * p'_l + cs * p.$$

For this representation $J'_t < J_t$ and by induction assumption f has a representation of the required form. This completes the proof. □

The restrictions imposed on the commutator relations are so strong, that we will not pursue this way any further.

Appendix B

Algorithmic Notation

We start with some general remarks about computability.

A set is *decidable* if the elements of the set can be represented in a data structure and there is an algorithm which can determine if two elements are equal.

An algebraic structure is *computable*, if the universe of the structure is decidable as set and for all functions and relations of the structure there is an algorithm which computes the function value for all elements for which the function is defined, respectively computes **true** or **false** for relations.

Where an *algorithm* is a finite description of a method with 'precisely' defined basic operations, which can be performed effectively. Here 'precisely' depends on the target of the algorithm: a human being or an electronic computing device.

In the next section we will make a few remarks on algorithm description and correctness and then we will discuss some algorithm implementation issues.

B.1 Algorithm Description

In this section we summarize the syntax of the pidgin programming language used in the description of the algorithms.

The syntax in extended BNF is contained in table B.1. 'name' denotes syntactic entities, '{}' denote (possibly empty) sequences, '()' denote required entities, '[]' denote optional entities. Key-words are denoted in bold-face and other terminal symbols are enclosed in quotes. Productions are denoted by '='. We do not define a syntax for data structures, since only sets and elements are used in mathematical notation.

So an algorithm is denoted by a specification of a header, a specification of input and output parameter sequences, followed by a sequence of statements. Statements can be mathematical statements, assignments, case selection (**if** statement) or repetition (**while** statement). In more detail we have

Algorithm: the beginning of the algorithm header,

algorithm	= **Algorithm:** ident '(' parameters ')' '.'
	input output
	block ident '.'
input	= **Input:** Specification of input parameters.
output	= **Output:** Specification of output parameters.
block	= **begin** statement-seq **end**
statement-seq	= statement { (';' | '.') statement }
statement	= (math-statement
	| assignment
	| **if** expression **then** statement-seq
	[**else** statement-seq] **end**
	| **while** expression **do** statement-seq **end**
	| **repeat** statement-seq **until** expression
	| **return** expression)
math-statement	= a valid mathematical statement
assignment	= ident '$\leftarrow$' expression
expression	= a valid mathematical expression
parameters	= ident { ',' ident }
ident	= variable identifier

Table B.1: Syntax of Algorithms

Input:	the specification of the algorithm inputs,
Output:	the specification of the algorithm outputs,
return	the terminating statement of an algorithm,
begin	the beginning of a statement sequence,
end	the end of a statement sequence,
if	the begining of the IF-statement,
then	the beginning of the truth case statement sequence in the IF-statement,
else	the beginning of the false case statement sequence in the IF-statement,
while	the beginning of the WHILE-statement,
do	the beginning of the body statement sequence of the WHILE-statement,
repeat	the beginning of the REPEAT-statement,
until	the end of the body statement sequence of the REPEAT-statement and the beginning of the exit condition,

The semantics is so called axiomatic (or mathematical) semantics, as defined in the Hoare calculus. A specification can be any mathematically meaningful condition or description of the input / output parameters (variables).

An algorithm is *partially correct*, if for all input values, which satisfy the input specification, *and* for which the algorithm stops, it 'produces' output values, which satisfy the output specification, An algorithm *terminates*, if for all input values, which satisfy the input specification, the algorithm stops.

An algorithm is *correct* if it terminates and is partially correct. In other words an algorithm is correct, if for all input values, which satisfy the input specification, the algorithm terminates and 'produces' output values, which satisfy the output specification,

B.2 Algorithm Implementation

The implementation of the algorithms uses the MAS (Modula-2 Algebra System) developed by myself [Kredel 1990] [Kredel 1991], which incorporates several systems for polynomial arithmetic [Gebauer, Kredel 1983] and coefficient arithmetic [Collins, Loos 1980]. In this section we give a rough overview of the system and the libraries. The presentation is mainly taken from the manuals. For a detailed description of the programs we must refer the reader to the MAS manuals and the program source texts.

B.2.1 MAS Modula-2 Algebra System

The MAS (Modula–2 Algebra System) is an experimental interactive computer algebra system combining imperative programming facilities with algebraic specification capabilities for design and study of algebraic algorithms.

MAS combines Modula-2 program development, a LISP interpreter with a Modula-2 like language and an algebraic specification component. MAS can be used interactively, but includes access to to the comprehensive ALDES/SAC-2 and DIP algebraic algorithm libraries. MAS can also be used as ordinary Modula-2 program library. Despite of its design it can directly access numerical Modula-2 libraries.

