J. Symbolic Computation (1990) **9**, 1–26

Non-commutative Gröbner Bases in Algebras of Solvable Type

A. KANDRI-RODY* AND V. WEISPFENNING

* *Département des Mathématiques, Université Cadi Ayyad, Marrakech, Morocco*

Lehrstuhl für Mathematik, Universität Passau, D-8390 Passau, FRG

(*Received 15 October 1986*)

We introduce a class of non-commutative polynomial rings over fields intermediate between commutative polynomial rings and general non-commutative polynomial rings. This class of *solvable polynomial rings* includes many rings arising naturally in mathematics and physics, such as iterated Ore extensions of fields and enveloping algebras of finite dimensional Lie algebras. We present algorithms that compute Gröbner bases of one- and two-sided ideals in solvable polynomial rings. They extend Buchberger's algorithm (see Buchberger, 1985) in the commutative case and Apel and Lassner's algorithms (see Apel & Lassner, 1988) for *one-sided* ideals in enveloping algebras of Lie algebras, as well as the results on *one-sided* standard bases in Weyl algebras, sketched in Galligo (1985). We show that reduced one- and two-sided Gröbner bases in solvable polynomial rings are unique, and we solve the word problem and the ideal membership problem for algebras of solvable type, in particular in Clifford algebras. Further applications include the computation of elimination ideals, computing in residue modules and the computation of generators for modules of syzygies.

Introduction

The method of Gröbner basis calculations introduced by Buchberger has turned out to be an invaluable tool in the algorithmic theory of commutative polynomial rings (see Buchberger, 1985). For non-commutative polynomial rings (i.e. finitely generated free associative algebras) R over a field K the situation is much less satisfying, as the analysis in Bergmann (1978) and Mora (1986) shows. Since Dickson's lemma does not hold, R is not Noetherian and finite Gröbner bases may not exist for finitely generated ideals. In fact, we show in section 6.3 that the membership problem for two-sided ideals in general non-commutative polynomial rings over fields is algorithmically unsolvable. Moreover, the unsolvability holds for a specific ideal with seven explicitly described generators in $\mathbb{Q}\langle X_1, X_2\rangle$.

In this paper, we treat the problem of finding Gröbner bases in polynomial rings R that are intermediate between the commutative and the most general non-commutative case. These rings R will be described axiomatically as follows: the elements of R are commutative polynomials over a field K, but the multiplication $*$ may be non-commutative. The decisive restriction on $*$ is that the difference between $f*g$ and a suitable scalar multiple of the corresponding commutative product $f \cdot g$ is smaller than $f \cdot g$ in the sense of an arbitrary but fixed admissible term order on R. This can be guaranteed by a few, simple axioms on $*$.

The class of polynomial rings of solvable type introduced in this way is quite comprehensive: It includes commutative polynomial rings; iterated Ore extensions of the

0747–7171/90/010001+26 $03.00/0

ground field K; quotients of a general non-commutative polynomial ring over K by fairly general commutation relations; and universal enveloping algebras of finite dimensional Lie algebras over K, in particular the Weyl algebras arising in quantum physics.

Reduction relations and one-sided Gröbner bases in a solvable polynomial ring are defined in a similar way as for commutative polynomial rings. The verification of their construction and characterisation algorithms is, however, more involved and requires many more Noetherian inductions on the admissible-term order in question.

An appropriate definition of a two-sided Gröbner basis, suitable for solving the ideal membership problem in solvable polynomial rings, is far more subtle. It turns out that an ideal basis can be both a left and right Gröbner basis without being a two-sided Gröbner basis. Nevertheless, we are able to construct and characterise two-sided Gröbner bases algorithmically.

As in the commutative case, left, right, and two-sided reduced Gröbner bases are uniquely determined by the left/right/two-sided ideal they generate. A central fact for the proof is that the concept of irreducibility is left/right symmetric, even though left and right reductions may be quite different.

The main application of the Gröbner basis technique is the algorithmic solution of the ideal membership problem for one- and two-sided ideals in solvable polynomial rings. As a side product, we find that all solvable polynomial rings are left and right Noetherian, a fact proved, by a different method based on Lesieur (1978), in El From (1983) for a special case. This, in turn, has the consequence that the word problem and the ideal membership problem is solvable in arbitrary finitely generated K-algebras of the solvable type, i.e. in quotients of a solvable polynomial ring by a two-sided ideal. These include all Clifford algebras and hence all Grassmann algebras.

Further applications include the computation of elimination ideals, computing in residue spaces of a solvable polynomial ring by a one-sided ideal—in particular an extension of Buchberger's criterion for finite dimensionality—and the computation of generating sets for modules of syzygies. The plan of the paper is as follows:

Section 1, *Solvable Polynomial Rings*, introduces polynomial rings of solvable type, their axiomatic definition, basic properties, and examples of such rings.

Section 2, *Algorithms*, presents the main algorithms of our study: the computation of products of polynomials, of left, right and two-sided Gröbner bases, as well as of reduced Gröbner bases from a given ideal basis.

Section 3, *Left Reduction and Left Gröbner Bases*, discusses left reduction, left S-polynomials and left Gröbner bases, together with their applications to elimination ideals, computing in residue spaces and to modules of syzygies.

Section 4, *Right and Reduced Gröbner Bases*, treats right Gröbner bases and their relation to their left-hand counterparts, and in addition reduced right and left Gröbner bases, their existence and uniqueness.

Section 5, *Two-sided Gröbner Bases*, is devoted to various equivalent characterisations and the construction of two-sided Gröbner bases and reduced two-sided Gröbner bases.

Section 6, *The Word Problem in Algebras of Solvable Type*, applies Gröbner bases to the algorithmic solution of the word problem and ideal membership problem in algebras of solvable type. Besides, it contains a uniform proof for the unsolvability of the ideal membership problem in general non-commutative polynomial rings over fields and the exponential space hardness of this problem for commutative polynomial rings, due to Mayr & Meyer (1982). We illustrate the method by a sample computation in the Aldes/SAC-2 implementation developed by Kredel.

Section 7, *Concluding Remarks*, summarises our results and indicates some problems and directions for further research.

The starting point for our study was El From's thesis on solvable polynomial rings that was kindly supplied by the author. Based on the definition of these rings in El From (1983), which correspond to the case of a pure lexicographical term order on R in the axiomatic framework, we developed the theory of Gröbner bases for these rings in summer 1986. After submission of this version in fall 1986, we learnt of the work of Apel and Lassner (1988) on Gröbner bases for *one-sided ideals* in enveloping algebras for finite-dimensional Lie algebras. Moreover, we realised the connection to the results on *one-sided* standard bases in Weyl algebras sketched in Galligo (1985). In spring 1987, we were able to incorporate the case of enveloping algebras (corresponding to a degree-compatible admissible-term order on R) into the present axiomatic framework, without any essential changes in sections 2–7. The algorithms have been implemented in the *Aldes/SAC-2 Distributive Polynomial System* of Gebauer & Kredel (1983), by Kredel at the University of Passau. We are indebted to H. Kredel for providing us with the sample computation used in section 6.

1. Solvable Polynomial Rings

Let K be a (commutative) field and let $R = K[X_1, \ldots, X_n]$ be the (commutative) polynomial ring in the indeterminates X_i over K. We let T denote the set of terms (power-products of the X_i) in R. For any polynomial $f \in R$, $T(f)$ denotes the set of terms occurring in f with non-zero coefficient.

An admissible order on T is a linear order "$<$" on T which turns $(T, 1, \ , <)$ into an ordered multiplicative monoid with smallest element 1. Any admissible order on T extends the divisibility relation on T; moreover, it induces in a natural way a linear quasiorder "$<$" on $R : f < g$ iff there exists $t \in T(g) \backslash T(f)$ such that for all $t' \in T$ with $t' > t$, $t' \in T(f)$ iff $t' \in T(g)$. Both the admissible order on T and the induced quasiorder on R are *well-founded* (*Noetherian*), i.e. admit no infinite, strictly decreasing chain. This is a consequence of the following fundamental lemma that is due to Dickson (1913), and has been rediscovered independently by several authors.

1.1. Dickson's Lemma. *For every infinite sequence (t_i) of terms there exists j such that for all $k > j$ there exists $i \leqslant j$ such that t_i, divides t_k.*

For fixed admissible order $<$ on T and $f \in R$, we let HT(f), HC(f), HM(f) (the highest term, highest coefficient, highest monomial of (f) denote the highest term t wrt $<$ in T(f), the coefficient a of t in f and the monomial $a \cdot t$ of f, respectively. $T(X_i, \ldots, X_j) = T \cap K[X_i, \ldots, X_j]$ is the set of all terms with indeterminates in $\{X_i, \ldots, X_j\}$ for $1 \leqslant i \leqslant j \leqslant n$.

The main objects of our study, *non-commutative polynomial rings of solvable type*, will be obtained from R by introducing a new multiplication on R subject to certain conditions: Fix an admissible order $<$ on T, and let $* : R^2 \rightarrow R$ be a new binary operation on R. Then we call (R, $*$) a polynomial ring of solvable type (or solvable polynomial ring for short), if the operation $*$ satisfies the following axioms:

Axioms 1.2.

(1) $(\mathrm{R}, 0, 1, +, -, *)$ *is an associative ring with* 1.

(2) *For all* $a, b \in \mathrm{K}$, $1 \leqslant h \leqslant i \leqslant j \leqslant k \leqslant n$, $t \in \mathrm{T}(X_i, \ldots, X_j)$,

(*i*) $a * bt = bt * a = abt$,

(*ii*) $X_h * bt = bX_h t$,

(*iii*) $bt * X_k = btX_k$.

(3) *For all* $1 \leqslant i \leqslant j \leqslant n$ *there exist* $0 \neq c_{ij} \in \mathrm{K}$ *and* $p_{ij} \in \mathrm{R}$ *such that* $X_j * X_i = c_{ij} X_i X_j + p_{ij}$ *and* $p_{ij} < X_i X_j$.

Any admissible order satisfying condition (3) will be called *$*$-compatible*. We will use the notation $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ for solvable polynomial rings $(\mathrm{R}, *)$ with $\mathrm{R} = \mathrm{K}[X_1, \ldots, X_n]$. $*$ will always denote the new (non-commutative) multiplication and $\cdot$ the commutative multiplication of $\mathrm{K}[X_1, \ldots, X_n]$. So $\mathrm{K}\{X_1, \ldots, X_n\}$ is an associative, but in general non-commutative extension ring of K, whose elements are "commutative polynomials".

Our first goal is to extend conditions (2) and (3) to arbitrary polynomials in R.

Lemma 1.3. *Let* $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ *be a solvable polynomial ring, let* $1 \leqslant i \leqslant n$, *and let* $f \in \mathrm{K}[X_1, \ldots, X_i]$, $g \in \mathrm{K}[X_i, \ldots, X_n)$. *Then* $f * g = f \cdot g$.

Proof. By Noetherian induction on (f, g) with respect to the lexicographical quasiorder on R^2 induced by a $*$-compatible admissible order $<$ on T: Let $g = bt + g'$, where $bt = \mathrm{HM}(g)$. If $f = a \in \mathrm{K}$, $g = b$, then $f * g = ab = f \cdot g$ by axiom 1.2 (2, i); for arbitrary g, we get by 1.2 (2, ii) and the induction assumption,

$$f * g = a * bt + a * g' = abt + ag' = ag = f \cdot g.$$

Next, let $f = as + f'$ with $as = \mathrm{HM}(f)$, and let $s = s'X_h$, where X_h, $h \leqslant i$ is the variable with highest subscript in s. Then, by axiom 1.2 (2, ii, iii) and induction assumption,

$$f * g = as * bt + f' * bt + as * g' + f' * g',$$

where (f', bt), (as, g'), $(f', g') < (f, g)$, and

$$as * bt = (as' * X_h) * bt = as' * (X_h * bt) = as' * bX_h t = abs'X_h t = as \cdot bt.$$

Consequently,

$$f * g = as \cdot bt + f' \cdot bt + as \cdot g' + f' \cdot g' = (as + f') \cdot (bt + g') = f \cdot g.$$

Lemma 1.4. *Let* $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ *be a solvable polynomial ring, let* $<$ *be a $*$-compatible admissible order on* R, *and let* $f, g \in \mathrm{R}$. *Then there exists an* $h \in \mathrm{R}$ *such that* $f * g = c \cdot f \cdot g + h$ *and* $h < f \cdot g$. *Moreover, c and h are uniquely determined by f and g.* Notation: $\mathrm{c} = \mathrm{fctr(f, g)}$.

Proof. *Uniqueness* is obvious. *Existence* is proved by Noetherian induction on $f \cdot g$ with respect to $<$: If $f = a \in \mathrm{K}$, then by lemma 1.3, $f * g = f \cdot g = f \cdot g + 0$; similarly for $g = b \in \mathrm{K}$. Next, let $f = as + f'$, $g = bt + g'$ with $as = \mathrm{HM}(f)$, $bt = \mathrm{HM}(g)$. Then by induction assumption,

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

where $0 \neq d_i \in \mathrm{K}$ and $k \in \mathrm{R}$, $k < s \cdot t$. So it suffices to show that the following holds.

CLAIM. *$as * b_t = d \cdot as \cdot bt + k'$ with $0 \neq d \in \mathrm{K}$, $k' \in \mathrm{R}$, $k' < s \cdot t$.*

If for some $1 \leqslant i \leqslant n$, $s \in \mathrm{T}(X_1, \ldots, X_i)$, $t \in \mathrm{T}(X_i, \ldots, X_n)$, then by lemma 1.3, $as * bt = as \cdot bt = 1 \cdot as \cdot bt + 0$. So, we may assume that $s \in \mathrm{T}(X_h, \ldots, X_j)$, $t \in \mathrm{T}(X_i, \ldots, X_k)$, where h, i are taken maximal and j, k minimal and $1 \leqslant h \leqslant j \leqslant n$, $1 \leqslant i \leqslant k \leqslant n$, $i < j$.

