AAECC manuscript No.
(will be inserted by the editor)

A Combinatorial Approach to Involution and δ-Regularity I: Involutive Bases in Polynomial Algebras of Solvable Type

Werner M. Seiler

AG "Computational Mathematics", Universität Kassel, 34132 Kassel, Germany
www.mathematik.uni-kassel.de/~seiler
e-mail: seiler@mathematik.uni-kassel.de

Received: date / Revised version: date

Abstract Involutive bases are a special form of non-reduced Gröbner bases with additional combinatorial properties. Their origin lies in the Janet-Riquier theory of linear systems of partial differential equations. We study them for a rather general class of polynomial algebras including also non-commutative algebras like those generated by linear differential and difference operators or universal enveloping algebras of (finite-dimensional) Lie algebras. We review their basic properties using the novel concept of a weak involutive basis and present concrete algorithms for their construction. As new original results, we develop a theory for involutive bases with respect to semigroup orders (as they appear in local computations) and over coefficient rings, respectively. In both cases it turns out that generally only weak involutive bases exist.

1 Introduction

In the late 19th and early 20th century a number of French mathematicians developed what is nowadays called the Janet-Riquier theory of differential equations [37–39,47,53,57,58]. It is a theory for general systems of differential equations, i. e. also for under- and overdetermined systems, and provides in particular a concrete algorithm for the completion to a so-called passive[1] system. In recent times, interest in the theory has been rekindled mainly in the context of Lie symmetry analysis, so that a number of references to modern works and implementations are contained in the review [36].

The defining property of passive systems is that they do not generate any non-trivial integrability conditions. As the precise definition of passivity requires the introduction of a ranking on the set of all derivatives and as every linear system

[1] Sometimes the equivalent term "involutive" is used which seems to go back to Lie.

of partial differential equations with constant coefficients bijectively corresponds to a polynomial submodule, it appears natural to relate this theory to the algebraic theory of Gröbner bases [1,6].

Essentially, the Janet-Riquier theory in its original form lacks only the concept of reduction to a normal form; otherwise it contains all the ingredients of Gröbner bases. Somewhat surprisingly, a rigorous links has been established only fairly recently first by Wu [61] and then by Gerdt and collaborators who introduced a special form of non-reduced Gröbner bases for polynomial ideals [20,21,62], the *involutive bases* (Wu's "well-behaved bases" correspond to Thomas bases in the language of [20]). A slightly different approach to involutive bases has been proposed by Apel [4]; it will not be used here.

The fundamental idea behind involutive bases (originating in the pioneering work of Janet [37,38]) is to assign to each generator in a basis a subset of all variables: its multiplicative variables. This assignment is called an involutive division, as it corresponds to a restriction of the usual divisibility relation of terms. We only permit to multiply each generator by polynomials in its multiplicative variables. This restriction makes the involutive standard representation unique and leads to additional combinatorial properties not shared by ordinary Gröbner bases.

Like Gröbner bases, involutive bases can be defined in many non-commutative algebras. We will work with a generalisation of the polynomial algebras of solvable type introduced by Kandry-Rodi and Weispfenning [41]. It is essentially equivalent to the generalisation discussed by Kredel [42] or to the G-algebras considered by Apel [2] and Levandovskyy [44,45]. In contrast to some of these works, we explicitly permit that the variables act on the coefficients, so that, say, linear differential operators with *variable* coefficients form a polynomial algebra of solvable type in our sense. Thus our framework automatically includes the work of Gerdt [18] on involutive bases for linear differential equations as a particular case.

This article is the first of two parts. It reviews the basic theory of involutive bases immediately in the framework of polynomial algebras of solvable type, as it appears to be the most natural setting. Indeed, we would like to stress that in our opinion the core of the involutive bases theory is the monomial theory (in fact, we will formulate it in the language of multi indices or exponent vectors, i. e. in the Abelian monoid $(\mathbb{N}_0^n, +)$, in order to avoid problems with non-commuting variables) and the subsequent extension to polynomials requires only straightforward normal form considerations.

While much of the presented material may already be found scattered in the literature (though not always in the generality presented here and sometimes with incorrect proofs), the article also contains original material. Compared to Gerdt and Blinkov [20], we give an alternative definition of involutive bases which naturally leads to the new notion of a *weak* involutive basis. While these weak bases are insufficient for the applications studied in Part II, they extend the applicability of the involutive completion algorithm to situations not covered before.

The main emphasis in the literature on involutive bases is on optimising the simple completion algorithm of Section 7 and on providing fast implementations; as the experiments reported in [23] demonstrate, the results have been striking. We will, however, ignore this rather technical topic and instead study in Part II a num-

ber of applications of involutive bases (mainly Pommaret bases) in the structure analysis of polynomial modules. Note, however, that in these applications we will restrict to the ordinary commutative polynomial ring.

This first part is organised as follows. The next section defines involutive divisions and bases within the Abelian monoid $(\mathbb{N}_0^n, +)$ of multi indices. It also introduces the two most important divisions named after Janet and Pommaret, respectively. Section 3 introduces the here used concept of polynomial algebras of solvable type. As the question whether Hilbert's Basis Theorem remains valid is non-trivial if the coefficients form only a ring and not a field, Section 4 collects some results on this problem. The following three sections define (weak) involutive bases and give concrete algorithms for their construction.

The next four sections study some generalisations of the basic theory. Section 8 analyses the relation between left and right ideals in polynomial algebras of solvable type and the computation of bases for two-sided ideals; this extension requires only a straightforward adaption of classical Gröbner basis theory. The following three sections contain original results. The first two ones generalise to semigroup orders and study the use of the Mora normal form. Finally, Section 11 considers involutive bases over rings. It turns out that in these more general situations usually only weak bases exist.

In a short appendix we fix our conventions for term orders which are inverse to the ones found in most textbooks on Gröbner bases. We also mention an elementary property of the degree reverse lexicographic term order that makes it particularly natural for Pommaret bases.

2 Involutive Divisions

We study the Abelian monoid $(\mathbb{N}_0^n, +)$ with the addition defined componentwise and call its elements *multi indices*. They may be identified in a natural way with the vertices of an n-dimensional integer lattice, so that we can easily visualise subsets of $\mathbb{N}_0^n$. For a multi index $\nu \in \mathbb{N}_0^n$ we introduce its *cone* $\mathcal{C}(\nu) = \nu + \mathbb{N}_0^n$, i. e. the set of all multi indices that can be reached from ν by adding another multi index. We say that ν *divides* μ, written $\nu \mid \mu$, if $\mu \in \mathcal{C}(\nu)$. Given a finite subset $\mathcal{N} \subset \mathbb{N}_0^n$, we define its *span* as the monoid ideal generated by $\mathcal{N}$:

$$\langle \mathcal{N} \rangle = \bigcup_{\nu \in \mathcal{N}} \mathcal{C}(\nu) \; . \tag{1}$$

The basic idea of an involutive division is to introduce a restriction of the cone of a multi index, the involutive cone: it is only allowed to add multi indices certain entries of which vanish. This is equivalent to a restriction of the above defined divisibility relation. The final goal will be having a *disjoint* union in (1) by using only these involutive cones on the right hand side. This point of view will naturally lead to the combinatorial decompositions discussed in Part II.

In order to finally give the definition of an involutive division, we need one more notation: let $N \subseteq \{1, \ldots, n\}$ be an arbitrary subset of the set of the first n integers; then we write $\mathbb{N}_N^n = \left\{\nu \in \mathbb{N}_0^n \mid \forall j \notin N : \nu_j = 0\right\}$ for the set of

all multi indices where the only entries which may be non-zero are those whose positions are contained in N.