The current implementations run on an Atari 1040ST / GEM-TOS, IBM–PC / MS–DOS (or compatible), and Commodore Amiga / Amiga-DOS, further implementations are planned on Unix workstations. MAS is completely written in the programming language Modula-2 [Wirth 1985].

B.2.2 Polynomial Systems

Polynomials are always represented in some (internal) canonical form. The most important canonical representations are:

- recursive representation,
- distributive (or distributed) representation,
- dense representation.

In the next section we will discuss only the distributive representation. For every representation there are algorithms to read and write polynomials, select parts of polynomials, construct polynomials and to perform basic arithmetic of polynomials (like sum, product, remainder, evaluation, substitution).

For more advanced methods like polynomial greatest common divisors or multivariate polynomial factorization there are algorithms for the recursive polynomial representation. For Gröbner bases and polynomial ideal decomposition or solving systems of polynomial equations there are algorithms for the distributive polynomial representation. The dense representation is mainly used for algorithms for fast univariate polynomial remainder computations.

There is a variety of application dependent 'fine tunings' of representations to optimize space, time or programming complexity of the algorithms which are not discussed here (and which are only partly available in the current system).

Program libraries are composed from the ALDES / SAC-2 computer algebra system by [Collins, Loos 1980], from the DIP polynomial system, which is based on the former, by [Gebauer, Kredel 1983], [Gebauer, Kredel 1984] and from further extensions by myself [Kredel 1988], [Kredel 1988a]. The collection of algorithms and global variables are called

'systems'. The systems are broken into modules according to specific characteristics of subcollections of the algorithms.

The available ALDES / SAC-2 polynomial libraries are the following:

ALDES / SAC–2 Polynomial System,
ALDES / SAC–2 Algebraic Number System,
ALDES / SAC–2 Polynomial GCD and Resultant System,
ALDES / SAC–2 Polynomial Factorization System,
ALDES / SAC–2 Real Root System.

The available DIP polynomial libraries are the following:

DIP Common Distributive Polynomial System,
DIP Distributive Integral Polynomial System,
DIP Distributive Rational Polynomial System,
DIP Distributive Arbitrary Domain Polynomial System,
DIP Buchberger Algorithm System (Gröbner bases),
DIP Polynomial Ideal Dimension System,
DIP Zero-dimensional Polynomial Ideal Decomposition System,
DIP Zero-dimensional Polynomial Ideal Real Root System.

As extension to the DIP system there are the libraries for non-commutative polynomial rings of solvable type:

DIP Non-commutative Rational Distributive Polynomial System,
DIP Non-commutative Gröbner Base System,
DIP Non-commutative Polynomial Center System.

B.2.3 Coefficient Rings

Although the representation of polynomials is independent of the representation of the coefficients the algorithms are implemented for specific coefficient rings.

Programs that work independently of the coefficient ring start with the program prefix '`P`' in case of the recursive polynomial representation and with '`DI`' in case of the distributive polynomial representation.

For the recursive representation there are algorithms for the following coefficient rings:

- integral numbers: $\mathbf{Z}$, program prefix '`IP`' for 'integral polynomial'
- rational numbers: $\mathbf{Q}$, program prefix '`RP`' for 'rational number polynomial'
- integral numbers modulo m: $\mathbf{Z}/_{(m)}$, program prefix '`MIP`' for 'modular integral polynomial'

- algebraic numbers over the rational numbers: $\mathbf{Q}[X]/_{(m_\alpha(X))}$, where $m_\alpha(X)$ denotes the minimal polynomial of α over $\mathbf{Q}$, program prefix '`AFP`' for 'algebraic number field polynomial'.

For the distributive representation there are algorithms for the following coefficient rings:

- integral numbers: $\mathbf{Z}$, program prefix '`DIIP`' for 'distributive integral polynomial'
- rational numbers: $\mathbf{Q}$, program prefix '`DIRP`' for 'distributive rational number polynomial'

In the so called 'distributive arbitrary domain polynomial system' there are algorithms for further coefficient rings.

B.2.4 Distributive Polynomial System

Let R be a commutative ring with 1 and let $S = R[X_1, \ldots, X_r]$ denote a (commutative) polynomial ring in $r \geq 0$ variables (indeterminates) $X_1, \ldots, X_r$. The elements of S are sums of *monomials*, where each monomial is a product of a *base coefficient* and a *term* (power product).