CASE 1. $h \leqslant i$. Then, we write $s = X_h s' = X_h * s'$ with $s' < s$, and by induction assumption on $as' \cdot bt$, we get

$$\begin{aligned} as * bt &= X_h * as' * bt = X_h * (d \cdot as' \cdot bt + k'') \\ &= dabX_h s't + X_h * k'' = d \cdot as \cdot bt + d'X_h \cdot k'' + k''' \end{aligned}$$

with $k'' < s' \cdot t < s \cdot t$, $0 \neq d$, $d' \in \mathrm{K}$, $k''' < X_h \cdot k'' < X_h \cdot s' \cdot t = s \cdot t$.

CASE 2. $j \leqslant i$. This is handled similarly.

CASE 3. $i < h$ and $k < j$. Then we write $s = s''X_j$, $t = X_i t''$ with $s'' \in \mathrm{T}(X_h, \ldots, X_j)$, $t'' \in \mathrm{T}(X_i, \ldots, X_k)$. By axiom 1.2 (2) and (3), we obtain

$$\begin{aligned} as * bt &= as'' * X_j * X_i * bt'' = as'' * (c_{ij} X_i X_j + p_{ij}) * bt'' \\ &= as'' * c_{ij} X_i * X_j * bt'' + as'' * p_{ij} * bt'', \end{aligned} \tag{+}$$

where $0 \neq c_{ij} \in \mathrm{K}$, $p_{ij} \in \mathrm{R}$, $p_{ij} < X_i X_j$. The second summand of (+) is handled by induction assumption.

Since $s'' \cdot X_i < s'' \cdot X_j X_i \leqslant s \cdot t$ and $X_j \cdot t'' < X_j X_i t'' \leqslant s \cdot t$, we can also apply induction assumption to the first summand of (+), and obtain:

$$(as'' * c_{ij} X_i) * (X_j * bt'') = (d' a c_{ij} X_i s'' + r) * (d'' bt'' X_j + r'), \tag{++}$$

with $0 \neq d$, $d' \in \mathrm{K}$, $r < s'' X_i$, $r' < X_j t''$.

Using axiom 1.2 (2) and the hypothesis of case 3, (++) equals

$$X_i * (d' a c_{ij} s'' * d'' bt'') * X_j + d' a c_{ij} X_i s'' * r' + r * d'' bt'' X_j + r * r'. \tag{+++}$$

Since $X_i s'' r' < X_i s'' X_j t'' = s \cdot t$, $rt'' X_j < s'' X_i t'' X_j = s \cdot t$ and $r \cdot r'' < s'' X_i X_j t'' = s \cdot t$, the last three summands of (+++) can be written as polynomials $< s \cdot t$ by the induction assumption. For the middle product of the first summand, we have $s'' \cdot t'' < s \cdot t$, and so again by the induction assumption, the first summand of (+++) equals

$$X_i * (d''' d' d'' c_{ij} abs'' t'') * X_j + X_i * r''' * X_j, \tag{++++}$$

with $0 \neq d''' \in \mathrm{K}$, $r''' \in \mathrm{R}$, $r''' < s'' \cdot t''$.

By the hypothesis of case 3, $s'' \cdot t'' \in \mathrm{T}(X_i, \ldots, X_j)$, and so by axiom 1.2 (2), the first summand of (++++) equals

$$d''' d' d'' c_{ij} ab X_i s'' t'' X_j = (d''' d' d'' c_{ij}) \cdot (as) \cdot (bt).$$

Finally, the second summand of (++++) is handled by twofold application of the induction assumption, yielding a polynomial $< s \cdot t$.

This completes the proof of the claim and hence of the lemma.

The proof of lemma 1.4 provides in fact an algorithm (relative to the admissible order $<$) constructing the element c and the polynomial h such that $f * g = c \cdot f \cdot g + h$. An explicit description of the algorithm PRODUCT is presented in section 2. Its partial correctness and termination follows readily from the proof of lemma 1.4. As a corollary we note the following.

LEMMA 1.5. *Let* $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ *be a solvable polynomial ring, let* $<$ *be a* $*$*-compatible, admissible order on* T, *and let* $f, g \in \mathrm{R}$. *Then, the following hold:*

(1) $\mathrm{HT}(f * g) = \mathrm{HT}(f) \cdot \mathrm{HT}(g)$ and $\mathrm{HM}(f * g) = \mathbf{fctr}(f, g) \cdot \mathrm{HM}(f) \cdot \mathrm{HM}(g)$;
(2) $\mathrm{HT}(f * g) = \mathrm{HT}(g * f) = \mathrm{HT}(f \cdot g)$;
(3) *For* $h \in \mathrm{R}$, $\mathrm{HT}(f) < \mathrm{HT}(g)$ implies $\mathrm{HT}(f * h) < \mathrm{HT}(g * h)$ *and* $\mathrm{HT}(h * f) < \mathrm{HT}(h * g)$.

PROOF.
(1) By lemma 1.4, $f * g = c \cdot f \cdot g + h$ with $h < f \cdot g$, $c = \mathbf{fctr}(f, g)$. So

$$\mathrm{HT}(f * g) = \mathrm{HT}(c \cdot f \cdot g) = \mathrm{HT}(f \cdot g) = \mathrm{HT}(f) \cdot \mathrm{HT}(g)$$

and $\mathrm{HM}(f * g) = \mathrm{HM}(c \cdot f \cdot g)$.
(2) This is immediate from (1).
(3) $\mathrm{HT}(f) < \mathrm{HT}(g)$ implies by (1) $\mathrm{HT}(\mathrm{f} * h) = \mathrm{HT}(f) \cdot \mathrm{HT}(h) < \mathrm{HT}(g) \cdot \mathrm{HT}(h) = \mathrm{HT}(g * h)$; similar for $\mathrm{HT}(h * f) < \mathrm{HT}(h * g)$.

In section 3, we are going to use the *division relation* s div t for terms $s, t \in \mathrm{T} \subseteq \mathrm{R}$. This relation is always taken *in the sense of the commutative multiplication* $\cdot$ on R. The same applies to the *quotient* $t//s$ (provided s div t) and the *least common multiple* $\mathrm{lcm}(s, t)$ of s and t.

For the remainder of this section, we will be concerned with *examples of solvable polynomial rings* and some systematic constructions that lead to such rings.

To begin with, we characterise solvable polynomial rings R, where the $*$-admissible order is pure lexicographic and $p_{ij} < X_j$, $c_{ij} = 1$ as iterated Ore extensions of the ground field K. Our arguments are based on ideas in El From (1983).

Let R be an associative ring with 1, let δ be a derivation on R and let $\mathrm{R}[X, \delta]$ be the ring of non-commutative polynomials $f(X) = \Sigma_i a_i X_i$ $(a_i \in \mathrm{R})$ with multiplication $*$ defined by $X * a = aX + \delta(a)$ for $a \in \mathrm{R}$. Then $\mathrm{R}[X, \delta]$ is called an Ore extension of R [see Ore, 1933; El From, 1983]. Whenever R is a K-algebra and δ is a K-derivation (i.e. $\delta(a) = 0$ for $a \in \mathrm{K}$), then $\mathrm{R}[X, \delta]$ is also a K-algebra. We refer to the lexicographical order on T with $X_1 < \ldots < X_n$ as the *pure lexicographical order*. If $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ is a solvable polynomial ring with respect to the pure lexicographical order, and if in lemma 1.2 (3), $c_{ij} = 1$ and $p_{ij} < X_j$, we say R is *solvable of strictly lexicographical type.*

THEOREM 1.6. *Let* K *be a field.*
(1) *If* R *is obtained from* K *by* n *successive Ore extensions introducing the indeterminates* $X_1, \ldots, X_n$ *and using only* K*-derivations, then* $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ *is solvable of strictly lexicographical type.*
(2) *Let* $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ *be a solvable polynomial ring of strictly lexicographical type. Then* R *can be obtained from* K *by* n *successive Ore extensions introducing the indeterminates* $X_1, \ldots, X_n$ *and using only* K*-derivations.*

PROOF.

(1) By induction on n. The case $n=1$ is trivial. For $n>1$. Let $R=R'[X_n, \delta_n]$, where δ_n is a K-derivation on R′ and R′ is obtained by $(n-1)$ successive Ore extensions of K using only K-derivations.

Then, by the induction assumption, $R'=K\{X_1, \ldots, X_{n-1}\}$ is solvable of strictly lexicographical type. We have to verify axioms 1.2 for R: (1) and (2) are obvious, since δ_n is a K-derivation. It suffices to consider (3) for $1 \leqslant i<j=n$: $X_n * X_i = X_i X_n + \delta_n(X_i)$, where $\delta_n(X_i) \in R'$, and so $\delta_n(X_i) < X_n$.

(2) By induction on n. The case $n=1$ is again trivial. For $n>1$, since for $1 \leqslant i<j<n$, $p_{ij} < X_j$, p_{ij} is an element of $K[X_1, \ldots, X_{j-1}]$. So $R'=K\{X_1, \ldots, X_{n-1}\}$ is also a solvable polynomial ring of strictly lexicographical type. We define an operation $\delta\colon R' \to R'$ by $\delta(f)=X_n * f - f * X_n = X_n * f - f \cdot X_n$. (Notice that by lemma 1.4 we have $\delta(f) < X_n$, and so $\delta(f) \in R'$.) It is straightforward to verify that δ is a K-derivation on R′. Moreover, for $f \in R$, $X_n * f = f \cdot X_n + \delta(f)$, and so $R=R'[X_n, \delta]$. The claim follows now from the induction assumption applied to R′.

Next, we construct solvable polynomial rings as quotients of non-commutative polynomial rings.

For any field K, we let $P=K\langle X_1, \ldots, X_n\rangle$ denote the ring of polynomials in non-commuting indeterminates $X_1, \ldots, X_n$ that commute with the elements of K, i.e. the free associative algebra over K generated by $\{X_1, \ldots, X_n\}$. So each $f \in P$ is a sum of monomials of the form aw, where $0 \neq a \in K$ and w is a word in $X_1, \ldots, X_n$. Fix an admissible order $<$ on the set T of commutative terms in $X_1, \ldots, X_n$. A *commutation system* for (P, $<$) is a family Q of polynomials in P of the form $Q=\{q_{ij}: 1 \leqslant i<j \leqslant n\}$, where each q_{ij} is of the form $q_{ij}=X_j X_i - c_{ij} X_i X_j - p_{ij}$, where $0 \neq c_{ij} \in K$ and p_{ij} are commutative polynomials in $K[X_1, \ldots, X_n]$ and $p_{ij} < X_i X_j$. We call c_{ij} (p_{ij}) the *commutator constants* (*commutator polynomials*) of the system Q. I(Q) denotes the two-sided ideal generated by Q in P. We need the following hypothesis on Q:

(H) I(Q) contains no non-zero commutative polynomial.

THEOREM 1.7. *Let Q be a commutation system for* (P, $<$), *let* $R=P/I(Q)$ *and denote the residue class of* X_i *mod* I(Q) *by* x_i. *Then* $R=K\langle x_1, \ldots, x_n\rangle$ *is isomorphic to a solvable polynomial ring* $R'=K\{Y_1, \ldots, Y_n\}$ *with respect to* $<$ *and the multiplication* $*$ *of* R′ *under an isomorphism* ρ *fixing* K *pointwise and mapping* x_i *onto* Y_i, *iff* Q *satisfies hypothesis* (H).

PROOF. "$\Rightarrow$": Let $\rho\colon R \to R'$ be the isomorphism above, and let $f(X_1, \ldots, X_n)$ be a non-zero commutative polynomial in P. Then $f(Y_1, \ldots, Y_n) \neq 0$, and so $f(\mathbf{x})=\rho^{-1}(f(\mathbf{Y})) \neq 0$, and so $f(\mathbf{X})$ is not in I(Q). "$\Leftarrow$": By hypothesis (H), $R'=K[Y_1, \ldots, Y_n]$ embeds into R via $Y_i \mapsto x_i$ as K-vector space. Denote the multiplication of R by $*$ and the commutative multiplication of $K[x_1, \ldots, x_n]$ by $\cdot$. We claim that $K[x_1, \ldots, x_n]$ is closed under $*$. Since every monomial in R is a $*$-product of an element of K and the x_i, this will imply that $R=K[x_1, \ldots, x_n]$ as set. Notice that, by definition of R, all the axioms 1.2—except possibly the closedness of $K[x_1, \ldots, x_n]$ under $*$—are valid in $K[x_1, \ldots, x_n]$. So lemmas 1.3 and 1.4 are valid for $f, g \in K[x_1, \ldots, x_n]$, and so $f * g = c \cdot f \cdot g + h \in K[x_1, \ldots, x_n]$, which proves the claim and the theorem.

For an arbitrary commutation system Q, hypothesis (H) may fail.

EXAMPLE 1.8. Let $P=K\langle X, Y, Z\rangle$ and let $Q=\{YX-XY-X,\ ZX-XZ-0,\ ZY-YZ-Z\}$. Then by expressing $(ZY)X=Z(YX)$ as commutative polynomials mod I(Q), we find that $X^2+XY+X \in I(Q)$.

On the other hand, it is not difficult to verify that (H) holds in the following special cases.

EXAMPLE 1.9.

(1) $n=2$, i.e. $P=K\langle X_1, X_2\rangle$.