Definition 2.1 ([20, Def. 3.2]) *An* involutive division L *is defined on the Abelian monoid* $(\mathbb{N}_0^n, +)$*, if for any finite set* $\mathcal{N} \subset \mathbb{N}_0^n$ *a subset* $N_{L,\mathcal{N}}(\nu) \subseteq \{1, \ldots, n\}$ *of* multiplicative indices *is associated to every multi index* $\nu \in \mathcal{N}$ *such that the* involutive cones $\mathcal{C}_{L,\mathcal{N}}(\nu) = \nu + \mathbb{N}^n_{N_{L,\mathcal{N}}(\nu)}$ *satisfy the following two conditions.*

1. *If there exist two elements* $\mu, \nu \in \mathcal{N}$ *with* $\mathcal{C}_{L,\mathcal{N}}(\mu) \cap \mathcal{C}_{L,\mathcal{N}}(\nu) \neq \emptyset$*, either* $\mathcal{C}_{L,\mathcal{N}}(\mu) \subseteq \mathcal{C}_{L,\mathcal{N}}(\nu)$ *or* $\mathcal{C}_{L,\mathcal{N}}(\nu) \subseteq \mathcal{C}_{L,\mathcal{N}}(\mu)$ *holds.*
2. *If* $\mathcal{N}' \subset \mathcal{N}$*, then* $N_{L,\mathcal{N}}(\nu) \subseteq N_{L,\mathcal{N}'}(\nu)$ *for all* $\nu \in \mathcal{N}'$*.*

An arbitrary multi index $\mu \in \mathbb{N}_0^n$ *is* involutively divisible *by* $\nu \in \mathcal{N}$*, written* $\nu \,|_{L,\mathcal{N}}\, \mu$*, if* $\mu \in \mathcal{C}_{L,\mathcal{N}}(\nu)$*.*

It is important to note that involutive divisibility is always defined with respect to both an involutive division L and a fixed finite set $\mathcal{N} \subset \mathbb{N}_0^n$: only an element of $\mathcal{N}$ can be an involutive divisor. Obviously, involutive divisibility $\nu \,|_{L,\mathcal{N}}\, \mu$ implies ordinary divisibility $\nu \mid \mu$, since the involutive cone $\mathcal{C}_{L,\mathcal{N}}(\nu)$ is a subset of the full cone $\mathcal{C}(\nu)$. The first condition in the above definition says that involutive cones can intersect only trivially: if two intersect, one must be a subset of the other.

The *non-multiplicative indices* form the complement of $N_{L,\mathcal{N}}(\nu)$ in $\{1, \ldots, n\}$ and are denoted by $\bar{N}_{L,\mathcal{N}}(\nu)$. If we remove some elements from the set $\mathcal{N}$ and determine the multiplicative indices of the remaining elements with respect to the subset $\mathcal{N}'$, we obtain in general a different result than before. The second condition for an involutive division says that while it may happen that a non-multiplicative index becomes multiplicative for some $\nu \in \mathcal{N}'$, the converse cannot happen.

Example 2.2 A classical involutive division is the *Janet division* J. In order to define it, we must introduce certain subsets of the given set $\mathcal{N} \subset \mathbb{N}_0^n$:

$$(d_k, \ldots, d_n) = \left\{ \nu \in \mathcal{N} \mid \nu_i = d_i\,,\ k \leq i \leq n \right\}. \tag{2}$$

The index n is multiplicative for $\nu \in \mathcal{N}$, if $\nu_n = \max_{\mu \in \mathcal{N}} \{\mu_n\}$, and $k < n$ is multiplicative for $\nu \in (d_{k+1}, \ldots, d_n)$, if $\nu_k = \max_{\mu \in (d_{k+1}, \ldots, d_n)} \{\mu_k\}$.

Obviously, this definition depends on the ordering of the variables $x_1, \ldots, x_n$ and we obtain variants by applying an arbitrary but fixed permutation $\pi \in S_n$ to the variables. In fact, Gerdt and Blinkov [20] use an "inverse" definition, i. e. they first apply the permutation $\begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \cdots & 1 \end{pmatrix}$. Our convention is the original one of Janet [39, pp. 16–17].

Gerdt et al. [22] designed a special data structure, the Janet tree, for the fast determination of Janet multiplicative indices and for a number of other operations useful in the construction of Janet bases (Blinkov [10] discusses similar tree structures also for other divisions). As shown in [32], this data structure is based on a special relation between the Janet division and the lexicographic term order (see the appendix for our non-standard conventions). This relation allows us to compute very quickly the multiplicative variables of any set $\mathcal{N}$ with Algorithm 1. The algorithm simply runs two pointers over the lexicographically ordered set $\mathcal{N}$ and changes accordingly the set $\mathcal{M}$ of potential multiplicative indices. $\lhd$

Algorithm 1 Multiplicative variables for the Janet division

Input: finite list $\mathcal{N} = \{\nu^{(1)}, \ldots, \nu^{(k)}\}$ of pairwise different multi indices from $\mathbb{N}_0^n$
Output: list $N = \big(N_{J,\mathcal{N}}(\nu^{(1)}), \ldots, N_{J,\mathcal{N}}(\nu^{(k)})\big)$ of lists with multiplicative variables
/1/ $\mathcal{N} \leftarrow \mathtt{sort}(\mathcal{N}, \prec_{\mathrm{lex}})$; $\nu \leftarrow \mathcal{N}[1]$
/2/ $p_1 \leftarrow n$; $\mathcal{M} \leftarrow \{1, \ldots, n\}$; $N[1] \leftarrow \mathcal{M}$
/3/ **for** j **from** 2 **to** $|\mathcal{N}|$ **do**
/4/ $p_2 \leftarrow \mathtt{max}\big\{i \mid (\nu - \mathcal{N}[j])_i \neq 0\big\}$; $\mathcal{M} \leftarrow \mathcal{M} \setminus \{p_2\}$
/5/ **if** $p_1 < p_2$ **then**
/6/ $\mathcal{M} \leftarrow \mathcal{M} \cup \{p_1, \ldots, p_2 - 1\}$
/7/ **end_if**
/8/ $N[j] \leftarrow \mathcal{M}$; $\nu \leftarrow \mathcal{N}[j]$; $p_1 \leftarrow p_2$
/9/ **end_for**
/10/ **return** N

Definition 2.3 ([21, Def. 2.2]) *The division L is* globally defined, *if the assignment of the multiplicative indices is independent of the set $\mathcal{N}$; in this case we write simply $N_L(\nu)$ for the sets of multiplicative variables.*

Example 2.4 Another very important division is the *Pommaret*[2] *division* P. It assigns the multiplicative indices according to a simple rule: if $1 \leq k \leq n$ is the smallest index such that $\nu_k > 0$ for some multi index $\nu \in \mathbb{N}_0^n \setminus \{[0, \ldots, 0]\}$, then we call k the *class* of ν, written $\mathrm{cls}\,\nu$, and set $N_P(\nu) = \{1, \ldots, k\}$. Finally, we define $N_P([0, \ldots, 0]) = \{1, \ldots, n\}$. Hence P is globally defined. Like the Janet division, it depends on the ordering of the variables $x_1, \ldots, x_n$ and thus one may again introduce simple variants by applying a permutation.

Above we have seen that the Janet division is in a certain sense related to the inverse lexicographic order. The Pommaret division has a special relation to class respecting orders (recall that according to Lemma A.1 any class respecting term order coincides on terms of the same degree with the reverse lexicographic order). Obviously, for homogeneous polynomials such orders always lead to maximal sets of multiplicative indices and thus to smaller bases. But we will also see in Part II that from a theoretical point of view Pommaret bases with respect to such an order are particularly useful. $\lhd$

Definition 2.5 *The* involutive span *of a finite set $\mathcal{N} \subset \mathbb{N}_0^n$ is*

$$\langle \mathcal{N} \rangle_L = \bigcup_{\nu \in \mathcal{N}} \mathcal{C}_{\mathcal{N},L}(\nu) \; . \tag{3}$$

The set $\mathcal{N}$ is weakly involutive *for the division L or a* weak involutive basis *of the monoid ideal $\langle \mathcal{N} \rangle$, if $\langle \mathcal{N} \rangle_L = \langle \mathcal{N} \rangle$. A weak involutive basis is a* strong involutive basis *or for short an* involutive basis, *if the union on the right hand side of (3) is disjoint, i. e. the intersections of the involutive cones are empty. We call any finite set $\mathcal{N} \subseteq \bar{\mathcal{N}} \subset \mathbb{N}_0^n$ such that $\langle \bar{\mathcal{N}} \rangle_L = \langle \mathcal{N} \rangle$ a* (weak) involutive completion *of $\mathcal{N}$. An* obstruction to involution *for the set $\mathcal{N}$ is a multi index $\nu \in \langle \mathcal{N} \rangle \setminus \langle \mathcal{N} \rangle_L$.*

[2] Historically seen, the terminology "Pommaret division" is a misnomer, as this division was already introduced by Janet [37, p. 30]. However, the name has been generally accepted by now, so we stick to it.

This definition is essentially equivalent to [20, Def. 4.1/2/3]. However, the distinction of weak and strong bases is new and will become important in the sequel. What Gerdt and Blinkov [20, Def. 4.1] call "involutive" corresponds to our notion of "weakly involutive."