Definition B.2.1 *Let $A(X_1, \ldots, X_r) \in S$, $A \neq 0$ and $r \geq 1$, then*

$$A(X_1, \ldots, X_r) = \sum_{i=1}^{k} a_i X_1^{e_{i1}} \cdot \ldots \cdot X_r^{e_{ir}} = \sum_{i=1}^{k} a_i X^{e_i}$$

with $a_i \neq 0$ for $i = 1, \ldots, k$ and natural numbers e_{ij} for $i = 1, \ldots, k$ and $j = 1, \ldots, r$. X^{e_i} is an abbreviation for $X_1^{e_{i1}} \cdot \ldots \cdot X_r^{e_{ir}}$. k is the number of terms of A. For $r > 0$ the representation of an exponent vector *$e_i = (e_{i1}, \ldots, e_{i,r-1}, e_{ir})$ is the list*

$$\epsilon_i = (e_{ir}, \ldots, e_{i2}, e_{i1}).$$

For $r = 0$ let $\epsilon = ()$, the empty list. The distributive representation *of A is the list*

$$\alpha = (\epsilon_k, \alpha_k, \ldots, \epsilon_2, \alpha_2, \epsilon_1, \alpha_1)$$

where the α_i denote the representations of the a_i and the ϵ_i are the representation of the exponent vectors, $i = 1, \ldots, k$. If $A = 0$ then $\alpha = 0$ and if $r = 0$ then $\alpha = ((), \alpha_1)$.

Note, that the variables $X_1, \ldots, X_r$ are not stored in the representing list. This is different to other computer algebra systems like REDUCE or muMATH. The representation is sparse in the sense, that only base coefficients $\neq 0$ are stored. The representation of the exponent vectors is dense in the sense, that also exponents $= 0$ are stored.

Examples:

1. Let $S = \mathbf{Z}[X]$, that is $R = \mathbf{Z}$ and $r = 1$. Let

$$A = 3X^4 + 5,$$

then $k = 2$ and $e_2 = (4), a_1 = 3, e_1 = (0), a_2 = 5$. The representation is then

$$\alpha = ((4), 3, (0), 5).$$

2. Let $S = \mathbf{Z}[X, Y]$, that is $R = \mathbf{Z}$ and $r = 2$. Let

$$A = (3X + 2)Y^2 + 5X = 3XY^2 + 2Y^2 + 5X,$$

then $k = 3$ and $e_3 = (1, 2), a_3 = 3, e_2 = (0, 2), a_2 = 2, e_1 = (1, 0), a_1 = 5$. The representation is then

$$\alpha = ((2, 1), 3, (2, 0), 2, (0, 1), 5).$$

3. Let $S = \mathbf{Q}[X, Y]$, that is $R = \mathbf{Q}$ and $r = 2$. Let

$$A = \frac{1}{4}X^2Y - \frac{3}{5},$$

then $k = 2$ and $e_2 = (2, 1), a_1 = \frac{1}{4}, e_1 = (0, 0), a_1 = \frac{-3}{5}$. The representation is then

$$\alpha = ((1, 2), (1, 4), (0, 0), (-3, 5)).$$

4. Let $S = \mathbf{Z}[X_1, X_2, X_3, X_4, X_5]$, that is $R = \mathbf{Z}$ and $r = 5$. Let

$$A = 5X_2X_3 + 7X_1^2,$$

then $k = 2$ and $e_2 = (0, 1, 1, 0, 0), a_2 = 5, e_1 = (2, 0, 0, 0, 0), a_1 = 7$. The representation is then

$$\alpha = ((0, 0, 1, 1, 0), 5, (0, 0, 0, 0, 2), 7).$$

Procedure names for exponent vector algorithms begin with '`EV`', for base coefficients arithmetic with '`RN`' (for rational numbers).

Bibliography (Books)

[Anderson, Fuller 1974] F. W. Anderson, K. R. Fuller, *Rings and categories of modules.* Springer, Berlin, 1974.

[Becker, Weispfenning 1992] T. Becker, V. Weispfenning, with H. Kredel, *Gröbner bases.* Forthcomming, Springer, New York, 1992.

[Bohro, Gabriel, Rentschler 1973] W. Bohro, P. Gabriel, R. Rentschler, *Primideale in Einhüllenden auflösbarer Lie-Algebren.* Lect. Notes Math. 357, 1973.

[Blyth 1986] T. S. Blyth, *Categories.* Longman, Harlow, 1986.

[Buchberger *et. al.* 1982] B. Buchberger, G. E. Collins, R, Loos (eds.), *Computer algebra, symbolic and algebraic computation.* Computing Supplement, Springer, Berlin, 1982/83.

[Cohn 1965] R. M. Cohn, *Difference Algebra.* Krieger Pub. Comp., Huntington, 1965; reprint Wiley & Sons, New York, 1980.

[Cohn 1971] P. M. Cohn, *Free rings and their relations.* London Math. Soc. Monographs 2, Academic Press, London, 1971.