(2) *More generally, suppose* $P=K\langle X_1,\ldots, X_{2n}\rangle$ and

$$p_{2i,2j}=p_{2i,2j-1}=p_{2i-1,2j}=p_{2i-1,2j-1}=0$$

for $1\leqslant i<j\leqslant n$, and $p_{2i-1,2i}\in K\langle X_{2i-1}\rangle$ for $1\leqslant i\leqslant n$. This includes in particular the Weyl algebra W_{2n} (see Dixmier, 1974; Galligo, 1985; Lassner, 1985).

(3) $P=K\langle X_1,\ldots, X_n\rangle$ and $p_{ij}\in K$ for $1\leqslant i<j\leqslant n$.

The general fact that underlies these examples is the following corollary to theorems 1.6 and 1.7.

COROLLARY 1.10. *Let $<$ be the pure lexicographical order on* T *and assume that the commutator constants c_{ij} of the system* Q *equal* 1 *and the commutator polynomials p_{ij} are in* $K[X_1,\ldots, X_{j-1}]$. *Then* Q *satisfies hypothesis* (H) *iff* $R=P/I(Q)$ *is an iterated Ore extension of* K *using* K-*derivations.*

We are indebted to F. Mora for pointing out to us the following relation between hypothesis (H) and his theory of non-commutative Gröbner bases in $K\langle X_1,\ldots, X_n\rangle$ (see Mora, 1986): Let W be the set of words in $X_1,\ldots, X_n$, and let $<'$ be a positive term ordering on W extending a given admissible order $<$ on T, and such that for $j>i$, $X_jX_i>'t$ for any $t\in T(X_1,\ldots, X_j)$. Then, the following holds.

THEOREM 1.11 (Mora). *Let* Q *be a commutation system for* $(P,<)$. *Then hypothesis* (H) *holds for* Q *iff* Q *is a Gröbner basis for* I(Q) *with respect to* $<$.

PROOF. [Using theorem 5.2 of Mora (1986) and the definitions therein.]

"$\Rightarrow$". Let $0\neq f\in I(Q)$. Then by (H), f is non-commutative, and so some word w in f is non-commutative, say $w=uX_jX_1v$ with $j>i$. Assume for a contradiction that f has no finite d-representation in terms of Q and that f is minimal with this property. Then f could be reduced using the polynomial $q_{ij}\in Q$, a contradiction.

"$\Leftarrow$". If $0\neq f$ is a commutative polynomial, then f is irreducible with respect to Q, since the highest word in q_{ij} is X_jX_i. So f has no finite d-representation in terms of Q, and hence f is not in I(Q).

For a positive term ordering $<'$ on W, theorem 5.2 of Mora (1986) provides an algorithm which decides whether a given finite set of polynomials in P forms a Gröbner basis with respect to $<'$. So theorem 1.11 has the following important consequence.

COROLLARY 1.12. *Let $<$ be an admissible order on* T *that can be extended to a positive term ordering $<'$ of* W *such that for $j>i$ and $t\in T(X_1,\ldots, X_j)$ $X_jX_i>'t$. Then, there is an algorithm that decides for any commutation system* Q *for* $(P,<)$, *whether* Q *satisfies hypothesis* (H).

For the case of the pure lexicographical order $<$ on T, the existence of such a positive term ordering $<'$ on W has been proved by Mora in a letter to us. With his kind permission, we present this term ordering $<'$ here. The definition of $<'$ on $\mathrm{W}(X_1, \ldots, X_n)$ is by induction on n: For $n=1$, the natural definition is the only possible. For $n>1$, put $X_n = Y$, $\mathrm{W}' = \mathrm{W}(X_1, \ldots, X_{n-1})$. Then words $u, v \in \mathrm{W}(X_1, \ldots, X_n)$ can be written uniquely in the form

$$u = a_1 Y a_2 Y \ldots a_r Y a_{r+1}, \quad v = b_1 Y b_2 Y \ldots b_s Y b_{s+1} \quad \text{with} \quad a_i, b_i \in \mathrm{W}'.$$

Then $u <' v$ iff $r < s$ or ($r = s$ and there exists j such that $a_i = b_i$ for $i > j$ and $a_j <' b_j$).

Finally, we remark that solvable polynomial rings of strictly lexicographical type can be constructed by using a more general kind of commutation systems, where the commutator polynomials p_{ij} may be non-commutative:

Theorem 1.13. *Let* $\mathrm{P} = \mathrm{K}\langle X_1, \ldots, X_n\rangle$ *and let* $\mathrm{Q} = \{X_j X_i - X_i X_j - p_{ij}(X_1, \ldots, X_{j-1}): 1 \leqslant i < j \leqslant n\}$, *where the* p_{ij} *may be non-commutative polynomials in* P. *Then* $\mathrm{R} = \mathrm{P}/\mathrm{I}(\mathrm{Q})$ *is a solvable polynomial ring of strictly lexicographical type iff* I(Q) *contains no non-zero commutative polynomial.*

Proof. Let $<$ be the pure lexicographical order on $\mathrm{T} = \mathrm{T}(X_1, \ldots, X_n)$. In view of theorem 1.7, it suffices to show that for $1 \leqslant i < j \leqslant n$, there exist commutative polynomials $p'_{ij} \in \mathrm{K}[X_1, \ldots, X_{j-1}]$ such that for

$$\mathrm{Q}' = \{X_j X_i - X_i X_j - p'_{ij}: 1 \leqslant i < j \leqslant n\}, \quad \mathrm{I}(\mathrm{Q}') = \mathrm{I}(\mathrm{Q}).$$

We construct p'_{ij} by induction on n. For $n \leqslant 2$, we may take $p'_{ij} = p_{ij}$. For $n > 2$, we put $\mathrm{P}_1 = K\langle X_1, \ldots, X_{n-1}\rangle$, $\mathrm{Q}_1 = \mathrm{Q} \cap \mathrm{P}_1$. Then $\mathrm{I}(\mathrm{Q}_1) \subseteq \mathrm{P}_1$ contains no non-zero commutative polynomial, and hence by induction assumption, $\mathrm{R}_1 = \mathrm{P}_1/\mathrm{I}(\mathrm{Q}_1)$ is a solvable polynomial ring of strictly lexicographical type. Moreover, for $1 \leqslant i < j < n$, one can construct commutative polynomials $p'_{ij}(X_1, \ldots, X_{j-1})$ such that for

$$\mathrm{Q}'_1 = \{X_j X_i - X_i X_j - p'_{ij}: 1 \leqslant i < j \leqslant n\}, \quad \mathrm{I}(\mathrm{Q}'_1) = \mathrm{I}(\mathrm{Q}_1).$$

Since for $1 \leqslant i < n, p_{ij} \in \mathrm{P}_1$, one can construct (using lemma 1.4 and the algorithm PRODUCT) commutative polynomials $p'_{in}(X_1, \ldots, X_{n-1})$ such that $p_{in} + \mathrm{I}(\mathrm{Q}_1) = p'_{in}$. Put

$$\mathrm{Q}' = \{X_j X_i - X_i X_j - p'_{ij}: 1 \leqslant i < j \leqslant n\};$$

then $\mathrm{I}(\mathrm{Q}_1) = \mathrm{I}(\mathrm{Q})$, since $\mathrm{I}(\mathrm{Q}'_1) = \mathrm{I}(\mathrm{Q}_1) \subseteq \mathrm{I}(\mathrm{Q})$.

The last construction we are going to consider is due to Apel & Lassner (1988) and in a more restricted context also to El From (1983). Let A be a finite dimensional Lie algebra over a ground field K and let $X_1, \ldots, X_n$ be a basis of A over K. Then there is a canonical construction of an associative K-algebra U(A) from A such that A embeds into U(A), when the Lie-product in U(A) is taken as the commutator $[a, b] = b * a - a * b$. U(A) is called the universal enveloping algebra of A (see Jacobson, 1962; Dixmier, 1974). By the Poincaré–Birkhoff–Witt theorem, the elements of U(A) can be represented uniquely as commutative polynomials in $\mathrm{K}[X_1, \ldots, X_n]$. Let us denote the (non-commutative) multiplication of U(A) by $*$. Then for $1 \leqslant i < j \leqslant n$, $X_j * X_i - X_i * X_j = [X_i, X_j] \in \mathrm{A}$, and so $[X_i, X_j]$ is a linear form in $X_1, \ldots, X_n$ with coefficients in K. Moreover, $*$ satisfies axioms 1.2 (1) and (2).

Let now $<$ be any degree-compatible admissible order on $\mathrm{T} = \mathrm{T}(X_1, \ldots, X_n)$ (i.e. $\deg(s) < \deg(t)$ implies $s < t$ for $s, t \in \mathrm{T}$). Then by the above, $X_j * X_i = X_i X_j + p_{ij}$ with $\deg(p_{ij}) \leqslant 1 < \deg(X_i X_j) = 2$; consequently, $p_{ij} < X_i X_j$ for $1 \leqslant i < j \leqslant n$, and so all the axioms 1.2 are satisfied. If A is a solvable Lie algebra (see Jacobson, 1962; Dixmier, 1974) then $p_{ij} \in \mathrm{K}[X_1, \ldots, X_{j-1}]$ for a suitable choice of the basis $X_1, \ldots, X_n$ of A, and so the axioms 1.2 are also satisfied for the pure lexicographical order (cf. Dixmier, 1974, 1.3.10; El From, 1983). Thus we have shown the following.

THEOREM 1.14. *Let* A *be a finite dimensional Lie algebra over* K. *Then the universal enveloping algebra* U(A) *of* A *is a solvable polynomial ring with respect to any degree-compatible admissible order* $<$ *on* T. *Moreover, if* A *is solvable, then* $<$ *may also be taken as the pure lexicographical order, when the basis* $X_1, \ldots, X_n$ *of* A *is chosen suitably.*

2. Algorithms

In this section we present the main algorithms of our study. We tacitly assume that a fixed polynomial ring of solvable type $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_n\}$ is given by its data c_{ij}, p_{ij}, where $1 \leqslant i < j \leqslant n$, and a computable, $*$-compatible, admissible order $<$ on the set T of terms in R. Recall that for $f \in \mathrm{R}$, $\mathrm{HM}(f)$ denotes the highest monomial of f; we let $\mathrm{REM}(f) = f - \mathrm{HM}(f) < f$ denote the remainder of f. For $\mathrm{P} \subseteq \mathrm{R}$, $\mathrm{I_L(P)}$, $\mathrm{I_R(P)}$, $\mathrm{I(P)}$ denote the left, right, two-sided ideal generated by P in R, respectively. The concepts of left reduction, (left) normal form, left S-polynomial $\mathrm{LSP}(f, g)$, left Gröbner bases (LGBs) and two-sided Gröbner bases (GBs) are defined in sections 3 and 4. Proofs for the correctness of the algorithms are also given in these sections, and in section 1, lemma 1.4, for the first algorithm PRODUCT.

Algorithm (PRODUCT)

Input: (f, g), a pair of polynomials in R.
Output: $p = \mathrm{PROD}(f, g)$, a polynomial in R with $p = f * g$.

```
BEGIN
  IF  $f \in K$  or  $g \in K$
  THEN  $PROD(f,g) := f \cdot g$
  ELSE
  BEGIN
    Write  $f = as + f'$, $g = bt + g'$  with  $as = HM(f)$, $bt = HM(g)$, $s, t \in T$;
    IF  for some $1 \leqslant i \leqslant n$, $s \in T(X_1, \ldots, X_i)$  and  $t \in T(X_i, \ldots, X_n)$
    THEN  $PROD(f,g) := abst + PROD(as,g') + PROD(f',bt) + PROD(f',g')$
    ELSE
    BEGIN
      Pick h,i maximal, j,k minimal with $1 \leqslant h \leqslant j \leqslant n$, $1 \leqslant i \leqslant k \leqslant n$, $i < j$,
      $s \in T(X_h, \ldots, X_j)$, $t \in T(X_i, \ldots, X_k)$;
      IF  $h \leqslant i$
      THEN  BEGIN write $s = X_h s'$;
                  $PROD(f,g) :=$
                  $HC(PROD(as',bt)) \cdot s \cdot t + PROD(X_h, REM(PROD(as',bt))) +$
                  $PROD(as,g') + PROD(f',g)$
            END
      ELSE
      BEGIN
        IF  $j \leqslant k$
        THEN  BEGIN write $t = t'X_k$;
                    $PROD(f,g) := HC(PROD(as,bt')) \cdot s \cdot t +$
```

```
                      $PROD(REM(PROD(as,bt')),X_k) +$
                      $PROD(f',bt) + PROD(f,g')$
            END
        ELSE  {i.e. if $i < h$  and  $k < j$}
        BEGIN  write $s = s''X_j$,  $t = X_i t''$;
                $h_1 := PROD(as'',c_{ij}X_i)$;  $h_2 := PROD(X_j,bt'')$;
                $e_1 u_1 := HM(h_1)//X_i$;
                $e_2 u_2 := HM(h_2)//X_k$;  {with $e_i \in K$}
                $h_3 := PROD(e_1 u_1, e_2 u_2)$;

            $PROD(f, g) := HM(h_3)X_iX_j$  +  $PROD(PROD(as'',p_{ij}),bt'')$  +
                          $PROD(PROD(X_i,REM(h_3)),X_j)$  +
                          $PROD(e_1 X_i u_1, REM(h_2))$  +
                          $PROD(REM(h_1), e_2 u_2 X_j)$  +
                          $PROD(REM(h_1), REM(h_2))$  +
                          $PROD(as,g')$  +  $PROD(f',bt)$  +
                          $PROD(f', g')$
        END
      END
    END
  END
END
```

Note that all recursive calls of PROD in this algorithm refer to inputs f^*, g^* with $f^* \cdot g^* < f \cdot g$.