Remark 2.6 An obvious necessary condition for a strong involutive basis is that no distinct multi indices $\mu, \nu \in \mathcal{N}$ exist such that $\mu \,|_{L,\mathcal{N}}\, \nu$. Sets with this property are called *involutively autoreduced* [20, Def. 3.8]. One easily checks that the definition of the Janet division implies that $\mathcal{C}_{\mathcal{N},J}(\mu) \cap \mathcal{C}_{\mathcal{N},L}(\nu) = \emptyset$ whenever $\mu \neq \nu$. Hence for this particular division any set is involutively autoreduced. ◁

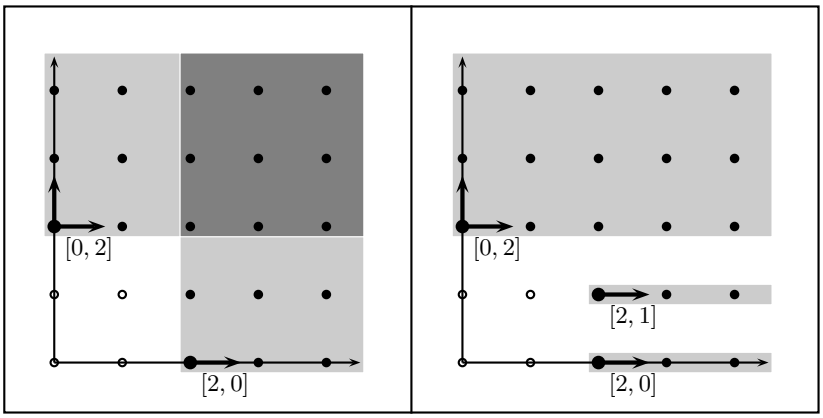

Fig. 1 *Left:* intersecting cones. *Right:* involutive cones.

Example 2.7 Figure 1 demonstrates the geometric interpretation of involutive divisions for $n = 2$. In both diagrams one can see the monoid ideal generated by the set $\mathcal{N} = \big\{[0,2],[2,0]\big\}$; the vertices belonging to it are marked by dark points. The arrows represent the multiplicative indices, i. e. the "allowed directions", for both the Janet and the Pommaret division, as they coincide for this example. The left diagram shows that the full cones of the two elements of $\mathcal{N}$ intersect in the darkly shaded area and that $\mathcal{N}$ is not (weakly) involutive, as the multi indices $[k,1]$ with $k \geq 2$ are obstructions to involution. The right diagram shows a strong involutive basis of $\langle\mathcal{N}\rangle$ for both the Janet and the Pommaret division. We must add to $\mathcal{N}$ the multi index $[2,1]$ and both for it and for $[2,0]$ only the index 1 is multiplicative. One clearly sees how the span $\langle\mathcal{N}\rangle$ is decomposed into three disjoint involutive cones: one of dimension 2, two of dimension 1. ◁

Proposition 2.8 *If $\mathcal{N}$ is a weakly involutive set, then a subset $\mathcal{N}' \subseteq \mathcal{N}$ exists such that $\mathcal{N}'$ is a strong involutive basis of $\langle\mathcal{N}\rangle$.*

Proof This proposition represents a nice motivation for the two conditions in Definition 2.1 of an involutive division. If $\mathcal{N}$ is not yet a strong involutive basis, the

union in (3) is not disjoint and intersecting involutive cones exist. By the first condition, this implies that some cones are contained in other ones; no other form of intersection is possible. If we eliminate the tips of these cones from $\mathcal{N}$, we get a subset $\mathcal{N}' \subset \mathcal{N}$ which, by the second condition, has the same involutive span, as the remaining elements may only gain additional multiplicative indices. Thus after a finite number of such eliminations we arrive at a strong involutive basis. □

Remark 2.9 Let $\mathcal{I}_1, \mathcal{I}_2$ be two monoid ideals in $\mathbb{N}_0^n$ and $\mathcal{N}_1, \mathcal{N}_2$ (weak) involutive bases of them for some division L. In general, we cannot expect that $\mathcal{N}_1 \cup \mathcal{N}_2$ is again a weak involutive basis of the ideal $\mathcal{I}_1 + \mathcal{I}_2$, as the involutive cones of the generators may shrink when taken with respect to the larger set $\mathcal{N}_1 \cup \mathcal{N}_2$. Only for a global division we always obtain at least a weak involutive basis (which may then be reduced to a strong basis according to Proposition 2.8). ◁

Recall that for arbitrary monoid ideals a basis $\mathcal{N}$ is called *minimal*, if it is not possible to remove an element of $\mathcal{N}$ without losing the property that we have a basis. A similar notion can be naturally introduced for involutive bases.

Definition 2.10 ([21, Def. 4.2]) *Let $\mathcal{I} \subseteq \mathbb{N}_0^n$ be a monoid ideal and L an involutive division. An involutive basis $\mathcal{N}$ of $\mathcal{I}$ with respect to L is called* minimal, *if any other involutive basis $\mathcal{N}'$ of $\mathcal{I}$ with respect to L satisfies $\mathcal{N} \subseteq \mathcal{N}'$.*

Obviously, the minimal involutive basis of a monoid ideal is unique, if it exists. For globally defined divisions, it is straightforward to show that any involutive basis is unique.

Proposition 2.11 ([21, Prop. 4.1]) *If the monoid ideal $\mathcal{I}$ has an involutive basis for the globally defined division L, then it is unique and thus minimal.*

The algorithmic construction of (weak) involutive completions for a given set $\mathcal{N} \subset \mathbb{N}_0^n$ will be discussed in detail in Section 6. For the moment we only note that we cannot expect that for an arbitrary set $\mathcal{N}$ and an arbitrary involutive division L an involutive basis $\mathcal{N}'$ of $\langle \mathcal{N} \rangle$ exists.

Example 2.12 We consider the set $\mathcal{N} = \big\{[1,1]\big\}$ for the Pommaret division. As $\operatorname{cls}[1,1] = 1$, we get $N_P([1,1]) = \{1\}$. So $\mathcal{C}_P([1,1]) \subsetneq \mathcal{C}([1,1])$. But any multi index contained in $\langle \mathcal{N} \rangle$ also has class 1. Hence no *finite* involutive basis of $\langle \mathcal{N} \rangle$ exists for the Pommaret division. We can generate it involutively only with the infinite set $\big\{[1,k] \mid k \in \mathbb{N}\big\}$. ◁

Remark 2.13 Since by definition an involutive basis is always finite, it does not really make sense to say that an infinite set involutively generates some monoid ideal. Ignoring this inconsistency for a moment, we now show that even if a monoid ideal does not possess a finite Pommaret basis, it has at least an infinite Pommaret basis with so much structure that it admits a simple finite description generalising the one found in the example above.

In order to see this fact, we consider first the case of an *irreducible* monoid ideal $\mathcal{I}$ in $\mathbb{N}_0^n$. It is well-known that any such $\mathcal{I}$ has a minimal basis of the form

$\{(\ell_1)_{i_1}, \ldots, (\ell_k)_{i_k}\}$ with $1 \leq k \leq n$, $\ell_j > 0$ and $1 \leq i_1 < \cdots < i_k \leq n$. Here $(\ell_j)_{i_j}$ is the multi index where all entries are zero except of the i_jth one which has the value ℓ_j. Such an ideal possesses a Pommaret basis, if and only if there are no "gaps" in the sequence $i_1 < \cdots < i_k \leq n$, i. e. $i_k = n$ and $i_1 = n-k+1$. Indeed, if a gap exists, say between i_j and i_{j+1}, then any Pommaret basis must contain the infinitely many multi indices of the form $(\ell_j)_{i_j} + (\ell)_{i_j+1}$ with $\ell > 0$ and thus cannot be finite (obviously, in this case a simple renumbering of the variables suffices to remedy this problem). Conversely, if no gaps appear, then it is easy to see that the set of all multi indices $[0, \ldots, 0, \ell_{i_j}, \mu_{i_j+1}, \ldots, \mu_n]$ with $1 \leq j \leq k$ and $0 \leq \mu_i < \ell_{n-k+i}$ is a strong Pommaret basis of $\mathcal{I}$.

For a general monoid ideal $\mathcal{I}$, we exploit that any monoid ideal in $\mathbb{N}_0^n$ possesses a unique irreducible decomposition [48, Thm. 5.27], i. e. we can always express $\mathcal{I}$ as the intersection of finitely many irreducible ideals. In Remark 6.5 we will show how a Pommaret basis of the intersection of two (monoid) ideals can be obtained from Pommaret bases of the ideals by simply taking least common multiples.