[Cohn 1977] P. M. Cohn, *Skew field constructions.* London Math. Soc. Lect. Notes 27, Cambridge Univ. Press, Cambridge, 1977.

[Cohn 1981] P. M. Cohn, *Universal Algebra.* rev. ed., D. Reidel Pub. Comp., Dordrecht, 1981.

[Dixmier 1974] J. Dixmier, *Algèbres enveloppantes.* Gauthier-Villars, Paris, 1974.

[Garey, Johnson 1978] M. R. Garey, D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness.* H. Freeman, San Francisco, 1978.

[Goodearl, Warfield 1989] K. R. Goodearl, R. B. Warfield jr., *An introduction to non-commutative Noetherian rings.* London Math. Soc. Stud. Texts 16, Cambridge Univ. Press, Cambridge, 1989.

[Gröbner 1968/70] W. Gröbner, *Algebraische Geometrie I, II.* Bib. Inst., Mannheim, 1968, 1970.

[Hirschfeld, Wheeler 1975] J. Hirschfeld, W. H. Wheeler, *Forcing, arithmetic, division rings.* Lect. Notes Math. 454, 1975.

[Ihringer 1988] T. Ihringer, *Allgemeine Algebra.* Teubner, Stuttgart, 1988.

[Jacobson 1962] A. Jacobson, *Lie Algebras.* Interscience Publishers 1962, also Dover Publ., 1979.

[J. Symb. Comp. 1986-] B. Buchberger (ed.), *Journal of Symbolic Computation.* Academic Press, London, published since 1986.

[Kolchin 1973] E. R. Kolchin, *Differential algebra and algebraic groups.* Academic Press, London, 1973.

[Kunz 1980] E. Kunz, *Einführung in die kommutative Algebra und algebraische Geometrie.* F. Vieweg, Braunschweig, 1980.

[Manin 1991] Y. I. Manin, *Topics in Noncommutative Geometry.* M. B. Porter Lectures, Rice Univ., Princeton Univ. Press, Oxford, 1991.

[McConnell, Robson 1987] J. C. McConnell, J. C. Robson, *Noncommutative Noetherian Rings.* Wiley – Interscience, New York, 1987.

[Potthoff 1981] K. Potthoff, *Einführung in die Modelltheorie und ihre Anwendungen.* Wiss. Buchges., Darmstadt, 1981.

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

[Ritt 1950] J. F. Ritt, *Differential Algebra.* Amer. Math. Soc. Publ. No. 33, 1950.

[Robinson 1974] A. Robinson, *Introduction to model theory and to the metamathematics of algebra.* Elsevier Pub., Amsterdam, *2 ed.* 1974, *2 print.* 1986.

[V. d. Waerden 1971] B. L. van der Waerden, *Moderne Algebra I, II.* Springer Leipzig, 1937 and *Algebra I, II.* Springer, Heidelberg, 1971.

[Weispfenning 1990/91] V. Weispfenning, *Nicht kommutative Noethersche Ringe.* Lecturs, University of Passau, 1990/91.

[Wirth 1985] N. Wirth, *Programming in Modula-2.* Springer, Heidelberg, 1985.

[Zariski, Samuel 1958/60] O. Zariski, P. Samuel, *Commutative Algebra I, II.* reprint by Springer, Heidelberg, 1979.

Bibliography (Articles)

[Abellanas, Martinez 1975] L. Abellanas, L. Martinez Alonso, *A general setting for Casimir invariants.* J. Math. Phys., vol. 16, no. 8, pp 1580–1584, 1975.

[Apel 1988] J. Apel, *Gröbner basen in nicht kommutativen Algebren und ihre Anwendungen.* Dissertation, Leipzig, 1988.

[Apel, Klaus 1990] J. Apel, U. Klaus, *Implementational aspects for non-commutative domains.* Proc. IV. Int. Conf. Computer Algebra in Physical Research 1990, JINR Dubna, Moscow UdSSR, 1990, World Scientific, Singapore, pp 127–132, 1991.

[Apel, Klaus 1991] J. Apel, U. Klaus, *FELIX – An assistant for algebraists.* Proc. ISSAC '91, Bonn, July 1991, ACM Press, pp 382–389, 1991.

[Apel, Lassner 1988] J. Apel, W. Lassner, *An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras.* J. Symb. Comp., **6**, pp 361–370, 1988.

[Armbruster, Kredel 1986] D. Armbruster, H. Kredel, *Constructing universal unfoldings using Gröbner bases.* J. Symb. Comp., **2**, pp 383–388, 1986.

[Bacsich 1972] P. D. Bacsich, *Cofinal simplicity and algebraic closedness.* Algebra Univ., vol. 2, pp 345–360, 1972.