Using this algorithm, the representation of $f * g$ as in lemma 1.4 can be obtained as follows: Put $c = \mathrm{HC}(\mathrm{PROD}(f, g))//(\mathrm{HC}(f) \cdot \mathrm{HC}(g))$, $h = \mathrm{PROD}(f, g) - c \cdot f \cdot g$. Then $f * g = cfg + h$, and by lemma 1.5, $\mathrm{HT}(\mathrm{PROD}(f, g)) = \mathrm{HT}(c \cdot f \cdot g)$, and so $h < f \cdot g$, and $c = \mathbf{fctr}(f, g)$.

Algorithm (LGRÖBNER) (comp. Buchberger, 1985, algorithm 6.2)

Input: P, a finite set of polynomials in R.
Output: $G = LGB(P)$, a left Gröbner basis in R with $I_L(G) = I_L(P)$, $P \subseteq G$.

```
BEGIN
  $G := P$ ;  $B := \{ \{f,g\} : f,g \in G, f \neq g \}$ ;
  REPEAT
    $\{f,g\}$ := a pair in B ;
    $B := B \setminus \{ \{f,g\} \}$ ;
    $p := LSP(f,g)$ ;
    $p'$ := a left normal form of p modulo G ;
    IF  $p' \neq 0$ ,  THEN
                  BEGIN
                    $B := B \cup \{ \{g,p'\} : g \in G \}$ ;
                    $G := G \cup \{p'\}$
                  END
  UNTIL  $B = \emptyset$ ;
LGB(P) := G
END
```

Note that the following fact is an invariant of the REPEAT-loop: For $\{f,g\} \subseteq G$ with $\{f, g\} \notin B$, $LSP(f, g) \xrightarrow[G]{*} 0$.

Algorithm (LRED)

Input: P, a finite set of polynomials in R.
Output: Q = LRED(P), a finite, reduced set of polynomials in R with $I_L(Q) = I_L(P)$. Moreover, if P is a LGB, the Q is a reduced LGB.

```
BEGIN
  Q := $\emptyset$ ;   B := P ;
  REPEAT
    p := a minimal element of B ;
    B := B $\setminus$ {p} ;
    p' := a left normal form of p modulo Q $\cup$ B ;
    IF  p $\neq$ p',  THEN
                   BEGIN
                     B := B $\cup$ Q $\cup$ {p'};   Q := $\emptyset$
                   END
                 ELSE  Q := Q $\cup$ {HC(p')$^{-1}$ $\cdot$ p'}
  UNTIL  B = $\emptyset$ ;
  LRED(P) := Q
END
```

Note that the following facts are invariants of the REPEAT-loop: $Q \cap B = \emptyset$; $I_L(Q \cup B) = I_L(P)$; every $f \in Q$ is in monic and in left normal form modulo $(Q \cup B) \setminus \{f\}$.

Algorithm (GRÖBNER = GRÖBNER (left))

Input: P, a finite set of polynomials in R.
Output: G = GB(P), a two-sided Gröbner basis in R with I(G) = I(P), $P \subseteq G$.

```
BEGIN
  B := P ;
  REPEAT
    G := LGB(B) ;   B := G ;   i := 0 ;
    REPEAT
      i := i+1 ;   Q := G ;
      REPEAT
        p := an element of Q ;
        Q := Q $\setminus$ {p} ;
        p' := a left normal form of p*$X_i$ modulo G ;
        IF  p' $\neq$ 0 ,  THEN  B := B $\cup$ {p'}
      UNTIL  Q = $\emptyset$
    UNTIL  i = n
  UNTIL  B = G ;
  GB(P) := G
END
```

The following assertions are invariants of the outermost REPEAT-loop: I(G) = I(P); G is a left Gröbner basis; $g * X_i \xrightarrow[\mathrm{B}]{*} 0$ for all $g \in \mathrm{G}$, $1 \leqslant i \leqslant n$; all $h \in \mathrm{B} \backslash \mathrm{G}$ are reduced modulo G.

Analogous algorithms RGRÖBNER, RRED, GRÖBNER(right) are defined by replacing everywhere "left" by "right".

Starting from a finite set F polynomials, a reduced LGB for $\mathrm{I_L(F)}$ (a reduced RGB for $\mathrm{I_R(F)}$, a reduced GB for I(F) can be obtained by composing the algorithm LGRÖBNER (RGRÖBNER, GRÖBNER) with the algorithm LRED (RRED, LRED or RRED) (see 3.18 and 4.5). More efficient algorithms for this purpose are, however, obtained by intertwining the two respective algorithms similar as in the commutative case (see Buchberger, 1985, 6.4).

3. Left Reduction and Left Gröbner Bases

Throughout this section, $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_r\}$ will be a polynomial ring of solvable type.

Let $f, f', p \in \mathrm{R}$. Then we say *f reduces to f' modulo p by erasing t (notation $f \xrightarrow[p]{} f'(t)$)*, if $\mathrm{HT}(p)$ div t, say $s = t//\mathrm{HT}(p)$, a is the coefficient of t in f, $b = \mathrm{HC}(p)$, $c = \mathbf{fctr}(s, \mathrm{HT}(p))$ and $f' = f - (a/bc) * s * p$. (Notice that, by lemma 1.5, $t \notin \mathrm{T}(f')$.) We say f reduces to f' modulo p (notation $f \xrightarrow[p]{} f'$), if $f \xrightarrow[p]{} f'(t)$ for some $t \in \mathrm{T}(f)$. Now let $\mathrm{P} \subseteq \mathrm{R}$; then we say *$f$ reduces to f' modulo* P (*notation* $f \xrightarrow[p]{} f'$), if for some $p \in \mathrm{P}$, $f \xrightarrow[p]{} f'$; *f is reducible modulo* P, if for some $f' \in \mathrm{R}$, $f \xrightarrow[p]{} f'$; if this is not the case, we say *f is irreducible* (or *in normal form*) *modulo* P.

Example 3.1. Let $\mathrm{R} = \mathrm{Q}\{X, Y\} = \mathrm{Q}\langle X, Y\rangle/\mathrm{I}(YX - XY - X)$, $<$ pure lexicographic with $X < Y$. Consider $\mathrm{P} = (p_1\, p_2)$ with $p_1 = XY^2 - X$, $p_2 = 3X^2Y - Y$. p_1 and p_2 are polynomials with highest terms $\mathrm{HT}(p_1) = XY^2$, $\mathrm{HT}(p_2) = X^2Y$. Then the polynomial $g = Y^4 + XY^3 + 2X^3Y + 1$ can be reduced with respect to P as follows:

$$g \xrightarrow[p_1]{} g' \xrightarrow[p_1]{} g'' \xrightarrow[p_2]{} g''',$$

where

$$g' = g - Y * p_1 = g - (XY + X) * Y^2 + XY + X = X^4 - XY^2 + 2X^3Y + XY + X + 1,$$

$$g'' = g' - (-p_1) = Y^4 + 2X^3Y + XY + 1,$$

$$g''' = g'' - \tfrac{2}{3}Xp_2 = Y^4 + \tfrac{5}{3}XY + 1,$$

which is irreducible modulo P.

Lemma 3.2. *Let* $\mathrm{P} \subseteq \mathrm{R}$. *Then the following hold:*

(1) *For all* $f, f' \in \mathrm{R}$, $f \xrightarrow[\mathrm{P}]{} f'$ *implies* $f' < f$.

(2) $\xrightarrow[\mathrm{P}]{}$ *is a Noetherian relation* (*i.e. there is no infinite sequence*

$$g \xrightarrow[\mathrm{P}]{} g' \xrightarrow[\mathrm{P}]{} g'' \xrightarrow[\mathrm{P}]{} \ldots \textit{ in } \mathrm{R}).$$

(3) *Every* $f \in \mathrm{R}$ *has a* (*not necessarily unique*) *normal form mod* P.

Proof.

(1) Suppose $f \xrightarrow[\mathrm{P}]{} f'(t)$. Then by 1.5, $t \in \mathrm{T}(f')$ and for all $v \in \mathrm{T}$ with $v > t$, $v \in \mathrm{T}(f)$ iff $v \in \mathrm{T}(f')$. This implies $f' < f$.

(2) If $f \xrightarrow[\mathrm{P}]{} f'$, then by (1) $f' < f$, and $<$ is a well-founded quasi-ordering of R.

(3) This follows immediately from (2).

We let $\overset{*}{\to}$ ($\overset{*}{\leftrightarrow}$) be the reflexive, transitive (the reflexive, symmetric, transitive) closure of $\to$. $f \downarrow g$ holds if $f \overset{*}{\to} h$ *and* $g \overset{*}{\to} h$ for some $h \in \mathrm{R}$.

LEMMA 3.3 *Let* f, g *be in* R, *and let* P *be a finite set of polynomials in* R. *Let* $\mathrm{I_L(P)}$ *be the left ideal generated by* P. *Then* $f \overset{*}{\underset{\mathrm{P}}{\leftrightarrow}} g$ *implies* $f-g \in \mathrm{I_L(P)}$.

The proof is by induction on k, where $f \overset{k}{\underset{\mathrm{P}}{\leftrightarrow}} g$.

Since $\underset{\mathrm{P}}{\to}$ is Noetherian, it is well known that:

$\underset{\mathrm{P}}{\to}$ is locally confluent iff
$\underset{\mathrm{P}}{\to}$ is confluent iff

$\underset{\mathrm{P}}{\to}$ satisfies the Church–Rosser property (see Huet, 1980, for more details).

The following lemmas will be useful in the proof of the main theorem 3.11.

LEMMA 3.4 (*Translation lemma*). *Let* $\to$ *be the reduction relation induced by a finite set* P *of polynomials in* R. *Let* $f, g, h, h' \in \mathrm{R}$, *where* $f = g+h$, $h \overset{*}{\to} h'$. *Then there exist* $f', g' \in \mathrm{R}$ *such that* $f \overset{*}{\to} f'$, $g \overset{*}{\to} g'$ *and* $f' = g'+h'$.

PROOF. By induction on n, where $h \overset{n}{\to} \mathrm{h}'$. The case $n = 0$ is obvious. If $h \overset{n+1}{\to} h'$, we find, by the induction assumption, polynomials f'', g'', h'' in R such that $f \overset{*}{\to} f''$, $g \overset{*}{\to} g''$, $h \overset{n}{\to} h'' \to h'$ and $f'' = g''+h''$. Let $h' = h'' - (c/d \cdot b)u * p$, where $c \in \mathrm{K}$, $u \in \mathrm{T}$, $p \in \mathrm{P}$, $b = \mathrm{HC}(p)$ and $d = \mathbf{fctr}(u, p)$. Let c_1 (c_2) be the coefficient of $u \cdot \mathrm{HT}(p)$ in f'' (g''), where c_1 (c_2) is zero if this term does not occur in f'' (g''). We put $f' = f'' - (c_1/d \cdot b)u * p$, $g' = g'' - (c_2/d \cdot b)u * p$. Then $c_1 = c_2 + c$, and so $f' = g'+h'$, and by definition $f'' \overset{*}{\to} f'$, $g'' \overset{*}{\to} g'$. Together with the induction assumption, this proves that $f \overset{*}{\to} f'$, $g \overset{*}{\to} g'$.

Specialising in lemma 3.4 $h' = 0$, we obtain the following.

LEMMA 3.5. For all finite $\mathrm{P} \subseteq \mathrm{R}$ and all $f, g \in \mathrm{R}$, $f-g \overset{*}{\underset{\mathrm{P}}{\to}} 0$ implies $f \underset{\mathrm{P}}{\downarrow} g$.

Recall that for $\mathrm{P} \subseteq \mathrm{R}$, $\mathrm{I_L(P)}$ denotes the left ideal generated by P and I(P) denotes two-sided ideal generated by P.

LEMMA 3.6. *Let* P *be a finite set of polynomials in* R.

(1) *For all* $f \in \mathrm{R}$, $p \in \mathrm{P}$, $f * p \overset{*}{\underset{\mathrm{P}}{\to}} 0$.
(2) *For all* $f, g \in \mathrm{R}$, $f-g \in \mathrm{I_L(P)}$ *implies* $f \overset{*}{\underset{\mathrm{P}}{\leftrightarrow}} g$.
(3) *Suppose that for all* $s, s' \in \mathrm{T}$, $p \in \mathrm{P}$, $s * p * s' \overset{*}{\underset{\mathrm{P}}{\to}} 0$. *Then for all* $f, g \in \mathrm{R}$, $f-g \in \mathrm{I(P)}$ *implies* $f \overset{*}{\underset{\mathrm{P}}{\leftrightarrow}} g$.

PROOF.

(1). Assume for a contradiction that $f \in \mathrm{R}$ is minimal such that for some $p \in \mathrm{P}$, not $f * p \overset{*}{\underset{\mathrm{P}}{\to}} 0$. Let $t = \mathrm{HT}(f * p)$. Then there exists a reduction $f * p \overset{*}{\underset{\mathrm{P}}{\to}} g = f * p - c * s * p$ (t) with $c \in \mathrm{K}$. By lemma 1.5, $\mathrm{HT}(f) = s$, and so $\mathrm{HT}(f - c \cdot s) < \mathrm{HT}(f)$, and so by the choice of f, $g = (f - c \cdot s) * p \overset{*}{\underset{\mathrm{P}}{\to}} 0$, and so $f * p \overset{*}{\underset{\mathrm{P}}{\to}} 0$.