As a simple corollary of these considerations, we find that any Artinian monoid ideal $\mathcal{I}$ has a finite Pommaret basis. Indeed, $\mathcal{I}$ is Artinian, if and only if it contains an irreducible ideal $\mathcal{J}$ with a minimal basis $\{(\ell_1)_1, \ldots, (\ell_n)_n\}$. As no gaps appear, $\mathcal{J}$ possesses a finite Pommaret basis $\mathcal{B}'$. Now the finite set $\mathcal{B} = \mathcal{B}' \cup (\mathcal{I} \setminus \mathcal{J})$ is trivially a weak Pommaret basis of $\mathcal{I}$. ◁

Definition 2.14 ([20, Def. 4.3]) *An involutive division L is* Noetherian, *if any finite subset $\mathcal{N} \subset \mathbb{N}_0^n$ possesses a finite involutive completion with respect to L.*

Lemma 2.15 ([20, Prop. 4.5]) *The Janet division is Noetherian.*

In fact, it is straightforward to provide explicitly a Janet basis for any monoid ideal $\mathcal{I}$ given a finite generating set $\mathcal{N} \subset \mathbb{N}_0^n$ of it: if we introduce the multi index $\mu = \operatorname{lcm}\mathcal{N}$, i. e. $\mu_i = \max_{\nu \in \mathcal{N}} \nu_i$, then the set

$$\bar{\mathcal{N}} = \left\{ \bar{\nu} \in \langle \mathcal{N} \rangle \mid \mu \in \mathcal{C}(\bar{\nu}) \right\} \tag{4}$$

is an involutive J-completion of $\mathcal{N}$ (note that generally smaller Janet bases of $\mathcal{I}$ exist; thus this observation is only of theoretical interest).

3 Polynomial Algebras of Solvable Type

Let $\mathcal{P} = \mathcal{R}[x_1, \ldots, x_n]$ be a polynomial ring over a unitary ring $\mathcal{R}$. If $\mathcal{R}$ is commutative, then $\mathcal{P}$ is a unitary commutative ring with respect to the usual multiplication. We equip the $\mathcal{R}$-module $\mathcal{P}$ with alternative multiplications, in particular with non-commutative ones. We allow that both the variables x_i do not commute any more and that they operate on the coefficients. The usual multiplication is denoted either by a dot $\cdot$ or by no symbol at all. Alternative multiplications $\mathcal{P} \times \mathcal{P} \to \mathcal{P}$ are always written as $f \star g$.

Like Gröbner bases, involutive bases are always defined with respect to a *term order* $\prec$. It selects in each polynomial $f \in \mathcal{P}$ a *leading term* $\operatorname{lt}_\prec f = x^\mu$ with *leading exponent* $\operatorname{le}_\prec f = \mu$. The coefficient $r \in \mathcal{R}$ of x^μ in f is the *leading*

coefficient $\mathrm{lc}_\prec f$ and the product rx^μ is the *leading monomial* $\mathrm{lm}_\prec f$. Based on the leading exponents we associate to each finite set $\mathcal{F} \subset \mathcal{P}$ a set $\mathrm{le}_\prec \mathcal{F} \subset \mathbb{N}_0^n$ to which we may apply the theory developed in the previous section. But this approach makes sense only, if the multiplication $\star$ and the chosen term order are compatible to each other in the following sense.

Definition 3.1 $(\mathcal{P}, \star, \prec)$ *is a* polynomial algebra of solvable type *over the unitary coefficient ring* $\mathcal{R}$ *for the term order* $\prec$*, if the multiplication* $\star : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ *satisfies three axioms.*

(i) $(\mathcal{P}, \star)$ *is a ring with unit* 1.
(ii) $\forall r \in \mathcal{R},\ f \in \mathcal{P} :\ r \star f = rf$.
(iii) $\forall \mu, \nu \in \mathbb{N}_0^n,\ r \in \mathcal{R} \setminus \{0\} :\ \mathrm{le}_\prec (x^\mu \star x^\nu) = \mu + \nu \ \wedge\ \mathrm{le}_\prec (x^\mu \star r) = \mu$.

Condition (i) ensures that arithmetics in $(\mathcal{P}, \star, \prec)$ obeys the usual associative and distributive laws. Because of Condition (ii), $(\mathcal{P}, \star)$ is a left $\mathcal{R}$-module. We do not require that it is a right $\mathcal{R}$-module, as this would exclude the possibility that the variables x_i operate non-linearly on $\mathcal{R}$. Condition (iii) ensures the compatibility of the new multiplication $\star$ and the term order $\prec$; we say that the multiplication $\star$ *respects the term order* $\prec$. It implies the existence of injective maps $\rho_\mu : \mathcal{R} \to \mathcal{R}$, maps $h_\mu : \mathcal{R} \to \mathcal{P}$ with $\mathrm{le}_\prec \big(h_\mu(r)\big) \prec \mu$ for all $r \in \mathcal{R}$, coefficients $r_{\mu\nu} \in \mathcal{R} \setminus \{0\}$ and polynomials $h_{\mu\nu} \in \mathcal{P}$ with $\mathrm{le}_\prec h_{\mu\nu} \prec \mu + \nu$ such that

$$x^\mu \star r = \rho_\mu(r) x^\mu + h_\mu(r)\ , \tag{5a}$$
$$x^\mu \star x^\nu = r_{\mu\nu} x^{\mu+\nu} + h_{\mu\nu}\ . \tag{5b}$$

Lemma 3.2 *The maps* ρ_μ *and the coefficients* $r_{\mu\nu}$ *satisfy for arbitrary multi indices* $\mu, \nu, \lambda \in \mathbb{N}_0^n$ *and for arbitrary ring elements* $r \in \mathcal{R}$

$$\rho_\mu\big(\rho_\nu(r)\big) r_{\mu\nu} = r_{\mu\nu} \rho_{\mu+\nu}(r)\ , \tag{6a}$$
$$\rho_\mu(r_{\nu\lambda}) r_{\mu,\nu+\lambda} = r_{\mu\nu} r_{\mu+\nu,\lambda}\ . \tag{6b}$$

Furthermore, all maps ρ_μ *are ring endomorphisms.*

Proof The first assertion is a trivial consequence of the associativity of the multiplication $\star$. The equations correspond to the leading coefficients of the equalities $x^\mu \star (x^\nu \star r) = (x^\mu \star x^\nu) \star r$ and $x^\mu \star (x^\nu \star x^\lambda) = (x^\mu \star x^\nu) \star x^\lambda$, respectively. The second assertion follows mainly from Condition (i). □

Remark 3.3 The term "algebra of solvable type" was coined by Kandry-Rody and Weispfenning [41], when they studied Gröbner bases for non-commutative rings. Their definition is more restrictive than ours, as it does not allow that the terms operate on the coefficients and requires a stronger form of compatibility between the multiplication $\star$ and the term order $\prec$. It automatically implies that $\star$ respects $\prec$. For our purposes, the latter property is decisive and thus we have used it in Definition 3.1 instead of the more technical axioms in [41].

Kredel [42] generalised the work of Kandry-Rody and Weispfenning [41] and considered essentially the same class of algebras as defined here. Various variants

of it have appeared under different names in the literature. Popular is in particular the approach to consider the algebras as the quotient of a free tensor algebra by an appropriate quadratic ideal [2,45]; one speaks then of *G-algebras*. In most cases, the authors restrict to the case of a (skew) coefficient field and do not allow that the variables operate on the coefficients. The corresponding theory of Gröbner bases has been treated at many places in the literature; besides the already cited works we mention in particular [11–13,26] where the name *PBW algebra* is used (see below for an explanation of this terminology). ◁

If $\mathcal{R}$ is a (skew) field, then for arbitrary polynomials $f, g \in \mathcal{P}$ an element $r \in \mathcal{R} \setminus \{0\}$ and a polynomial $h \in \mathcal{P}$ satisfying $\mathrm{le}_\prec h \prec \mathrm{le}_\prec (f \cdot g)$ exist such that

$$f \star g = r\,(f \cdot g) + h\ . \tag{7}$$

Indeed, if $\mathrm{lm}_\prec f = ax^\mu$ and $\mathrm{lm}_\prec g = bx^\nu$, then a simple computation yields that r is the (unique) solution of the equation $a\rho_\mu(b)r_{\mu\nu} = rab$ and h is the difference $f \star g - r(f \cdot g)$. Under this assumption we may reformulate Condition (iii) as

(iii)' $\forall f, g \in \mathcal{P} : \mathrm{le}_\prec (f \star g) = \mathrm{le}_\prec f + \mathrm{le}_\prec g$.

The next result is a simple consequence of Condition (iii).