[Bacsich 1973] P. D. Bacsich, *Defining algebraic elements.* J. Symb. Logic, vol. 38, no. 1, pp 93–101, 1973.

[Bartol *et. al.* 1983] W. M. Bartol, *et. al.*, *Report on the programming language LOGLAN 82.* Polish Scientific Publications, Warsaw, 1984.

[Beck *et. al.* 1976] R. E. Beck, B. Kolman, I. N. Steward, *Computing the strucutre of a Lie algebra.* Proc. Computers in nonassociative rings and algebras, San Antonio, Jan. 1976, Academic Press, New York, pp 167–188, 1977.

[Bergman 1978] G. M. Bergman, *The diamond lemma for ring theory.* Adv. in Math. 29, pp 178–218, 1978.

[Becker 1990] T. Becker, *Standard bases and some computations in rings of power series.* J. Symb. Comp. **10**, pp 165–178, 1990.

[Becker 1991] T. Becker, *Standard bases in power series rings: uniqueness and superfluous critical pairs.* University of Passau, 1991.

[Böge *et. al.* 1986] W. Böge, R. Gebauer, H. Kredel. *Some examples for solving systems of algebraic equations by calculating Gröbner bases.* J. Symb. Comp. **1**, pp 83–98, 1986.

[Buchberger 1965] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Dissertation, University of Insbruck, 1965.

[Buchberger 1979] B. Buchberger, *A criterion for detecting unnecessary reductions in the construction of Gröbner bases.* Proc. EUROSAM '79, Marseille, Lect. Notes Comp. Sci. 72, pp 3–21, 1979.

[Buchberger 1985] B. Buchberger, *Gröbner Bases: an algorithmic method in polynomial ideal theory.* In: Progress, directions and open problems in multidimensional systems theory. (N.K.Bose ed.) Reidel Publ. Comp., pp 184–232, 1985.

[Clausen, Fortenbacher 1989] M. Clausen, A. Fortenbacher, *Efficient solution of linear diophantine equations.* J. Symb. Comp. **8**, pp 201–216, 1989.

[Collins, Loos 1980] G. E. Collins, R. Loos, *ALDES and SAC-2 now available.* ACM SIGSAM Bulletin Vol. 12, No. 2, p 19, 1980.

[Conatser, Huddleston 1976] C. W. Conatser, P. L. Huddleston,
Computation of Casimir invariants of Lie algebras. Proc. Computers in nonassociative rings and algebras, San Antonio, Jan. 1976, Academic Press, New York, pp 157–166, 1977.

[Dickson 1913] L. E. Dickson, *Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors.* Amer. J. Math. **35**, pp 413–426, 1913.

[Dixmier 1968/70] J. Dixmier, *Sur les algèbres de Weyl, II.* Bull. Soc. Math. France, 96, pp 209–242, 1968; Bull. Sc. Math. 2^e série, 94, pp 289–301, 1970.

[El From 1983] Y. El From, *Sur les algèbres de type résoluble.* Thèse de 3e cycle, Universite Pierre et Marie Curie, Paris 6, 1983.

[Furukawa *et. al.* 1986] A. Furukawa, T. Sasaki, H. Kobayashi, *Gröbner bases of a module over $K[x_1, \ldots, x_n]$ and polynomial solutions of a system of linear equations.* Proc. SYMSAC '86, Waterloo, Ontario, ACM Press, pp 222–224, 1986.

[Gao, Chou 1991] Xiao-Shan Gao, Shang-Ching Chou, *Computations with parametric equations.* Proc. ISSAC '91, Bonn, July 1991, ACM Press, pp 122–127, 1991.

[Galligo 1985] A. Galligo, *Some algorithmic questions on ideals of differential operators.* Proc. EUROCAL '85, Linz, 1985, Lect. Notes Comp. Sci. 204, pp 413–421, 1985.

[Gateva-Ivanova 1988] T. Gateva-Ivanova, *On the Noetherianity of some associative finitely presented algebras.* Preprint Univ. Sofia, 1988.

[Gebauer, Kredel 1983] R. Gebauer, H. Kredel, *Distributive polynomial system.* Several Technical Reports University of Heidelberg, 1983.

[Gebauer, Kredel 1984] R. Gebauer, H. Kredel, *Buchberger algorithm system.* Technical Report University of Heidelberg, 1984. (See also ACM SIGSAM Bulletin Vol. 18, No. 1, p 19.)

[Gianni 1987] P. Gianni, *Properties of Gröbner bases under specialization.* Proc. EUROCAL '87, Leipzig, 1987, Lect. Notes Comp. Sci. 378, pp 293–297, 1990.