(2) and (3). Note that $f-g \in \mathrm{I_L(P)}$ iff

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

and $\mathrm{f}-g \in \mathrm{I(P)}$ iff

$$f-g = \sum_{i=1}^{k} s_i * p_i * s_i'$$

for some $c_i \in \mathrm{K}$, s_i, $s_i' \in \mathrm{T}$, $p \in \mathrm{P}$. By (1), $c \cdot s * p \xrightarrow[p]{*} 0$ for all $c \in \mathrm{K}$, $s \in \mathrm{T}$, $p \in \mathrm{P}$. The lemma is now shown by induction on k, using lemma 3.5.

Definition. A finite set G of polynomials in R is a *left Gröbner basis* (*LGB*) if the left reduction relation $\rightarrow$ induced by G is confluent (i.e. $f \xrightarrow{*} f_1$ and $f \xrightarrow{*} f_2$ imply $f_1 \downarrow f_2$ for all $f, f_1, f_2 \in \mathrm{R}$).

Example 3.7. Let R and P be as in example 3.1. Then P is not a LGB. Indeed,

$$X^2Y^2 \xrightarrow[p_1]{} X^2Y^2 - X * (XY^2 - X) = X^2,$$

which is is normal form modulo P, and on the other hand

$$\begin{aligned} X^2Y^2 \xrightarrow[p_2]{} \mathrm{X}^2\mathrm{Y}^2 - \tfrac{1}{3}\mathrm{X} * \mathrm{p}_2 &= \mathrm{X}^2\mathrm{Y}^2 - \mathrm{Y} * \mathrm{X}^2\mathrm{Y} + \tfrac{1}{3}\mathrm{Y}^2 \\ &= -2\mathrm{X}^2\mathrm{Y} + \tfrac{1}{3}\mathrm{Y}^2 \xrightarrow[p_2]{} -2X^2Y + \tfrac{1}{3}Y^2 + \tfrac{2}{3}p_2 \\ &= \tfrac{1}{3}(Y^2 - 2Y), \end{aligned}$$

which is also in normal form modulo P.

Lemma 3.8. *Let* G *be a finite subset of* R. *Then the following assertions are equivalent.*

(1) G *is a left Gröbner basis.*
(2) *For all* $f, g \in \mathrm{R}$, $f-g \in \mathrm{I_L(G)}$ *implies* $f \downarrow g$.
(3) *For all* $f \in \mathrm{I_L(G)}$, $f \xrightarrow[G]{*} 0$.
(4) *For all* $0 \neq f \in \mathrm{I_L(G)}$, f *is reducible modulo* G.
(5) *For all* $0 \neq f \in \mathrm{I_L(G)}$, *there exists* $g \in \mathrm{G}$ *such that* $\mathrm{HT}(g)$ *div* $\mathrm{HT}(f)$.

Proof.

(1) ⇒ (2). By lemma 3.6 (1), $f-g \in \mathrm{I_L(G)}$ implies $f \overset{*}{\underset{G}{\leftrightarrow}} g$. By (1), $\xrightarrow[G]{}$ has the Church–Rosser property, and so $f \downarrow g$.

(2) ⇒ (3). Specialise $g = 0$ in (2).

(3) ⇒ (1). Let $f \xrightarrow[G]{*} f_1$, $f \xrightarrow[G]{*} f_2$. Then by lemma 3.3, $f_1 - f_2 \in \mathrm{I_L(G)}$, and so by (3), $f_1 - f_2 \xrightarrow[G]{*} 0$. By lemma 3.5, this implies $f_1 \downarrow f_2$. Thus we have shown that $\xrightarrow[G]{}$ is confluent.

(3) ⇒ (5). Let $0 \neq f \in \mathrm{I_L(G)}$, let $f = f_0 \xrightarrow[G]{} f_1 \xrightarrow[G]{} f_2 \ldots \xrightarrow[G]{} f_m = 0$, and $0 \leqslant k < m$ be minimal with $\mathrm{HT}(f_k) = \mathrm{HT}(f)$. Then $f_k \xrightarrow[G]{} f_{k+1}(\mathrm{HT}(f))$, and so $\mathrm{HT}(g)$ div $\mathrm{HT}(f)$ for some $g \in \mathrm{G}$.

(5) ⇒ (4). This is trivial.

(4) ⇒ (3). Assume $0 \neq f \in \mathrm{I_L(G)}$ is minimal such that not $f \xrightarrow[G]{*} 0$. Then for some $f' \in \mathrm{I_L(G)}$, $f \xrightarrow[G]{} f' \xrightarrow[G]{*} 0$, and so $f \xrightarrow[G]{*} 0$, a contradiction.

As in the commutative case, we need to define the notion of a *left S-polynomial*, in order to characterise and construct left Gröbner bases. We will show that $\mathrm{P} \subseteq \mathrm{R}$ is a left Gröbner basis iff the left S-polynomials between all pairs of polynomials in P reduce to zero.

Definition. Let f, g be polynomials in R with highest coefficients a, b and highest terms s, t, respectively. Let $t' = \mathrm{lcm}(s, t)$ (as defined in section 1), let $u = t'//s$, $v = t'//t$ and let $c = \mathbf{fctr}(u, \mathrm{HT}(f))$, $d = \mathbf{fctr}(v, \mathrm{HT}(g))$. Then the *left S-polynomial of f and g* is defined as follows:

$$\mathrm{LSP}(f, g) = \mathrm{LSP}_1(f, g) - \mathrm{LSP}_2(f, g),$$

where

$$\mathrm{LSP}_1(f, g) = b \cdot d * u * f, \quad \mathrm{LSP}_2(f, g) = a \cdot c * v * g.$$

Example 3.9. Let

$$\mathrm{R} = \mathrm{Q}\{X, Y, Z\} = \mathrm{Q}\langle X, Y, Z\rangle / \mathrm{I}(\{YX - XY - 2, ZX - XZ - 1, ZY - YZ\}).$$

Consider $f = 2X^2YZ + XY^3$ and $g = 3XY^2 - X$. We have $\mathrm{HT}(f) = X^2YZ$, $\mathrm{HT}(g) = XY^2$ and $\mathrm{lcm}(X^2YZ, XY^2) = X^2Y^2Z$. So

$$\begin{aligned} \mathrm{LSP}(f, g) &= 3Y * (2X^2YZ + XY^3) - 2XZ * (3XY^2 - X) \\ &= 6(X^2Y + 4X) * YZ + 3(XY + 2)Y^3 - 6X(XZ + 1)Y^2 + 2X(XZ + 1) \\ &= 24XYZ + 2X^2Z + 3XY^4 + 6Y^3 - 6XY^2 + 2X. \end{aligned}$$

Lemma 3.10. *Let $\mathrm{P} \subseteq \mathrm{R}$, $f \in \mathrm{R}$ be such that $\xrightarrow[\mathrm{P}]{}$ is confluent on $\mathrm{F} = \{h \in \mathrm{R} : h < f\}$.*

(1) *If $h_1 \in \mathrm{F}$, $h_1 \xrightarrow[\mathrm{P}]{*} 0$, $h_2 \xrightarrow[\mathrm{P}]{*} 0$, $h = h_1 + h_2$, then $h \xrightarrow[\mathrm{P}]{*} 0$.*
(2) *If $c \in \mathrm{K}$, $s \in \mathrm{T}$, $g \in \mathrm{R}$ such that $s * g \in \mathrm{F}$ and $g \xrightarrow[\mathrm{P}]{*} 0$, then $c * s * g \xrightarrow[\mathrm{P}]{*} 0$.*

Proof.

(1) By lemma 3.5, $h \downarrow h_1$, say $h \xrightarrow[\mathrm{P}]{*} h_3 \xleftarrow[\mathrm{P}]{*} h_1$, and $h_1 \xrightarrow[\mathrm{P}]{*} 0$. By the confluence of $\xrightarrow[\mathrm{P}]{}$ on F, there exists $h_4 \in \mathrm{R}$, such that $h_3 \xrightarrow[\mathrm{P}]{*} h_4 \xleftarrow[\mathrm{P}]{*} 0$, and so $h_4 = 0$, and so $h \xrightarrow[\mathrm{P}]{*} 0$.
(2) Assume for a contradiction that $g \in \mathrm{R}$ is a minimal with $s * g \in \mathrm{F}$, $g \xrightarrow[\mathrm{P}]{*} 0$, not $c * s * g \xrightarrow[\mathrm{P}]{*} 0$. Then for some $g_1 \in^* \mathrm{R}$, $g \xrightarrow[\mathrm{P}]{*} g_1 \xrightarrow[\mathrm{P}]{*} 0$, where $g_1 = g - h * p$, $h \in \mathrm{R}$, $p \in \mathrm{P}$ and $\mathrm{HT}(g_1) < \mathrm{HT}(g)$; so by lemma 1.5, $\mathrm{HT}(s * g_1) < \mathrm{HT}(s * g)$, and so $s * g_1 \in \mathrm{F}$. Consequently, $c * s * g = c * s * g_1 + c * s * h * p$, and by lemma 3.6 (1), $c * s * h * p \xrightarrow[\mathrm{P}]{*} 0$, and by the choice of g, $c * s * g_1 \xrightarrow[\mathrm{P}]{*} 0$. So by (1), $c * s * g \xrightarrow[\mathrm{P}]{} 0$.

Theorem 3.11. *Let G be a finite set of polynomials in R. Then G is a LGB iff for all $f, g \in \mathrm{G}$, $\mathrm{LSP}(f, g) \xrightarrow[\mathrm{G}]{*} 0$.*

Proof.

(⇒:) For $f, g \in \mathrm{G}$, $h = \mathrm{LSP}(f, g) \in \mathrm{I_L}(\mathrm{HG})$, and so by lemma 3.8, $h \xrightarrow[\mathrm{G}]{*} 0$.
(⇐:) In order to show that $\xrightarrow[\mathrm{G}]{}$ is locally confluent, assume that $f, f_1, f_2 \in \mathrm{R}$, $p_1, p_2 \in \mathrm{G}$ are such that $f \xrightarrow[p_1]{} f_1$, $f \xrightarrow[p_2]{} f_2$. By induction on the well-founded quasi-ordering $<$, we may assume that the reduction relation $\xrightarrow[\mathrm{G}]{}$ is locally confluent and hence confluent on $\mathrm{F} = \{h \in \mathrm{R} : h < f\}$. By lemma 3.5, it suffices to show that $f_2 - f_1 \xrightarrow[\mathrm{G}]{*} 0$. Let $\mathrm{HT}(p_1) = s_i$, $\mathrm{HC}(p_i) = b_i$, $f_1 = f - a_i * u_i * p_i$ with $a_i \in \mathrm{K}$, $u_i \in \mathrm{T}$. Then $t_i = u_i s_i \in \mathrm{T}(f)$ for $i = 1, 2$. We distinguish two cases.

Case 1. (This case does neither use the hypothesis nor the induction assumption.) $t_1 \neq t_2$, say $t_2 < t_1$. Then $f_2 - f_1 = a_1 * u_1 * p_1 - a_2 * u_2 p_2$. Since $\mathrm{HT}(u_1 * p_1) = t_1 > t_2 = \mathrm{HT}(u_2 * p_2)$, the monomial $a_1 b_1 t_1$ occurs in $f_2 - f_1$, and so

$$f_2 - f_1 \xrightarrow[p_1]{} (f_2 - f_1) - a_1 * u_1 * p_1 = a_2 * u_2 * p_2 \xrightarrow[p_2]{} 0.$$

Case 2. $t_1 = t_2 =: t$; let c be the coefficient of t in f. Then $\mathrm{HC}(a_i * u_i * p_i) = c$ for $i = 1, 2$. Let $t' = \mathrm{lcm}(s_1, s_2) = u_i' s_i$, and let $w \cdot t' = t$ for uniquely determined $u_i', w \in \mathrm{T}$. Let $d = \mathrm{HC}(\mathrm{LSP}_i(p_1, p_2))$ and let $d' = \mathbf{fctr}(w, t')$; then

$$\mathrm{HC}(c/dd') \cdot \mathrm{LSP}_i(p_1, p_2) = c$$

for $i=1, 2$. So

$$\begin{aligned} f_2-f_1 &= a_1 * u_1 * p_1 - a_2 * u_2 * p_2 = (a_1 * u_1 * p_1 - (c/dd') * w * u_1' * p_1) \\ &\quad + (c/d') * w * (\mathrm{LSP}_1(p_1, p_2) - \mathrm{LSP}_2(p_1, p_2)) \\ &\quad + (c/dd') * w * u_2' p_2 - a_2 * u_2 * p_2) \\ &= (a_1 u_1 - (c/dd') * w * u_1') * p_1 + (c/d') * w * \mathrm{LSP}(p_1, p_2) \\ &\quad + (c/dd') * w * u_2' - a_2 * u_2) * p_2. \end{aligned}$$

By lemma 3.6 (1),

$$(a_1 u_1 - (c/dd') * w * u_1') * p_1 \xrightarrow[G]{*} 0 \quad \text{and} \quad (c/dd') * w * u_2' - a_2 u_2) * p_2 \xrightarrow[G]{*} 0,$$

and by hypothesis $\mathrm{LSP}(p_1, p_2) \xrightarrow[G]{*} 0$, and so by lemma 3.10 (2), $(c/d') * w * \mathrm{LSP}(p_1, p_2) \xrightarrow[G]{*} 0$, since $w * \mathrm{LSP}(p_1, p_2) < w \cdot t' = t \lesssim f$, i.e. $w * \mathrm{LSP}(p_1, p_2) \in \mathrm{F}$. We can now apply 3.10 (1) twice to conclude that $f_2 - f_1 \xrightarrow[G]{*} 0$.

Corollary 3.12. *For any* $g \in \mathrm{R}$, $\{g\}$ *is a* LGB.