Proposition 3.4 *The product $\star$ is fixed, as soon as the following data are given: constants $r_{ij} \in \mathcal{R}\setminus\{0\}$, polynomials $h_{ij} \in \mathcal{P}$ and maps $\rho_i : \mathcal{R} \to \mathcal{R}$, $h_i : \mathcal{R} \to \mathcal{P}$ such that for $1 \leq i \leq n$*

$$x_i \star r = \rho_i(r)x_i + h_i(r)\ , \quad \forall r \in \mathcal{R}\ , \tag{8a}$$

$$x_i \star x_j = r_{ij}x_j \star x_i + h_{ij}\ , \quad \forall 1 \leq j < i\ . \tag{8b}$$

Of course, the data in Proposition 3.4 cannot be chosen arbitrarily. Besides the obvious conditions on the leading exponents of the polynomials h_{ij} and $h_i(r)$ imposed by Condition (iii), each map ρ_i must be an injective $\mathcal{R}$-endomorphism and each map h_i must satisfy $h_i(r+s) = h_i(r) + h_i(s)$ and a kind of pseudo-Leibniz rule $h_i(rs) = \rho_i(r)h_i(s) + h_i(r) \star s$. The associativity of $\star$ imposes further rather complicated conditions on the data. For the case of a G-algebra with the multiplication defined by rewrite rules, they have been explicitly determined by Levandovskyy [44,45] who called them *non-degeneracy conditions* (see also the extensive discussion by Kredel [42, Sect. 3.3]).

Examples of polynomial algebras of solvable type abound in the literature. We mention here only some particularly important ones. *Ore algebras*, as originally introduced by Noether and Schmeidler [50] and later systematically studied by Ore [52], are solvable for any term order $\prec$. Note that this class includes in particular rings of linear differential or difference operators.

Bell and Goodearl [7] introduced the *Poincaré-Birkhoff-Witt extension* (for short *PBW extension*) of a ring $\mathcal{R}$ as a ring $\mathcal{P} \supseteq \mathcal{R}$ containing a finite number of elements $x_1, \ldots, x_n \in \mathcal{P}$ such that (i) $\mathcal{P}$ is freely generated as a left $\mathcal{R}$-module by the monomials x^μ with $\mu \in \mathbb{N}_0^n$, (ii) $x_i \star r - r \star x_i \in \mathcal{R}$ for all $r \in \mathcal{R}$ and (iii) $x_i \star x_j - x_j \star x_i \in \mathcal{R} + \mathcal{R}x_1 + \cdots \mathcal{R}x_n$. Obviously, any such extension is

a polynomial algebra of solvable type in the sense of Definition 3.1 for all degree compatible term orders (but generally not for other orders).

The classical example of such a PBW extension is the *universal enveloping algebra* $\mathfrak{U}(\mathfrak{g})$ of a finite-dimensional Lie algebra $\mathfrak{g}$ which also explains the name: the Poincaré-Birkhoff-Witt theorem asserts that the monomials form a basis of these algebras [60]. They still fit into the framework developed by Kandry-Rody and Weispfenning [41], as the x_i do not act on the coefficients. This is no longer the case for the more general *skew enveloping algebras* $\mathfrak{R}\#\mathfrak{U}(\mathfrak{g})$ where $\mathfrak{R}$ is a $\Bbbk$-algebra on which the elements of $\mathfrak{g}$ act as derivations [46, Sect. 1.7.10].

In all these examples, the coefficients $r_{\mu\nu}$ appearing in (5) are one; thus (8b) are classical commutation relations. This is not true for the *quantised enveloping algebras* $\mathfrak{U}_h(\mathfrak{g})$ introduced by Drinfeld [17] and Jimbo [40] or the even more general *q-algebras* introduced by Berger [8]. The latter ones are characterised by the fact that the polynomials h_{ij} in (8b) are at most quadratic with the additional restriction that h_{ij} may contain only those quadratic terms $x_k x_\ell$ that satisfy $i < k \leq \ell < j$ and $k - i = j - \ell$. Thus any such algebra is a polynomial algebra of solvable type for all degree compatible term orders.

If $(\mathcal{P}, \star, \prec)$ is a polynomial algebra of solvable type with a degree compatible term order $\prec$, then $\mathcal{P}$ is a filtered ring with respect to the standard filtration $\Sigma_q = \bigoplus_{i=0}^{q} \mathcal{P}_i$ and we may introduce the *associated graded algebra* by setting $(\mathrm{gr}_\Sigma \mathcal{P})_q = \Sigma_q / \Sigma_{q-1}$. It is easy to see that $\mathrm{gr}_\Sigma \mathcal{P}$ is again a polynomial algebra of solvable type for $\prec$. If in (8) $\deg h_i(r) = 0$, $\deg h_{ij} \leq 1$, $\rho_i = \mathrm{id}_\mathcal{R}$ and $r_{ij} = 1$ (which is for example the case for all Poincaré-Birkhoff-Witt extensions), then in fact $\mathrm{gr}_\Sigma \mathcal{P} = (\mathcal{P}, \cdot)$, the commutative polynomial ring. In this case one sometimes speaks of an *almost commutative* algebra [46, Sect. 8.4.2].

Proposition 3.5 *If the ring $\mathcal{R}$ is an integral domain, then any polynomial algebra $(\mathcal{P}, \star, \prec)$ of solvable type over it is an integral domain, too, and a left Ore domain.*

Proof The first assertion is a trivial consequence of (7): if $\mathcal{R}$ has no zero divisors, then $f \cdot g \neq 0$ implies $f \star g \neq 0$. Hence $\mathcal{P}$ does not contain any zero divisors.

For the second one we must verify the *left Ore conditions* [15, 51]: we must show that one can find for any two polynomials $f, g \in \mathcal{P}$ with $f \star g \neq 0$ two further polynomials $\phi, \psi \in \mathcal{P} \setminus \{0\}$ such that $\phi \star f = \psi \star g$. We describe now a concrete algorithm for this task.

We set $\mathcal{F}_0 = \{f, g\}$ and choose coefficients $r_0, s_0 \in \mathcal{R}$ such that in the difference $r_0 g \star f - s_0 f \star g = \bar{h}_1$ the leading terms cancel. Then we perform a (left) pseudo-reduction of $\bar{h}_1$ with respect to $\mathcal{F}_0$. It leads with an appropriately chosen coefficient $t_0 \in \mathcal{R}$ to an equation of the form

$$t_0 \bar{h}_1 = \phi_0 \star f + \psi_0 \star g + h_1 \tag{9}$$

where the remainder h_1 satisfies $\mathrm{le}_\prec h_1 \notin \langle \mathrm{le}_\prec \mathcal{F}_0 \rangle$. If $h_1 = 0$, we are done and the polynomials $\phi = t_0 r_0 g - \phi_0$ and $\psi = t_0 s_0 f + \psi_0$ form a solution of our problem. By Part (iii) of Definition 3.1 we have $\mathrm{le}_\prec \bar{h}_1 \prec \mathrm{le}_\prec f + \mathrm{le}_\prec g$. This implies by the monotonicity of term orders that $\mathrm{le}_\prec \phi_0 \prec \mathrm{le}_\prec g$ and $\mathrm{le}_\prec \psi_0 \prec \mathrm{le}_\prec f$. Thus we have found a non-trivial solution.

Otherwise we set $\mathcal{F}_1 = \mathcal{F}_0 \cup \{h_1\}$ and choose coefficients $r_1, s_1 \in \mathcal{R}$ such that in the difference $r_1 f \star h_1 - s_1 h_1 \star f = \bar{h}_2$ the leading terms cancel. Now we perform a (left) pseudo-reduction of $\bar{h}_2$ with respect to $\mathcal{F}_1$. This computation yields a coefficient $t_1 \in \mathcal{R}$ and polynomials $\phi_1, \psi_1, \rho_1 \in \mathcal{P}$ such that

$$t_1 \bar{h}_2 = \phi_1 \star f + \psi_1 \star g + \rho_1 \star h_1 + h_2 \tag{10}$$

where the remainder h_2 satisfies $\mathrm{le}_\prec h_2 \notin \langle \mathrm{le}_\prec \mathcal{F}_1 \rangle$. If $h_2 = 0$, then we are done, as we can substitute h_1 from (9) and obtain thus for our problem the solution $\phi = (t_1 r_1 f - \rho_1) \star (t_0 r_0 g - \phi_0) - t_1 s_1 h_1 - \phi_1$ and $\psi = (t_1 r_1 f - \rho_1) \star (t_0 s_0 f + \psi_0) + \psi_1$. By the same reasoning on the leading exponents as above, it is a non-trivial one.