[Huet 1980] G. Huet, *Confluent reductions: Abstract properties and applications to term rewriting systems.* J. ACM, **27**, pp 797–821, 1980.

[Jaffar, Lassez 1987] J. Jaffar, J.-L. Lassez, *Constraint Logic Programming.* Proc. 14th Annual ACM Symp. on Principles of Programming Languages, Munich, FRG, Jan. 1987, ACM, pp 111–119, 1987.

[Kapur, Madlener 1989] D. Kapur, K. Madlener, *A completion procedure for computing a canonical basis for a k-subalgebra.* Proc. Computers and Mathematics, Cambridge MA, 1989, Springer, New York, pp 1–11, 1990.

[Kandri-Rody, Weispfenning 1988] A. Kandri-Rody, V. Weispfenning, *Non-commutative Gröbner bases in algebras of solvable type.* J. Symb. Comp., **9**, pp 1–26, 1990. also available as: Technical Report University of Passau, MIP-8807, March 1988.

[Kredel 1988] H. Kredel, *From SAC-2 to Modula-2.* Proc. ISSAC '88, Rome 1988, Lect. Notes Comp. Sci. 358, pp 447–455, 1988.

[Kredel 1988a] H. Kredel, *Distributive polynomial interpreter system.* Technical Report University of Passau, 1988.

[Kredel, Weispfenning 1988] H. Kredel, V. Weispfenning, *Computing dimension and independent sets for polynomial ideals.* J. Symb. Comp., **6**, pp 231–248, 1988.

[Kredel 1990] H. Kredel, *MAS Modula-2 algebra system.* Proc. DISCO '90, Capri 1990, Lect. Notes Comp. Sci. 429, pp 270–271, 1990. Manuals and Technical Reports University of Passau, 1990.

[Kredel, Weispfenning 1990] H. Kredel, V. Weispfenning, *Parametric Gröbner bases for noncommutative Polynomials.* Proc. IV. Int. Conv. Computer Algebra in Physical Research 1990, JINR, Dubna, Moscow UdSSR, May 1990, World Scientific, Singapore, pp 236–244, 1991.

[Kredel 1990a] H. Kredel, *Computing in polynomial rings of solvable type.* Proc. IV. Int. Conv. Computer Algebra in Physical Research 1990, JINR, Dubna, Moscow UdSSR, May 1990, World Scientific, Singapore, pp 211–221, 1991.

[Kredel 1991] H. Kredel, *The MAS Specification Component.* Proc. PLILP '91, Passau, 1991, Lect. Notes Comp. Sci. 528, pp 39–50, 1991.

[Labonté 1990] G. Labonté, *An algorithm for the construction of matrix representations for finitely presented non-commutative algebras.* J. Symb. Comp. **9**, pp 27–38, 1990.

[Lassner 1985] W. Lassner, *An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras.* Proc. EUROCAL '85, Linz 1985, Lect. Notes Comp. Sci. 204, pp 99–115, 1985.

[Lesieur, Croisot 1963] L. Lesieur, R. Croisot, *Algèbre Noethériene non commutative.* Mémorial des sciences mathématiques, fasc. CLIV, Gauthier-Villars, Paris, 1963.

[Lesieur 1978] L. Lesieur, *Conditions Noéthérienes dans l'anneau de polynomes de Ore* $A[X, \sigma, \delta]$. Séminaire d'algèbre P. Dubreil, Paris, Lect. Notes Math. 641, pp 220–234, 1978.

[Lorenz 1981] M. Lorenz, *Completely prime ideals in Ore extensions.* Comm. Algebra, vol. 9(11), pp 1227–1232, 1981.

[Malcev 1937] A. Malcev, *On the immersion of an algebraic ring into a field.* Math. Annalen, **113**, pp 686–691, 1937.

[Mora 1985] T. Mora, *Gröbner bases for non-commutative polynomial rings.* Proc. AAECE-3, Grenoble 1985, Lect. Notes Comp. Sci. 229, pp 353–362, 1985.

[Mora 1986] T. Mora, *Standard bases and non-Noetherianity: Non-commutative polynomial rings.* Proc. AAECE-4, Karlsruhe 1986, Lect. Notes Comp. Sci. 307, pp 98–109, 1986.

[Mora 1988] T. Mora, *Gröbner Bases in non-commutative algebras.* Proc. ISSAC '88, Rome, July 1988, Lect. Notes Comp. Sci. 358, pp 150–161, 1988.

[Möller, Mora 1986] H. M. Möller, T. Mora, *New constructive methods in classical ideal theory.* J. of Algebra, **100**, pp 138–178, 1986.