Another well-known fact about Gröbner bases in commutative polynomial rings R is the following (see Buchberger, 1985): any finite set of monomials in R is a Gröbner basis with respect to any admissible order on T. This is no longer true for solvable polynomial rings: Let $\mathrm{R} = \mathbb{Q}\langle X, Y\rangle / YX - XY - 1$ and let $\mathrm{P} = \{X, Y\}$. Then $1 = Y * X - X * Y \in \mathrm{I_L(P)}$, and so P is not a LGB.

By the way of contrast, the computation of *left elimination ideals* works as in the commutative case (cf. Buchberger, 1985).

Corollary 3.13. *Let* $\mathrm{R} = \mathrm{K}\{X_1, \ldots, X_r\}$, $0 \leqslant m < r$, $\mathrm{R}' = \mathrm{K}\{X_1, \ldots, X_m\}$, *assume* T *is ordered pure lexicographically*, $X_1 < \ldots < X_r$, *let* G *be a (reduced) left Gröbner basis in* R *with respect to* $<$, *and let* $\mathrm{G}' = \mathrm{G} \cap \mathrm{R}'$. *Then* G′ *is a (reduced) left Gröbner basis in* R′ *and* $\mathrm{I_L(G)} \cap \mathrm{R}' = \mathrm{I_L'(G')}$, *where* $\mathrm{I_L'(H)}$ *denotes the left ideal generated by* H *in* R′.

Proof. Whenever $h \in \mathrm{R}'$ and $h \xrightarrow[g]{} h'\ (t)$ for some $g \in \mathrm{G}$, the $\mathrm{HT}(g)$ div t, and so $\mathrm{HT}(g) \in \mathrm{R}'$, and so $g \in \mathrm{R}'$. This shows that G′ is a (reduced) left Gröbner basis in R′. Next, let $f \in \mathrm{I_L(G)} \cap \mathrm{R}'$. Then $f \xrightarrow[G]{*} 0$, and so by the above, $f \xrightarrow[G']{*} 0$, and so $f \in \mathrm{I_L'(G')}$. Then converse inclusion $\mathrm{I_L'(G')} \subseteq \mathrm{I_L(G)} \cap \mathrm{R}'$ is obvious.

The main use of theorem 3.11 consists in the fact that left Gröbner bases can be constructed algorithmically: Consider the algorithm LGRÖBNER. When the algorithm terminates, G is by lemma 3.3 a finite extension of P with $\mathrm{I_L(P)} = \mathrm{I_L(G)}$; moreover, for all $f, g \in \mathrm{G}$, $\mathrm{LSP}(f, g) \xrightarrow[G]{*} 0$, and so by 3.11 G is a LGB. Whenever a new polynomial p is added to G in the course of the computation, then for all $g \in \mathrm{G}$, not $\mathrm{HT}(g)$ div $\mathrm{HT}(p)$; so by Dickson's lemma 1.1, the algorithm terminates.

As in the commutative case (see Buchberger, 1985, problem 6.8, method 6.6), left Gröbner bases provide an explicit basis for the vector space $\mathrm{R}/\mathrm{I_L(G)}$ over K.

Corollary 3.14. *Let* G *be a* LGB *in* R, *let* $\mathrm{B} = \{s \in \mathrm{T}$: *For all* $g \in \mathrm{G}$, *not* $\mathrm{HT}(g)$ *div* $s\}$, *and let* $[s]$ *denote the coset of* s *modulo* $\mathrm{I_L(G)}$. *Then*

(1) $\mathrm{B}' = \{[s] : s \in \mathrm{B}\}$ *is a* K*-basis of the vector space* $\mathrm{R}/\mathrm{I_L(G)}$.
(2) $\mathrm{R}/\mathrm{I_L(G)}$ *is finite-dimensional iff for every* $1 \leqslant i \leqslant r$ *there exist* $g_i \in \mathrm{G}$ *such that* $\mathrm{HT}(g_i)$ *is a power of* X_i.

Proof.

(1) Assume for a contradiction that $\sum_{1\leqslant i\leqslant k} a_i[s_i]=[0]$ for certain $0\neq a_i\in K$ and pairwise different $s_i\in B$. Then $f=\sum_{1\leqslant i\leqslant k} a_is_i\in I_L(G)$, and so $f\xrightarrow[G]{*}0$, and so some s_j is reducible modulo G, and so HT(g) div s_j for some $g\in G$, a contradiction. This shows that B′ is linearly independent. Next let $f\in R$ be arbitrary, and let $f'=\sum_{1\leqslant i\leqslant k} a_is_i$ (with $s_i>s_{i+1}$) be the normal form of f modulo G. Then $s_i\in B$ for all i, $[f]=[f']=\sum_{1\leqslant i\leqslant k} a_i[s_i]$, and so B′ spans $R/I_L(G)$.

(2) If the condition on G is satisfied then the degree of all $s_i\in B$ is bounded, and so B is finite. Conversely, if the condition fails for i, then B contains all powers of X_i, and so B is infinite.

We close this section with the computation a generating set for the left R-module of syzygies with respect to a left Gröbner basis. The method is modelled after the commutative case presented in Buchberger (1976); the special case that R is the universal enveloping algebra of a finite-dimensional Lie algebra is handled also in Apel & Lassner (1988).

Call a polynomial $f\in R$ *monic*, if $HC(f)=1$. A set F of polynomials in R is *monic* if every $f\in F$ is monic. Let $G=\{g_1,\ldots,g_m\}$ be a monic left Gröbner basis, and let

$$M=\{h_1,\ldots,h_m\}\in R^m: h_1*g_1+\ldots+h_m*g_m=0\}$$

be the corresponding left R-module of syzygies. Let

$$f_{ij}=\mathrm{LSP}(g_i,g_j)=e_{ij}*u_{ij}*g_i-d_{ij}*v_{ij}*g_j,$$

where $u_{ij}, v_{ij}\in T$, $d_{ij}, e_{ij}\in K$, and

$$\mathrm{HC}(e_{ij}*u_{ij}*g_i)=\mathrm{HC}(d_{ij}*v_{ij}*g_j)$$

for $1\leqslant i<j\leqslant m$. Since $f_{ij}\xrightarrow[G]{*}0$, one can compute polynomials $q_{ijk}\in R$ such that

$$f_{ij}=q_{ij1}*g_1+\ldots+q_{ijm}*g_m \quad\text{and}\quad \mathrm{HT}(q_{ijk}*g_k)\leqslant\mathrm{HT}(f_{ij})<\mathrm{HT}(u_{ij}*g_i),\ \mathrm{HT}(v_{ij}*g_j).$$

Put $r_{ijk}=q_{ijk}$ for $k\neq i,j$,

and put

$$r_{iji}=q_{iji}-e_{ij}\cdot u_{ij},\quad r_{ijj}=q_{ijj}+d_{ij}\cdot v_{ij},$$
$$b_{ij}=(r_{ij1},\ldots,r_{ijm})\in R^m,\quad B=\{b_{ij}:1\leqslant i<j\leqslant m\}.$$

Theorem 3.15. B generates M as a left R-module.

Proof.

1. Since $f_{ij}-e_{ij}u_{ij}*g_i+d_{ij}v_{ij}*g_j=0$, we have

$$\begin{aligned}0&=\sum_{1\leqslant k\leqslant m,\,k\neq i,j} q_{ijk}*g_k+(q_{iji}-e_{ij}u_{ij})*g_i+(q_{ijj}+d_{ij}v_{ij})*g_j\\&=\sum_{1\leqslant k\leqslant m} r_{ijk}*g_k.\end{aligned}$$

Consequently, $b_{ij}\in M$.

2. Assume for a contradiction that there exists $h=(h_1,\ldots,h_m)\in \mathrm{M}$ such that $h\neq \sum_{1\leqslant i<j\leqslant m} f_{ij}b_{ij}$ for all $f_{ij}\in \mathrm{R}$. Pick h such that $\max\{\mathrm{HT}(h_i * g_i):1\leqslant i\leqslant m\}=:t$ is minimal, and among all these, such that the number of elements in $\{i:\mathrm{HT}(h_i * g_i)=t\}$ is minimal. Let $a_k=\mathrm{HC}(h_k)$. Since $\sum_{1\leqslant k\leqslant m} h_k * g_k=0$, there exist $1\leqslant i<j\leqslant m$ such that $\mathrm{HM}(h_i * g_i)=\mathrm{HM}(h_j * g_j)=c\cdot t$. Pick $v\in \mathrm{T}$ with $t=v\cdot u_{ij}\cdot \mathrm{HT}(g_i)$ $=v\cdot v_{ij}\cdot \mathrm{HT}(g_j)$. By (1.), $\sum_{1\leqslant k\leqslant m} r_{ijk} * g_k=0$, and so $0=\sum_{1\leqslant k\leqslant m} h'_k * g_k$, where
$$h'_k=h_k-(c/dd')v * r_{ijk},\ d=HC(e_{ij} * u_{ij} * g_i)=\mathrm{HC}(d_{ij} * v_{ij} * g_j),$$
$$d'=\mathbf{fctr}\ (v,\mathrm{HT}(u_{ij} * g_i))=\mathbf{fctr}\ (v,\mathrm{HT}(v_{ij} * g_j)).$$

Claim. $\mathrm{HT}(h'_i * g_i)<t$, $\mathrm{HT}(h'_j * g_j)\leqslant t$, and for $k\neq i,j$, $\mathrm{HT}(h'_k * g_k)<t(\leqslant t)$, if $\mathrm{HT}(h_k * g_k)$ $<t(\leqslant t)$.

Granted the claim, we can apply induction assumption to $h'=(h'_1,\ldots,h'_m)\in \mathrm{M}$, and find $p_{ij}\in \mathrm{R}$ such that $h'=\sum_{1\leqslant i<j\leqslant m} p_{ij} * b_{ij}$. Since $h=h'+(c/dd') * v * b_{ij}$, we obtain $h=\sum_{1\leqslant i<j\leqslant m} [p_{ij}+(c/dd') * v] * b_{ij}$, a contradiction.

Proof of the Claim.
$$\mathrm{HT}(h_i * g_i-(c/dd') * v * u_{ij} * g_i+(c/dd') * v * q_{iji} * g_i)<t,$$
since
$$\mathrm{HM}(h_i * g_i)=\mathrm{HM}[(c/dd') * v * u_{ij} * g_i]$$
and
$$\mathrm{HT}[(c/dd') * v * q_{iji} * g_i]<v\cdot u_{ij}\cdot \mathrm{HT}(g_i)=t.$$
Similarly,
$$\mathrm{HT}(h_j * g_j)+(c/dd') * v * v_{ij} * g_j-(c/dd') * v * q_{ijj} * g_j)\leqslant v\cdot v_{ij}\cdot \mathrm{HT}(g_j)=t.$$
For $k\neq i,j$,
$$\mathrm{HT}(h_k * g_k+(c/dd') * v * q_{ijk} * g_k)\leqslant \max(\mathrm{HT}(h_k * g_k),$$
so
$$v\cdot \mathrm{HT}(q_{ijk} * g_k))<t(\leqslant t),\ \text{if } \mathrm{HT}(h_k * g_k)<t(\leqslant t).$$

Given an arbitrary finite set $\mathrm{F}=\{f_1,\ldots,f_r\}$ of polynomials in R; then a basis of $\mathrm{M}=\{h\in \mathrm{R}^r:h * f=0\}$ can be computed from theorem 3.14 and a left Gröbner basis G for $\mathrm{I_L(F)}$ as in the commutative case (see Buchberger, 1976).

4. Right and Reduced Gröbner Bases

All the definitions given in section 3 in terms of left reduction and left ideals can of course be duplicated for right reduction ($\overset{r}{\rightarrow}$) and right ideals $\mathrm{I_R(P)}$. This yields corresponding results for *right Gröbner bases* (RGB's). In general, a set G of polynomials in R may be a LGB without being a RGB, and the reverse is true.

Example 4.1. Let $\mathrm{R}=\mathbb{Q}\langle X,Y\rangle/\mathrm{I}(YX-XY-1)$ and let $\mathrm{G}=\{p_1,p_2\}\in \mathrm{R}$ with $p_1=X$, $p_2=XY+1$. Then G is a LGB, since $\mathrm{LSP}(p_1,p_2)=Y * p_1-p_2=Y * X-XY-1=0$. On the other hand, $1=p_2-p_1 * Y\in \mathrm{I_R(G)}$, but 1 is irreducible modulo G with respect to right reductions; so G is not a RGB.

By way of contrast, the notion of reducibility is left-right symmetric:

LEMMA 4.2. *Let* $P \subseteq R$, $f \in R$. *Then* f *is left-reducible modulo* P *iff* f *is right-reducible modulo* P.

PROOF. Let $p \in P$, $t \in T(f)$; then $f \to f'(t)$ iff $HT(p)$ div t iff $f \xrightarrow{r} f'(t)$.

Accordingly, we may define $P \subseteq R$ to be *reduced* if all polynomials in P are monic and in (left and right) normal form modulo $P \backslash \{p\}$. As in the commutative case (see Buchberger, 1985, theorem 6.3), left or right reduced Gröbner bases are unique:

PROPOSITION 4.3. *Let* G, H *be reduced LGBs (reduced RGBs) and let* $I_L(G) = I_L(H)$, $(I_R(G) = I_R(H))$. *Then* $G = H$.

We omit the proof, since it is almost identical to that of theorem 4.4 below. Somewhat surprisingly, reduced Gröbner bases are also unique in the mixed left–right case:

THEOREM 4.4. *Let* G *be a reduced LGB,* H *a reduced RGB, and let* $I_L(G) = I_R(H)$. *Then* $G = H$.