Otherwise we iterate: we set $\mathcal{F}_2 = \mathcal{F}_1 \cup \{h_2\}$, choose coefficients $r_2, s_2 \in \mathcal{R}$ such that in the difference $r_2 f \star h_2 - s_2 h_2 \star f = \bar{h}_3$ the leading terms cancel, compute the remainder h_3 of a (left) pseudo-reduction of $\bar{h}_3$ with respect to $\mathcal{F}_2$ and so on. If the iteration stops, i. e. if the remainder h_N vanishes for some value $N \in \mathbb{N}$, then we can construct non-zero polynomials ϕ, ψ with $\phi \star f = \psi \star g$ by substituting all remainders h_i by their defining equations. The iteration terminates by a simple Noetherian argument: $\langle \mathrm{le}_\prec \mathcal{F}_0 \rangle \subset \langle \mathrm{le}_\prec \mathcal{F}_1 \rangle \subset \langle \mathrm{le}_\prec \mathcal{F}_2 \rangle \subset \cdots$ is a strictly ascending chain of monoid ideals in $\mathbb{N}_0^n$ and thus cannot be infinite. □

Obviously, we can show by the same argument that $\mathcal{P}$ is a right Ore domain. The Ore multipliers ϕ, ψ constructed in the proof above are not unique. Instead of always analysing differences of the form $r_i f \star h_i - s_i h_i \star f$, we could have used differences of the form $r_i g \star h_i - s_i h_i \star g$ or we could have alternated between using f and g and so on. In general, each ansatz will lead to different multipliers.

We have given here a direct and in particular constructive proof that $\mathcal{P}$ satisfies the left and right Ore conditions. Instead we could have tried to invoke Theorem 2.1.15 of [46] stating that any right Noetherian integral domain is also a right Ore domain. However, as we will see in the next section, if the coefficient ring $\mathcal{R}$ of $\mathcal{P}$ is not a field, then the question whether or not $\mathcal{P}$ is (left or right) Noetherian becomes nontrivial in general.

Example 3.6 In the commutative polynomial ring one has always the trivial solution $\phi = g$ and $\psi = f$. One might expect that in the non-commutative case one only has to add some lower terms to it. However, this is not the case. Consider the universal enveloping algebra of the Lie algebra $\mathfrak{so}(3)$. We may write it as $\mathfrak{U}\big(\mathfrak{so}(3)\big) = \mathbb{k}[x_1, x_2, x_3]$ with the multiplication $\star$ defined by the relations:

$$\begin{aligned} x_1 \star x_2 &= x_1 x_2 \,, & x_2 \star x_1 &= x_1 x_2 - x_3 \,, \\ x_1 \star x_3 &= x_1 x_3 \,, & x_3 \star x_1 &= x_1 x_3 + x_2 \,, \\ x_2 \star x_3 &= x_2 x_3 \,, & x_3 \star x_2 &= x_2 x_3 - x_1 \,. \end{aligned} \tag{11}$$

This multiplication obviously respects any degree compatible term order but not the lexicographic order. Choosing $f = x_1$ and $g = x_2$, possible solutions for $\phi \star f = \psi \star g$ are $\phi = x_2^2 - 1$ and $\psi = x_1 x_2 - 2x_3$ or $\phi = x_1 x_2 + x_3$ and $\psi = x_1^2 - 1$. They are easily constructed using the algorithm of the proof of Proposition 3.5 once with f and once with g. Here we must use polynomials of degree 2; it is not possible to find a solution of degree 1. ◁

4 Hilbert's Basis Theorem for Solvable Algebras

A classical property of the ordinary polynomial ring $\mathcal{P} = \mathcal{R}[x_1, \dots, x_n]$, which is crucial in the theory of Gröbner bases, is Hilbert's Basis Theorem. For our more general class of polynomial algebras, it remains true only under additional assumptions. As $\mathcal{P}$ is generally non-commutative, we must distinguish left, right and two-sided ideals and thus also study separately whether $\mathcal{P}$ is left or right Noetherian.

With the exception of Section 8, we will exclusively work with left ideals and thus do not introduce special notations. This restriction to left ideals is not only for convenience but stems from the fundamental left-right asymmetry of Definition 3.1 of a polynomial algebra of solvable type where products $r \star x^\mu$ and $x^\mu \star r$ are treated completely different. For this reason we discuss only the question when $\mathcal{P}$ is left Noetherian (see also Remark 4.8 below).

Most classical proofs of Hilbert's Basis Theorem consider only the univariate case and then extend inductively to an arbitrary (but finite) number of variables. However, this inductive approach is not possible in arbitrary polynomial algebras of solvable type, as the multiplication $\star$ does not necessarily restrict to a subalgebra with fewer variables. A simple counterexample is provided by the universal enveloping algebra $\mathfrak{U}\big(\mathfrak{so}(3)\big)$ introduced in Example 3.6 where $\star$ cannot be restricted to the subspace $\Bbbk[x_1, x_2]$ since $x_2 \star x_1 = x_1 x_2 - x_3$. This observation motivates the following definition.

Definition 4.1 *The polynomial algebra of solvable type $(\mathcal{P}, \star, \prec)$ is called* iterated*, if it satisfies the following three conditions.*

(i) $\mathcal{P}$ can be written in the form $\mathcal{P} = \mathcal{R}[x_1][x_2]\cdots[x_n]$ where each intermediate ring $\mathcal{P}_{(k)} = \mathcal{R}[x_1][x_2]\cdots[x_k]$ is again solvable for the corresponding restrictions of the multiplication $\star$ and the term order $\prec$.
(ii) The equality $x_k \star \mathcal{P}_{(k-1)} + \mathcal{P}_{(k-1)} = \mathcal{P}_{(k-1)} \star x_k + \mathcal{P}_{(k-1)}$ holds for $1 \leq k \leq n$.
(iii) In (5b) the coefficients $r_{\mu\nu}$ are units whenever the multi indices are of the form $\mu = \ell_k$, $\nu = m_k$ for $1 \leq k \leq n$ and arbitrary values $\ell, m \in \mathbb{N}$.

For iterated polynomial algebras of solvable type we may apply the usual inductive technique for proving a basis theorem. The following result is proven in [46, Theorem 1.2.9/10] for Ore algebras, but it is fairly straightforward to adapt the proof such that it remains valid for our more general class of algebras (see [55, Sect. 3.3] for the details). The main idea of this proof consists of expressing any polynomial $f = \sum_\ell a_\ell x_k^\ell \in \mathcal{P}_{(k)}$ with coefficients $a_\ell \in \mathcal{P}_{(k-1)}$ in the "reverse" form $f = \sum_\ell x_k^\ell \star \bar{a}_\ell$ where again $\bar{a}_\ell \in \mathcal{P}_{(k-1)}$. Condition (ii) guarantees that this rewriting is always possible. In the proof, one multiplies such "reverse" polynomials from the left by powers x_k^m; Condition (iii) ensures that all arising coefficients on the left are units and thus can be cancelled by multiplying with their inverse.

Theorem 4.2 *If $(\mathcal{P}, \star, \prec)$ is an iterated polynomial algebra of solvable type over a left Noetherian ring $\mathcal{R}$, then $\mathcal{P}$ is a left Noetherian ring, too.*

The additional conditions in Definition 4.1 cannot be omitted, if a basis theorem is to hold. McConnell and Robson [46, Example 1.2.11] provide a concrete

counterexample of a univariate polynomial ring of solvable type which violates them and which is neither left nor right Noetherian.

With some complications, the central (univariate) arguments in the proof of Theorem 4.2 can be directly generalised to multivariate polynomial rings. However, this requires again certain assumptions on the commutation relations (5) in order to ensure that all necessary computations are possible.

Definition 4.3 *The polynomial algebra of solvable type* $(\mathcal{P}, \star, \prec)$ *has* centred commutation relations*, if (i) there exists a field* $\Bbbk \subseteq \mathcal{R}$ *lying in the centre of* $\mathcal{R}$*, (ii) the functions* ρ_μ *in (5a) are of the form* $\rho_\mu(r) = \bar{\rho}_\mu(r)r$ *with functions* $\bar{\rho}_\mu : \mathcal{R} \to \Bbbk$ *and (iii) we have* $r_{\mu\nu} \in \Bbbk$ *in (5b).*

Using König's Lemma, Kredel proved in his thesis [42, Sect. 3.5] the following version of Hilbert's Basis Theorem.