[Noether, Schmeidler 1920] E. Noether, W. Schmeidler, *Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrücken.* Math. Zeitschr., **8**, pp 1–35, 1920.

[Ore 1931] O. Ore, *Linear equations in non-commutative fields.* Ann. of Math. 32, pp 463–477, 1931.

[Ore 1933] O. Ore, *Theory of non-commutative polynomials.* Ann. of Math. 34, pp 480–508, 1933.

[Patera *et. al.* 1976] J. Patera, R. T. Sharp, P. Winternitz, H. Zassenhaus, *Invariants of real low dimnension Lie algebras.* J. Math. Phys., vol. 17, no. 6, pp 986–993, 1976.

[Pankrat'ev 1989] E. V. Pankrat'ev, *Computations in differential and difference modules.* Acta Appl. Math. **16**, pp 167–189, 1989.

[Petermann, Apel 1988] J. Apel, U. Petermann, *A program for algebraic computations in quotient skew fields of enveloping algebras of Lie algebras.* Karl-Marx-University Leipzig, preprint 1988.

[Philipp 1991] J. Philipp, *Syzygien Berechnung im Computer Algebra System MAS.* Diploma thesis, University of Passau, 1991.

[Robbiano 1985] L. Robbiano, *Term orderings on the polynomial ring.* Proc. EUROCAL '85, Linz, 1985, Lect. Notes Comp. Sci. 204, pp 513–517, 1985.

[Robbiano, Sweedler 1988] L. Robbiano, M. Sweedler, *Subalgebra bases.* Proc. Commutative Algebra, Salvador, 1988, Lect. Notes Math. 1430, pp 61–87, 1988.

[Robinson 1971] A. Robinson, *On the notion of algebraic closedness for non-commutative groups and fields.* J. symb. Logic 36, pp 441–444, 1971.

[Schönfeld 1991] E. Schönfeld, *Parametrische Gröbner Basen im Computer Algebra System ALDES/SAC-2.* Diploma thesis, University of Passau, 1991.

[Schwartz 1988] N. Schwartz, *Stability of Gröbner bases.* J. pure and appl. Algebra, **53**, pp 171–186, 1988.

[Shannon, Sweedler 1988] D. Shannon, M. Sweedler, *Using Gröbner bases to determine algebra membership, split surjective algebra homomorphisms determine birational equivalence.* J. Symb. Comp., **6**, pp 267–273, 1988.

[Simmons 1972] H. Simmons, *Existentially closed structures.* J. Symb. Logic, vol. 37, no. 2, pp 293–310, 1972.

[Sigurdsson 1984] G. Sigurdson, *Differential operator rings whose prime factors have bounded Goldie dimension.* Arch. Math., vol. 42, pp 348–353, 1984.

[Sit 1991] W. Y. Sit, *A theory for parametric linear systems.* Proc. ISSAC '91, Bonn, July, 1991, ACM Press, pp 112–121, 1991.

[Smith 1990] S. P. Smith, *A class of algebras similar to the enveloping algebra of* $sl(2)$. Trans. AMS. vol. 322, no. 1, pp 285–314, 1990.

[Stafford 1978] J. T. Stafford, *Module structure of Weyl algebras.* J. London Math. Soc. (2), 18, pp 429–442, 1978.

[Stokes 1989] T. Stokes, *Gröbner bases in exterior algebra.* preprint University of Tasmania, 1989.

[Weispfenning 1977] V. Weispfenning, *Nullstellensätze – A model theoretic framework.* Zeitschr. f. math. Logik und Grundlagen d. Math., Bd. 23, pp 539–545, 1977.

[Weispfenning 1983] V. Weispfenning, *Aspects of quantifier elimination in algebra.* In: Universal Algebra and its Links with Logic, Algebra, Combinatorics and Computer Science, P. Burmeister et. al. (eds.), Proc. "25. Arbeitstagung über Allgemeine Algebra", Darmstadt, 1983, Heldermann Verlag, pp 85–105, 1984.

[Weispfenning 1987] V. Weispfenning,
Constructing universal Gröbner bases. Proc. AAECC-5, Menorca 1987, Lect. Notes Comp. Sci. 356, pp 195–201, 1987.

[Weispfenning 1987] V. Weispfenning, *Admissible orders and linear forms.*
ACM SIGSAM Bull. **21**, pp 16–18, 1987.

[Weispfenning 1990] V. Weispfenning, *Comprehensive Gröbner bases.* preprint in: Technical Report University of Passau, MIP-9003, 1990.

[Winkler *et. al.* 1985] F. Winkler, B. Buchberger, F. Lichtenberger, H. Rolletschek, *An algorithm for constructing canonical bases of polynomial ideals.* ACM, TOMS **11**, pp 66–78, 1985.