PROOF. Assume for a contradiction that $G \Delta H = (G \backslash H) \cup (H \backslash G) \neq \emptyset$, and let f be minimal in $G \Delta H$. By symmetry, we may assume that $f \in G \backslash H$. Since $f \in I_L(G) = I_R(H)$, $f \xrightarrow[H]{r*} 0$, say $f \xrightarrow[p]{r} f_1 \xrightarrow[H]{r*} 0$ for some $p \in H$. If $p < f$ then by the choice of f, $p \in G \cap H$, and so $p \neq f$, and so f is reducible modulo $G \backslash \{f\}$, a contradiction. So $p \gtrsim f$, and so $HM(f) = HM(p)$, and so $f_1 = f - p$. We claim that $f_1 = 0$, which yields the desired contradiction $f = p \in H$. For, otherwise $0 \neq f_1 \in I_L(G)$, and so $s = HT(f_1)$ is reducible modulo

$$G' = \{g \in G : g < f\} = H' = \{h \in H : h < f\}.$$

But then $s \in T(f)$ or $s \in T(p)$, and so f is reducible modulo G' or p is reducible modulo H', a contradiction.

Next, we prove the partial correctness of the algorithm LRED of section 2; termination of the algorithm is obvious by Dickson's lemma.

PROPOSITION 4.5. *Let* G *be a LGB in* R.

(1) *Let* $g, h \in G$, $t \in T(g)$ *be such that* $g \xrightarrow[h]{} g_1(t)$, *and let* $f \in R$ *be reducible modulo* G. *Then* f *is also reducible modulo* $(G \backslash \{g\}) \cup \{g_1\}$.

(2) *LRED(G) is a LGB.*

PROOF.

(2) Follows from (1) using lemma 3.8 (4).

(1) If f is reducible mod $G \backslash \{g\}$, there is nothing to prove; otherwise, f is reducible mod $\{g\}$. If $t < HT(g)$, then $HT(g_1) = HT(g)$, and so f is reducible mod $\{g_1\}$. If $t = HT(g)$, then $HT(h)$ div t, and so f is reducible mod $\{h\}$.

In contrast to example 4.1, we have the following result.

PROPOSITION 4.6. *Let* G *be LGB such that* $I_R(G) \subseteq I_L(G)$. *Then* G *is also a RGB.*

PROOF. By 3.8 (4), every $f \in I_R(G) \subseteq I_L(G)$ is (left- and hence right-) reducible modulo G. So by the right-hand analogue of 3.8, G is a RGB.

We close this section by a new proof of the fact that R is *Noetherian with respect to one-*

and two-sided ideals [see El From (1983); the proof there is based on Lesieur (1978)]. Our method is based on Dickson's lemma, and is well known in the commutative case (see Buchberger, 1985).

THEOREM 4.7. R *is left and right Noetherian and hence Noetherian.*

PROOF. We show that R is left-Noetherian. Let $\{f_n\}_{n\in\mathrm{N}}$ be a sequence of polynomials in R, let $\mathrm{I}_n=\mathrm{I_L}(\{f_1,\ldots,f_n\})$, and assume for a contradiction that $f_{n+1}\notin \mathrm{I}_n$. Let f'_{n+1} be a normal form for f_{n+1} modulo $\{f_1,\ldots,f_n\}$ with respect to left reduction. Then $f'_{n+1}\neq 0$, since by lemma 3.3 $f_{n+1}-f'_{n+1}\in\mathrm{I_L}(\{f_1,\ldots,f_n\})$. Then for all $1\leqslant i\leqslant n$, not $\mathrm{HT}(f_i)\operatorname{div}\mathrm{HT}(f_{n+1})$, contradicting Dickson's lemma.

5. Two-sided Gröbner Bases

In this section, we show how to characterise and compute *Gröbner bases for two-sided ideals* from the left (or right) Gröbner bases obtained in sections 3 and 4. Instead of extending the reduction relation, we keep left (or right) reduction and introduce an additional closure condition for two-sided Gröbner bases. The apparent left–right asymmetry of this definition is resolved in theorem 5.4.

Throughout this section, $\mathrm{R}=\mathrm{K}\{X_1,\ldots,X_r\}$ is a polynomial ring of solvable type, "$\rightarrow$" denotes left reduction and "$\dashrightarrow$" right reduction. The following easy lemma characterises the coincidence of one- and two-sided ideals.

LEMMA 5.1. *Let* $\mathrm{P}\subseteq\mathrm{R}$. *Then the following are equivalent:*

(1) $\mathrm{I_R(P)}\subseteq\mathrm{I_L(P)}$;
(2) $\mathrm{I_L(P)}=\mathrm{I(P)}$;
(3) *For all* $s\in\mathrm{T}$, $p\in\mathrm{P}$, $p*s\in\mathrm{I_L(P)}$;
(4) *For all* $1\leqslant j\leqslant r$, $p\in\mathrm{P}$, $p*X_j\in\mathrm{I_L(P)}$.

A corresponding equivalence holds for $\mathrm{I_R(P)}$ *and* $\mathrm{I(P)}$.

PROOF.
(1)$\Rightarrow$(4) is trivial.
(4)$\Rightarrow$(3) uses induction on the length of s.
(3)$\Rightarrow$(2) and (2)$\Rightarrow$(1) follow from the fact that every $f\in\mathrm{I_R(P)}$ ($f\in\mathrm{I(P)}$) is a sum of products $p*s$ ($s*p*s'$) with $p\in\mathrm{P}$, $s,s'\in\mathrm{T}$.

The next lemma is well known in the commutative case (see Buchberger, 1985, problem 6.14, method 6.13).

LEMMA 5.2. *Let* G *be a left Gröbner basis in* R *and let* $0\neq f\in\mathrm{I_L(G)}$. *Then there exist* $a_i\in\mathrm{K}$, $s_i\in\mathrm{T}$, $p_i\in\mathrm{G}$ $(1\leqslant i\leqslant k)$ *such that* $f=\sum_{1\leqslant i\leqslant k} a_i*s_i*p_i$ *and* $s_i\cdot\mathrm{HT}(p_i)\leqslant\mathrm{HT}(f)$.

PROOF. By lemma 3.8, $f\xrightarrow[\mathrm{G}]{*}0$. We show the lemma by induction on k, where k is the number of reduction steps $f\xrightarrow[\mathrm{G}]{k}0$. If $k=1$, then $f=a*s*p$ for some $a\in\mathrm{K}$, $s\in\mathrm{T}$, $p\in\mathrm{G}$, and so by lemma 1.5, $\mathrm{HT}(f)=s\cdot\mathrm{HT}(p)$. For $k>1$, let $f\xrightarrow[\mathrm{G}]{}f_1\xrightarrow[\mathrm{G}]{k-1}0$, and let $f_1=f-a_k*s_k*p_k$ with $a_k\in\mathrm{K}$, $s_k\in\mathrm{T}$, $p_k\in\mathrm{G}$, $s_k\cdot\mathrm{HT}(p_k)\leqslant\mathrm{HT}(f)$. The claim follows now from the induction assumption applied to f_1.

As a consequence we can now improve lemma 5.1 for LGBs.

LEMMA 5.3. *Let* G *be a left Gröbner basis in* R. *Then* $I_L(G) = I(G)$ *implies* $I_R(G) = I(G)$.

PROOF. Assume for a contradiction that $A = I(G) \backslash I_R(G)$ is non-empty, and pick $f \in A$ minimal with respect to the quasi-ordering $<$ on R. Then $f \in I_L(G)$, and so by lemma 5.2 there exist $a_i \in K$, $s_i \in T$, $p_i \in G$ $(1 \leqslant i \leqslant k)$ such that $s_i \cdot HT(p_i) \leqslant HT(f)$ and $f = \sum_{1 \leqslant i \leqslant k} a_i * s_i * p_i$. Let $p_i' = s_i * p_i - p_i * s_i \in I(G)$. By lemma 1.5, $HT(s_i * p_i) = HT(p_i * s_i)$, and so $p_i' < HT(s_i * p_i) \leqslant HT(f)$. By the minimal choice of f, $p_i' \in I_R(G)$, and so $s_i * p_i = p_i' + p_i * s_i \in I_R(G)$, and so $f \in I_R(G)$. This contradicts the choice of f.

THEOREM 5.4. *Let* G *be a finite set of polynomials in* R. *Then the following assertions are equivalent.*

(1) G *is a LGB and* $I_L(G) = I_R(G)$.
(2) G *is a LGB and* $I_L(G) = I(G)$.
(3) *For all* $f, g \in R$ *with* $f - g \in I(G)$, $f \downarrow g$ *modulo* G.
(4) *For all* $f \in I(G)$, $f \overset{*}{\underset{G}{\to}} 0$.
(5) *For all* $0 \neq f \in I(G)$, f *is (left) reducible modulo* G.
(6) G *is a LGB and for all* $1 \leqslant i \leqslant r$, $p \in G$, $p * X_i \overset{*}{\underset{G}{\to}} 0$.
(7) *For all* $0 \neq f \in I(G)$, *there exists* $g \in G$ *such that* $HT(g)$ *div* $HT(f)$.
(1′) G *is a RGB and* $I_R(G) = I_L(G)$.
(2′) G *is a RGB and* $I_R(G) = I(G)$.
(3′) *For all* $f, g \in R$ *with* $f - g \in I(G)$, $f \downarrow' g$ *modulo* G.
(4′) *For all* $f \in I(G)$, $f \overset{\prime *}{\underset{G}{\to}} 0$.
(5′) *For all* $0 \neq f \in I(G)$, f *is (right) reducible modulo* G.
(6′) G *is a RGB and for all* $1 \leqslant i \leqslant r$, $p \in G$, $X_i * p \overset{\prime *}{\underset{G}{\to}} 0$.

PROOF. The equivalence between (1) and (2) follows from 5.3, the equivalence between (2), (3), (4), (5), (7) from 3.8, and the equivalence between (2) and (6) from 5.1. (1′)–(6′) are the right-hand analogues of (1)–(6), and hence also equivalent. Finally, (5) and (5′) are equivalent by 4.2. (Alternatively, one can argue that (7) is left–right symmetric or one may derive the equivalence of (1) and (1′) from 4.6.)

DEFINITION. A finite set G of polynomials in R is a *(two-sided) Gröbner basis (GB)*, if it satisfies the equivalent conditions of theorem 5.4. By these equivalences, the concept is completely left–right symmetric.

In order to show the partial correctness of the algorithm GRÖBNER, we take 5.4 (6) as a characterisation of Gröbner bases. When the algorithm terminates, G is obviously a LGB extending P and satisfying 5.4 (6). Termination is again guaranteed by Dickson's lemma.

The following proposition shows that reduced two-sided Gröbner bases can be obtained in the same fashion as reduced one-sided Gröbner bases by simply composing the algorithms GB and LRED (or GB and RRED). For a more efficient algorithm, one may intertwine both algorithms similar as in the commutative case (see Buchberger, 1985, 6.4).

PROPOSITION 5.5. *Let* G *be a* GB *in* R *and let* H = LRED(G). *Then* H *is a reduced* GB *in* R *with* $I(H) = I(G)$.

PROOF. By 4.5, H is a reduced LGB and $I_L(H) = I_L(G)$. So by 5.4, we have to show that

$I_L(H) = I(H)$. By definition of the algorithm LRED, it will suffice to show the following:

(*) If $P \subseteq R$ with $I_L(P) = I(P)$, $p, q \in P$, $p \neq q$,

$$p \xrightarrow[q]{} p' = p - c * s * q, \quad P' = (P \backslash \{p\}) \cup \{p'\},$$

then $I_L(P') = I(P')$.

Let $1 \leqslant i \leqslant r$; then $p * X_i \in I_L(P)$, $c * s * q * X_i \in I_L(P)$, and so

$$p' * X_i = p * X_i - c * s * q * X_i \in I_L(P),$$

say $p' * X_i = f * p + g$ with $f \in R$, $g \in I_L(P \backslash \{p\})$. So

$$p' * X_i = f * p' + f * s * q + g \in I_L(P').$$

By lemma 5.1, this proves (*).

The computation of elimination ideals given in 3.13 works for two-sided ideals as well.

Proposition 5.6. *Let* $R = K\{X_1, \ldots, X_r\}$, $0 \leqslant m < r$, $R' = K\{X_1, \ldots, X_m\}$, *assume* T *is ordered pure lexicographically,* $X_1 < \ldots < X_r$, *let* G *be a (reduced) Gröbner basis in* R *with respect to* $<$, *and let* $G' = G \cap R'$. *Then* G' *is a (reduced) Gröbner basis in* R' *and* $I(G) \cap R' = I'(G')$, *where* I'(H) *denotes the two-sided ideal generated by* H *in* R'.

Proof. In order to prove that G' is a (reduced) Gröbner basis, it suffices by 3.13 and 5.4 to show that, for $1 \leqslant i \leqslant m$, $g \in G'$, $g * X_i \xrightarrow[G']{*} 0$; this follows as in the proof of 3.13 from the fact that $g * X_i \xrightarrow[G]{*} 0$.

Next, let $f \in I(G) \cap R'$. Then by 5.4 $f \xrightarrow[G]{*} 0$, and so $f \xrightarrow[G']{*} 0$, and so $f \in I'(G')$. The converse inclusion $I'(G') \subseteq I(G) \cap R'$ is obvious.

Finally we note the following facts:

(a) By 4.4 and 5.4 (2), reduced Gröbner bases are uniquely determined by the two-sided ideal they generate.

(b) For a GB G, the K-vector space R/I(G) has an explicit basis given by 3.14 (1); 3.14 (2) provides a method to decide whether R/I(G) is finite dimensional.

(c) By 3.12, a singleton $\{g\}$ R is a GB in R iff $I_L(g) = I_R(g)$.