Theorem 4.4 *Let* $(\mathcal{P}, \star, \prec)$ *be a polynomial algebra of solvable type with centred commutation relations over a left Noetherian coefficient ring* $\mathcal{R}$*. Then* $\mathcal{P}$ *is left Noetherian, too.*

A third proof assumes that the ring $\mathcal{P}$ possesses a *filtration* Σ. Using an approach detailed in [9] for the special case of the Weyl algebra (but which does not use any special properties of the Weyl algebra), one obtains the following general result where it is not even necessary to assume that $\mathcal{P}$ is a polynomial ring. Note that it covers any polynomial algebra of solvable type which is almost commutative and thus a large part of the algebras having appeared in the literature so far.

Theorem 4.5 *Let* Σ *be a filtration on the ring* $\mathcal{P}$*. If the associated graded ring* $\operatorname{gr}_\Sigma \mathcal{P}$ *is left Noetherian, then* $\mathcal{P}$ *is left Noetherian, too.*

Because of Condition (iii) in Definition 3.1 we can define Gröbner bases for ideals in algebras of solvable type. For a (commutative) coefficient field $\mathcal{R} = \Bbbk$, such a definition becomes trivial and from now on we will restrict to this case; the general case will be discussed only in Section 11.

Definition 4.6 *Let* $(\mathcal{P}, \star, \prec)$ *be a polynomial algebra of solvable type over a field* $\Bbbk$ *and* $\mathcal{I} \subseteq \mathcal{P}$ *a left ideal. A finite set* $\mathcal{G} \subset \mathcal{I}$ *is a* Gröbner basis *of* $\mathcal{I}$ *(for the term order* $\prec$*), if* $\langle \operatorname{le}_\prec \mathcal{G} \rangle = \operatorname{le}_\prec \mathcal{I}$*.*

For the ordinary multiplication this definition reduces to the classical one. The decisive point, explaining the conditions imposed in Definition 3.1, is that normal forms with respect to a finite set $\mathcal{F} \subset \mathcal{P}$ may be computed in algebras of solvable type in precisely the same way as in the ordinary polynomial ring. Assume we are given a polynomial $f \in \mathcal{P}$ such that $\operatorname{le}_\prec g \mid \operatorname{le}_\prec f$ for some $g \in \mathcal{G}$ and set $\mu = \operatorname{le}_\prec f - \operatorname{le}_\prec g$. If we consider $g_\mu = x^\mu \star g$, then by (iii) $\operatorname{le}_\prec g_\mu = \operatorname{le}_\prec f$. Setting $d = \operatorname{lc}_\prec f / \operatorname{lc}_\prec g_\mu$, we find by (ii) that $\operatorname{le}_\prec (f - dg_\mu) \prec \operatorname{le}_\prec f$. Hence we may use the usual algorithms for computing normal form; in particular, they always terminate by the same argument as in the ordinary case. Note that in general $d \neq \operatorname{lc}_\prec f / \operatorname{lc}_\prec g$, if $r \neq 1$ in (7), and that normal form computations are typically more expensive due to the appearance of the additional polynomial h in (7).

The classical Gröbner basis theory can be straightforwardly extended to polynomial algebras of solvable type [2,12,13,41,42,44,45], as most proofs are based on the computation of normal forms. The remaining arguments mostly take place in the monoid $\mathbb{N}_0^n$ and thus can be applied without changes. In particular, a trivial adaption of the standard (commutative) proof leads to the following result crucial for the termination of Buchberger's algorithm.

Theorem 4.7 *Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type over a field. Then $\mathcal{P}$ is a left Noetherian ring and every left ideal $\mathcal{I} \subseteq \mathcal{P}$ possesses a Gröbner basis with respect to $\prec$.*

Remark 4.8 Even in the case of a coefficient field we cannot generally expect $\mathcal{P}$ to be a *right* Noetherian ring, too; a concrete counterexample is provided again by McConnell and Robson [46, Example 1.2.11]. In the proof of Theorem 4.7 one essentially uses that in normal form computations one always multiplies with elements of $\mathcal{P}$ from the left. Because of the already above mentioned left-right asymmetry of Definition 3.1, right ideals show in general a completely different behaviour. In order to obtain right Noetherian rings we must either adapt correspondingly our definition of a solvable algebra or impose additional conditions on the commutation relations (5).

The simplest possibility is to require that all the maps ρ_μ in (5) are automorphisms (by Proposition 3.4 it suffices, if the maps ρ_i in (8a) satisfy this condition). In this case we have $\Bbbk \star x_i + \Bbbk = x_i \star \Bbbk + \Bbbk$ for all variables x_i implying that we can rewrite any polynomial $f = \sum_\mu c_\mu x^\mu$ in the "reverse" form $f = \sum_\mu x^\mu \star \tilde{c}_\mu$. Now a straightforward adaption of the classical proof of Theorem 4.7 shows that the ring $\mathcal{P}$ is also right Noetherian. $\lhd$

We do not give more details on Gröbner bases, as they can be found in the above cited references. Instead we will present in the next section a completely different approach leading to involutive bases.

5 Involutive Bases

We proceed to define involutive bases for left ideals in polynomial algebras of solvable type. In principle, we could at once consider submodules of free modules over such an algebra. As this only complicates the notation, we restrict to the ideal case and the extension to submodules goes as for Gröbner bases.

Definition 5.1 *Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type over a field $\Bbbk$ and $\mathcal{I} \subseteq \mathcal{P}$ a non-zero left ideal. A finite subset $\mathcal{H} \subset \mathcal{I}$ is a* weak involutive basis *of $\mathcal{I}$ for an involutive division L on $\mathbb{N}_0^n$, if its leading exponents $\mathrm{le}_\prec \mathcal{H}$ form a weak involutive basis of the monoid ideal $\mathrm{le}_\prec \mathcal{I}$. The subset $\mathcal{H}$ is a* (strong) involutive basis *of $\mathcal{I}$, if $\mathrm{le}_\prec \mathcal{H}$ is a strong involutive basis of $\mathrm{le}_\prec \mathcal{I}$ and no two distinct elements of $\mathcal{H}$ have the same leading exponents.*

Remark 5.2 This definition of an involutive basis is different from the original one given by Gerdt and Blinkov [20, Def. 6.2]. Firstly, the distinction into weak and

strong bases is new. Secondly, our definition does not require that an involutive basis is involutively autoreduced as the one by Gerdt and Blinkov; this condition entails that their bases are always strongly involutive. Finally, from a "philosophical" point of view, our approach is a natural extension of Definition 4.6 of a Gröbner basis in the ring $\mathcal{P}$, whereas the approach of Gerdt and Blinkov [20] is modelled on the equivalent characterisation of Gröbner bases by the vanishing of the normal forms of ideal members. However, it will follow from our results below that both approaches are essentially equivalent. $\lhd$

Definition 5.1 implies immediately that any weak involutive basis is a Gröbner basis. As in Section 2, we call any finite set $\mathcal{F} \subset \mathcal{P}$ *(weakly) involutive*, if it is a (weak) involutive basis of the ideal $\langle \mathcal{F} \rangle$ generated by it.

Definition 5.3 *Let $\mathcal{F} \subset \mathcal{P} \setminus \{0\}$ be a finite set and L an involutive division on $\mathbb{N}_0^n$. We assign to each element $f \in \mathcal{F}$ a set of* multiplicative variables

$$X_{L,\mathcal{F},\prec}(f) = \big\{ x_i \mid i \in N_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec f) \big\} \,. \tag{12}$$

The involutive span *of $\mathcal{F}$ is then the set*

$$\langle \mathcal{F} \rangle_{L,\prec} = \sum_{f \in \mathcal{F}} \Bbbk\big[X_{L,\mathcal{F},\prec}(f)\big] \star f \subseteq \langle \mathcal{F} \rangle \,. \tag{13}$$

An important aspect of Gröbner bases is the existence of standard representations for ideal elements. For (weak) involutive bases a similar characterisation exists and in the case of strong bases we even obtain unique representations.

Theorem 5.4 *Let $\mathcal{I} \subseteq \mathcal{P}$ be a non-zero ideal, $\mathcal{H} \subset \mathcal{I} \setminus \{0\}$ a finite set and L an involutive division on $\mathbb{N}_0^n$. Then the following two statements are equivalent.*

(i) *The set $\mathcal{H}$ is a weak involutive basis of $\mathcal{I}$ with respect to L and $\prec$.*
(ii) *Every polynomial $f \in \mathcal{I}$ can be written in the form*

$$f = \sum_{h \in \mathcal{H}} P_h \star h \tag{14}$$

where the coefficients $P_h \in \Bbbk[X_{L,\mathcal{H},\prec}(h)]$ satisfy $\mathrm{le}_\prec (P_h \star h) \preceq \mathrm{le}_\prec f$ for all polynomials $h \in \mathcal{H}$.