[Zacharias 1978] G. Zacharias, *Generalized Gröbner bases in commutative polynomial rings.* Bachelor thesis, MIT, Dep. of Comp. Sci., 1978.

[Zassenhaus 1976] H. Zassenhaus, *On the invariants of a Lie group, I.* Proc. Computers in nonassociative rings and algebras, San Antonio, Jan. 1976, Academic Press, New York, pp 139–156, 1977.

List of Special Notations

In addition to TEX's menagerie of mathematical symbols we use the following notation. The numbers refer to the page number where the notation is defined or first used.

$\mathbf{N}$	natural numbers, including 0 22
$\mathbf{Z}$	integral numbers, integers, 22
$\mathbf{Q}$	rational numbers, 30
$\mathbf{R}$, $\mathbf{P}$	rings, 23
$\mathbf{K}$, $\mathbf{L}$, $\mathbf{E}$	(skew) fields, 30
$\mathcal{M}$	model classes, 216
$\mathcal{T}$	theories, 216
$\mathcal{V}$	varieties, 233
$\|A\|$	cardinality of the set A, 22
$A \times B$	cartesian product of the sets A and B, 22
$\mathrm{char}(R)$	the characteristic of R,
A/I	residue class ring of a ring A modulo an ideal I, 100
$Q(R)$	quotient ring or quotient field of a ring R (if it exists), 210
$R\{X_1, \ldots, X_n; Q, Q'\}$	solvable polynomial ring over the ring R in the variables $X_1, \ldots, X_n$, $n \geq 0$ with commutator relations Q between the $X_1, \ldots, X_n$ and with commutator relations Q' between the $X_1, \ldots, X_n$ and the ring R, 33
a^{-1}	the inverse of a, 30
$\mathrm{abs}(a)$	the absolute value of a,

$\mathrm{lcm}(a, b)$	the least common multiple of a and b,
$T(g)$	the set of terms of the polynomial g, 31
$\mathrm{mult}(V)$	the set of multiples of the terms in V, 32
$\mathrm{coeff}(t, g)$	the coefficient of the term t in the polynomial g, 32
$\mathrm{HT}(g)$	the head term of the polynomial g, 32
$\mathrm{HM}(g)$	the head monomial of the polynomial g, 32
$\mathrm{HC}(g)$	the head coefficient of the polynomial g, 32
$\longrightarrow$	a reduction relation, 66
$\downarrow$	reduce to a common element, 66
$\mathrm{LSP}(f, g)$	the left S-polynomial of the polynomials f and g, 77
$\mathrm{RSP}(f, g)$	the right S-polynomial of the polynomials f and g, 90
$\mathrm{LNF}(g, F)$	the left normal form of the polynomial g with respect to the polynomials F, 74
$\mathrm{RNF}(g, F)$	the right normal form of the polynomial g with respect to the polynomials F, 89
$\mathrm{ideal}(F)$	the ideal generated by F, 24
$\mathrm{module}(N)$	the submodule generated by N, 114
$\mathrm{subalg}(F)$	the subalgebra generated by F, 118
$\mathrm{rad}(I)$	the prime radical of I, 28
$\text{c-rad}(I)$	the complete prime radical of I, 28
$\mathrm{spec}(R)$	the prime spectrum of R, 189
$\text{c-spec}(R)$	the complete prime spectrum of R, 189
$\mathrm{cen}(R)$	the center of R, 59
$[a, b]$	the commutator $ab - ba$ of some ring elements a, b, 59
`Tm`	the set of terms of some language,
`Fm`	the set of first order formulas of some language,

`PFm`	the set of first order prime formulas of some language,
place_Q	a formula, denoting a place condition with respect to commutator relations Q, 224
χ_{FQ}	a formula, denoting a consistence condition with respect to a set of polynomials F and commutator relations Q, 228
$A \sqsubseteq B$	A is a L-substructure of B, 22
$A \prec B$	A is an elementary L-substructure of B, 218
$A \models \varphi$	the formular φ holds in A, 23
$\text{Mod}(\mathcal{T})$	the class of models of a theory $\mathcal{T}$, 216
$\text{EC}(\mathcal{M})$	the class of existentially complete structures of a class of structures $\mathcal{M}$, 219
$\text{Thy}(\mathcal{M})$	the theory of a class of models $\mathcal{M}$, 216
true	the value true, 22
false	the value false, 22
$\text{Mor}_{\mathbf{C}}(X, Y)$	the set of morphisms from X to Y, where X, Y are objects of some category $\mathbf{C}$, 214

Author Index

Subject Index

C

D

E

F

G

H

I

U

V

W

Z