Example: In $R = Q\{X, Y\}$ with $X < Y$, $\{X\}$ is a GB, if the commutation relation in R is $Y * X = X * Y + X$; if, however, this relation is $Y * X = X * Y + 1$, then $\{X\}$ is not a GB, since $1 = Y * X - X * Y$ is in $I(X)$. So in this case, $\{X\}$ is a LGB and a RGB, but not a GB.

6. The Word Problem in Algebras of Solvable Type

Let $R = K\{X_1, \ldots, X_n\}$ be a solvable polynomial ring over K, let I be a two-sided ideal in R, let $A = R/I$ and let $a_i = x_i + I$ for $1 \leqslant i \leqslant n$. Then we call A an *algebra of solvable type over* K, generated by $a_1, \ldots, a_n$. Since by theorem 4.7, R is Noetherian, I has a finite basis F. By section 5, one can construct a Gröbner basis G of I from F using the algorithm *GRÖBNER*.

Example. Let

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

be a quadratic form in $K[X_1, \ldots, X_n]$. Then $Q(X)$ determines a *Clifford algebra* C (see van der Waerden, 1967, section 93). We are going to show that any Clifford algebra C is in fact an algebra of solvable type: Let

$$R = K\{X_1, \ldots, X_n\} = K\langle X_1, \ldots, X_n\rangle / I(Q'),$$

where Q′ is the commutation system

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

Then by 1.9 (3), Q′ satisfies hypothesis (H), and so R is indeed a polynomial ring of solvable type. Next, let I be the two-sided ideal in R generated by $P = \{X_i^2 - q_i : 1 \leqslant i \leqslant n\}$. It is not difficult to verify that P is a two-sided Gröbner basis in R. So $f \in R$ is in normal form modulo $\xrightarrow[P]{}$ iff f is at most linear in each X_i, $1 \leqslant i \leqslant n$. This shows that R/I is in fact the Clifford algebra determined by Q. Taking Q as the zero form, this shows in particular, that any Grassmann algebra (see van der Waerden, 1967, section 93) is an algebra of solvable type.

The results of the previous sections can now be applied to solve the word problem in A and the membership problem for one- and two-sided ideals in A.

The *word problem* in A asks for a method to decide, whether for a given polynomial $f(X_1, \ldots, X_n)$ in R, $f(a_1, \ldots, a_n) = 0$ in A. A solution is obtained as follows. Reduce f to its normal form $f^{\sim}$ with respect to G. Then $f(a_1, \ldots, a_n) = 0$ iff $f(X_1, \ldots, X_n) \in I$ iff $f^{\sim}(X_1, \ldots, X_n) = 0$.

Then *ideal membership problem* in A can be treated in the same manner. Given a two-sided (left, right) ideal $J \subseteq A$ with finite basis F′, construct a (left, right) Gröbner basis G′ of I+J from $G \cup F'$, and let $f^{\sim}$ be a (left, right) normal form of f with respect to G′. Then $f(a_1, \ldots, a_n) \in J$ iff $f^{\sim} = 0$.

As in the commutative case, the algorithms solving these problems split into two parts. First, the computation of a suitable Gröbner basis; then the reduction of the given polynomial to its normal form with respect to this Gröbner basis. For a fixed polynomial ring R of solvable type and fixed ideals I, J the first part may be regarded as a preprocessing step of potentially high complexity. [Even in the commutative case, the ideal membership problem is exponential space hard (see Mayr & Meyer, 1982; Buchberger, 1976, and corollary 6.2 below).] The second step—reduction of an input polynomial modulo the Gröbner basis—is then quite fast. For non-commutative R, another preprocessing step is required beforehand. The inductive computation of a list of products $s * t$ of terms up to a degree to be estimated; if higher products occur in the subsequent steps, this list has to be enlarged as necessary.

The algorithms of section 2 have been implemented in the Aldes/SAC-2 Distributive Polynomial System by Kredel (see Gebauer & Kredel, 1983). With his kind permission, we here present a sample of the results obtained by this system.

$R = \mathbb{Q}\{A, X, Y\}$, where T is ordered pure lexicographically, $A < X < Y$. The commutation relations are $Y * X = X * Y + A$, $X * A = A * X$, $Y * A = A * Y$. Input polynomials are $F = \{Y^3 - 2AX - A, X^2 + A\}$. F is verified by the system to be left-reduced in 0·03 s using the list of products $(Y * X, Y * X^2)$. A left Gröbner basis G for F is obtained in 1·47 s using the list of products $(Y * X, Y * X^2, Y^2 * X, Y^2 * X^2, Y^3 * X^2)$.

$$G = \{Y^3 + X^2Y + XY, X^2 + X, AXY^2 + \tfrac{1}{2}AY^2 + A^2Y, AY^2 - 12A^2XY - 6A^2Y - 8A^3,$$
$$A^2Y - 4A^3X - 2A^3, A^3X + \tfrac{1}{2}A^3, A^3, A^2X + \tfrac{1}{2}A^2, A^2\}.$$

From G, the reduced left Gröbner basis G′ of F is obtained in 1·47 s using the same list of products, $G' = \{A^2, X^2+X, AY^2, Y^3-2AX-A\}$. Finally, the reduced two-sided Gröbner basis G″ of F is obtained in 1·93 s using again the same list of products, $G'' = \{A, X^2+X, Y^3\}$. (All computing times on IBM 9370 under VM/CMS.)

We close this section with a uniform proof for the facts that the ideal membership problem for commutative polynomial rings over fields is EXPSPACE-hard and that this problem for general non-commutative polynomial rings over fields is undecidable.

Let K be a field, let $s_i(X_1, \dots, X_n)$, $t_i(X_1, \dots, X_n)$, $0 \leqslant i \leqslant m$, be (commutative) words in $X_1, \dots, X_n$, regarded as elements of the free (commutative) monoid generated by $X_1, \dots, X_n$, or of the (commutative) polynomial ring $S = K\langle X_1, \dots, X_n\rangle(K[X_1, \dots, X_n])$ over K. We let I denote the two-sided ideal in S generated by $s_1 - t_1, \dots, s_m - t_m$. Then the following proposition was proved for the commutative case by two different methods in Eilenberg & Schutzenberger (1969) and Mayr & Meyer (1982).

Proposition 6.1. *The implication* $s_1 = t_1 \wedge \dots \wedge s_m = t_m \to s_0 = t_0$ *holds in all (commutative) monoids iff* $s_0 = t_0 \in I$.

Our proof is adapted from Eilenberg & Schutzenberger (1969, p. 187).

"⇒": Let R = S/I, and denote the residues of X_i modulo I by x_i. Then $s_i(x) = t_i(x)$ in R for $1 \leqslant i \leqslant m$, and so $s_0(x) = t_0(x)$, and so $s_0(x) - t_0(x) \in I$.

"⇐": Suppose M is a (commutative) monoid containing elements $a_1, \dots, a_n$ such that $s_i(a) = t_i(a)$ for $1 \leqslant i \leqslant m$, but $s_0(a) \neq t_0(a)$. Form the monoid ring R = K[M], and recall that M is canonically embedded into R. Let $h: S \to R$ be the homomorphism of K-algebras mapping X_i onto a_i for $1 \leqslant i \leqslant N$, and let J be the kernel of h. Then $I \subseteq J$, but $s_0 - t_0 \notin J$, and so $s_0 - t_0 \notin I$.

Corollary 6.2 (Mayr & Meyer, 1982). *The ideal membership problem for* $K[X_1, \dots, X_n]$ *is EXPSPACE-hard.*

Proof. By Mayr & Meyer (1982) the word problem for commutative semigroups is EXPSPACE-hard. Since any (commutative) semigroup can be embedded into a (commutative) monoid, the same applies to commutative monoids. By 6.1, the word problem for (commutative) monoids is polynomial time reducible to the ideal membership problem for R.

Corollary 6.3. *For any ground field* K *and any* $n \geqslant 2$, *the membership problem for finitely generated two-sided ideals in* $K\langle X_1, \dots, X_n\rangle$ *is undecidable. In particular, there exists words* $s_i(X_1, X_2)$, $t_i(X_1 X_2)$ *in* $Q\langle X_1, X_2\rangle$ $(1 \leqslant i \leqslant 7)$, *such that the membership problem for the two-sided ideal generated by* $s_1 - t_1, \dots, s_7 - t_7$ *is undecidable.*

Proof. Post and Markov proved independently that the word problem for semigroups and hence for monoids is undecidable. Scott and Hall improved this result to the effect that there are seven explicitly constructible pairs of words (s_i, t_i) in the free monoid generated by X_1, X_2, such that the word problem specialised to these s_i, t_i $(1 \leqslant i \leqslant 7)$ is undecidable (see Boone, 1959). The corollary follows from this fact by 6.1.

7. Concluding Remarks

We have shown that Buchberger's method of computing Gröbner bases can be extended to solvable polynomial rings R over a field K. As a consequence, we have solved the word problem and ideal membership problem in all algebras arising as quotients of R. This line of research is continued in Weispfenning (1988) by a construction of Gröbner bases in solvable polynomial rings that are independent of a specific admissible order of the terms.

The results suggest some directions for further research.

(1) In the commutative case, Buchberger's algorithm has been extended to polynomial rings over Euclidean domains (see Kandri-Rody & Kapur, 1984*a*, *b*). A corresponding extension of our algorithms to solvable polynomials with hypothesis (H) over a Euclidean domain should be routine.

(2) The algorithms of section 2 should be improved in efficiency along the lines of the commutative case (see Buchberger, 1985, 6.4).

(3) In corollary 6.3, we have shown that the membership problem for finitely generated two-sided ideals in a non-commutative polynomial ring over e.g. the field of rationals is undecidable. *Question:* Where is the borderline between a decidable and an undecidable ideal membership problem in non-commutative polynomial rings? More precisely, determine the ideals I in $\mathrm{K}\langle X_1, \ldots, X_n\rangle$ such that I contains no commutative polynomial $\neq 0$ and such that $\mathrm{R} = \mathrm{K}\langle X_1, \ldots, X_n\rangle/\mathrm{I}$ has a decidable membership problem for finitely generated two-sided ideals.

The paper is the outcome of the collaboration of the authors in 1986 and 1987 at the University of Heidelberg and the Université Cadi Ayyad, Marrakech. We gratefully acknowledge financial support for the first author by a DAAD-research grant and for the second author by a DFG-Heisenberg grant.

References

Apel, J., Lassner, W. (1988). An extension of Buchberger's algorithm and calculations in enveloping fields of Lie Algebras. *J. Symbolic Comp.*, **6**, 361–370.

Bergmann, G. M. (1978). The diamond lemma in ring theory. *Adv. Math.* **29**, 178–218.

Boone, W. W. (1959). The word problem. *Ann. Math.* **70**, 207–265.

Buchberger, B. (1976). Some properties of Gröbner bases for polynomial ideals. *ACM SIGSAM Bull.* **10**, (4), 19–24.

Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In *Recent Trends in Multidimensional Systems* (N. K. Bose, ed.), chap. 6. Dordrecht: Reidel.

Dickson, L. E. (1913). Finiteness of the odd perfect and primitive abundant numbers with *n* distinct prime factors. *Amer. J. Math.* **35**, 413–426.

Dixmier, J. (1974). *Algèbres enveloppantes.* Paris: Gauthier-Villars.

Eilenberg, S., Schutzenberger, M. F. (1969). Rational sets in commutative monoids. *J. Algebra* **13**, 173–191.

El From, Y. (1983). Sur les algèbres de type résoluble. Thèse de 3e cycle, Univ. Paris 6.

Galligo, A. (1985). Some algorithmic questions on ideals of differential operators. *Proc. EUROCAL '85, Springer LNCS* **204**, 413–421.

Gebauer, R., Kredel, H. (1983). *Distributive Polynomial System.* Several Technical Reports, University of Heidelberg, Heidelberg, FRG.

Huet, G. (1980). Confluent reductions: Abstract properties and applications to term rewriting systems. *J. ACM* **27**, 797–821.

Jacobson, N. (1962). *Lie Algebras.* New York: Dover.

Kandri-Rody, A., Kapur, D. (1984*a*). Algorithms for computing the Gröbner bases of polynomial ideals over various Euclidean rings. *Proc. EUROSAM '84, Springer LNCS* **174**, 195–205.

Kandri-Rody, A., Kapur, D. (1984*b*). An algorithm for computing the Gröbner basis of a polynomial ideal over a Euclidean ring. *GE CRD Report 84CRD045*, see also (1988), *J. Symb. Comp.* **6**, 37–58.

Lassner, W. (1985). Symbol representation of non-commutative algebras. *Proc. EUROCAL '85, Springer LNCS* **204**, 99–115.

Lesieur, L. (1978). Conditions Noéthériennes dans l'anneau de polynomes de Ore A[X, σ, δ], Séminaire d'algèbre P. Dubreil, Paris 1977–78. *Springer LNM* **641**, 220–234.

Mayr, E. W., Meyer, A. R. (1982). The complexity of the word problem for commutative semigroups and polynomial ideals. *Adv. Math.* **46**, 305–329.

Mora, F. (1986). Gröbner bases for non-commutative polynomial rings. *Proc. AAECC-3, Springer LNCS* **229**, 353–362.

Ore, O. (1933). Theory of non-commutative polynomials. *Ann. Math.* **34**, 480–508.

van der Waerden, B. L. (1967). *Algebra*, 5th edn. Berlin: Springer.

Weispfenning, V. (1988). Constructing universal Gröbner bases. *Proc. AAECC-5, LNCS* **356**, 408–417. Berlin: Springer.

Winkler, F., Buchberger, B., Lichtenberger, F., Rolletschek, H. (1985). An algorithm for constructing canonical bases of polynomial ideals. *ACM/TOMS* **11**, 66–78.