$\mathcal{H}$ is a strong involutive basis, if and only if the representation (14) is unique.

Proof Let us first assume that the set $\mathcal{H}$ is a weak involutive basis. Take an arbitrary polynomial $f \in \mathcal{I}$. According to Definition 5.1, its leading exponent $\mathrm{le}_\prec f$ lies in the involutive cone $\mathcal{C}_{L,\mathrm{le}_\prec \mathcal{H}}(h)$ of at least one element $h \in \mathcal{H}$. Let $\mu = \mathrm{le}_\prec f - \mathrm{le}_\prec h$ and set $f_1 = f - cx^\mu \star h$ where the coefficient $c \in \Bbbk$ is chosen such that the leading terms cancel. Obviously, $f_1 \in \mathcal{I}$ and $\mathrm{le}_\prec f_1 \prec \mathrm{le}_\prec f$. Iteration yields a sequence of polynomials $f_i \in \mathcal{I}$. After a finite number of steps we must reach $f_N = 0$, as the leading exponents are always decreasing and by assumption the leading exponent of *any* polynomial in $\mathcal{I}$ possesses an involutive divisor in $\mathrm{le}_\prec \mathcal{H}$. But this implies the existence of a representation of the form (14).

Now assume that $\mathcal{H}$ is even a strong involutive basis and take an involutive standard representation (14). By definition of a strong basis, there exists one and only one generator $h \in \mathcal{H}$ such that $\mathrm{le}_\prec(P_h \star h) = \mathrm{le}_\prec f$. This fact determines uniquely $\mathrm{le}_\prec P_h$. Applying the same argument to $f - (\mathrm{lt}_\prec P_h) \star h$ shows by recursion that the representation (14) is indeed unique.

For the converse note that (ii) trivially implies that $\mathrm{le}_\prec f \in \langle \mathrm{le}_\prec \mathcal{H} \rangle_{L,\prec}$ for any polynomial $f \in \mathcal{I}$. Thus $\mathrm{le}_\prec \mathcal{I} \subseteq \langle \mathrm{le}_\prec \mathcal{H} \rangle_{L,\prec}$. As the converse inclusion is obvious, we have in fact an equality and $\mathcal{H}$ is a weak involutive basis.

Now let us assume that the set $\mathcal{H}$ is only a weak but not a strong involutive basis of $\mathcal{I}$. This implies the existence of two generators $h_1, h_2 \in \mathcal{H}$ such that $\mathcal{C}_{L,\mathrm{le}_\prec \mathcal{H}}(\mathrm{le}_\prec h_2) \subset \mathcal{C}_{L,\mathrm{le}_\prec \mathcal{H}}(\mathrm{le}_\prec h_1)$. Hence we have $\mathrm{lm}_\prec h_2 = \mathrm{lm}_\prec (cx^\mu \star h_1)$ for suitably chosen $c \in \Bbbk$ and $\mu \in \mathbb{N}_0^n$. Consider the polynomial $h_2 - cx^\mu \star h_1 \in \mathcal{I}$. If it vanishes, we have found a non-trivial involutive standard representation of 0. Otherwise an involutive standard representation $h_2 - cx^\mu \star h_1 = \sum_{h \in \mathcal{H}} P_h \star h$ with $P_h \in \Bbbk[X_{L,\mathcal{H},\prec}(h)]$ exists. Setting $P'_h = P_h$ for all generators $h \neq h_1, h_2$ and $P'_{h_1} = P_{h_1} + cx^\mu$, $P'_{h_2} = P_{h_2} - 1$ yields again a non-trivial involutive standard representation $0 = \sum_{h \in \mathcal{H}} P'_h \star h$. The existence of such a non-trivial representation of 0 immediately implies that (14) cannot be unique. Thus only for a strong involutive basis the involutive standard representation is always unique. □

Corollary 5.5 *Let the set $\mathcal{H}$ be a weak involutive basis of the left ideal $\mathcal{I} \subseteq \mathcal{P}$. Then $\langle \mathcal{H} \rangle_{L,\prec} = \mathcal{I}$. If $\mathcal{H}$ is even a strong involutive basis of $\mathcal{I}$, then $\mathcal{I}$ possesses as $\Bbbk$-linear space a direct sum decomposition $\mathcal{I} = \bigoplus_{h \in \mathcal{H}} \Bbbk[X_{L,\mathcal{H},\prec}(h)] \star h$.*

Proof It follows immediately from Theorem 5.4 that $\mathcal{I} \subseteq \langle \mathcal{H} \rangle_{L,\prec}$. But as $\mathcal{H}$ is also a Gröbner basis of $\mathcal{I}$, we have in fact equality. The direct sum decomposition for a strong involutive basis is a trivial consequence of the uniqueness of the involutive standard representation in this case. □

Example 5.6 It is *not* true that any set $\mathcal{F}$ with $\langle \mathcal{F} \rangle_{L,\prec} = \mathcal{I}$ is a weak involutive basis of the ideal $\mathcal{I}$. Consider in the ordinary polynomial ring $\Bbbk[x, y]$ the ideal $\mathcal{I}$ generated by the two polynomials $f_1 = y^2$ and $f_2 = y^2 + x^2$. If we order the variables as $x_1 = x$ and $x_2 = y$, then the set $\mathcal{F} = \{f_1, f_2\}$ trivially satisfies $\langle \mathcal{F} \rangle_{J,\prec} = \mathcal{I}$, as with respect to the Janet division all variables are multiplicative for each generator. However, $\mathrm{le}_\prec \mathcal{F} = \{[0, 2]\}$ does *not* generate $\mathrm{le}_\prec \mathcal{I}$, as obviously $[2, 0] \in \mathrm{le}_\prec \mathcal{I} \setminus \langle \{[0, 2]\} \rangle$. Thus $\mathcal{F}$ is not a weak Janet basis (neither is the autoreduced set $\mathcal{F}' = \{y^2, x^2\}$, as $x^2 y \notin \langle \mathcal{F}' \rangle_{J,\prec}$). ◁

Proposition 5.7 *Let $\mathcal{I} \subseteq \mathcal{P}$ be an ideal and $\mathcal{H} \subset \mathcal{P}$ a weak involutive basis of it for the involutive division L. Then there exists a subset $\mathcal{H}' \subseteq \mathcal{H}$ which is a strong involutive basis of $\mathcal{I}$.*

Proof If the set $\mathrm{le}_\prec \mathcal{H}$ is already a strong involutive basis of $\mathrm{le}_\prec \mathcal{I}$, we are done. Otherwise $\mathcal{H}$ contains polynomials h_1, h_2 such that $\mathrm{le}_\prec h_1 \,|_{L,\mathrm{le}_\prec \mathcal{H}}\, \mathrm{le}_\prec h_2$. Consider the subset $\mathcal{H}' = \mathcal{H} \setminus \{h_2\}$. As in the proof of Proposition 2.8 one easily shows that $\mathrm{le}_\prec \mathcal{H}' = \mathrm{le}_\prec \mathcal{H} \setminus \{\mathrm{le}_\prec h_2\}$ is still a weak involutive basis of $\mathrm{le}_\prec \mathcal{I}$ and thus $\mathcal{H}'$ is still a weak involutive basis of $\mathcal{I}$. After a finite number of such eliminations we must reach a strong involutive basis. □

Given this result, one may wonder why we have introduced the notion of a weak basis. The reason is that in more general situations like computations in local rings or polynomial algebras over coefficient rings (treated in later sections) strong bases rarely exist.

Definition 5.8 ([20, Def. 5.2]) *Let $\mathcal{F} \subset \mathcal{P}$ be a finite set and L an involutive division. A polynomial $g \in \mathcal{P}$ is* involutively reducible *with respect to $\mathcal{F}$, if it contains a term x^μ such that $\mathrm{le}_\prec f \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \mu$ for some $f \in \mathcal{F}$. It is in* involutive normal form *with respect to $\mathcal{F}$, if it is not involutively reducible. The set $\mathcal{F}$ is* involutively autoreduced, *if no polynomial $f \in \mathcal{F}$ contains a term x^μ such that another polynomial $f' \in \mathcal{F} \setminus \{f\}$ exists with $\mathrm{le}_\prec f' \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \mu$.*

Remark 5.9 The definition of an involutively autoreduced set *cannot* be formulated more concisely by saying that each $f \in \mathcal{F}$ is in involutive normal form with respect to $\mathcal{F} \setminus \{f\}$. If we are not dealing with a global division, the removal of f from $\mathcal{F}$ will generally change the assignment of the multiplicative indices and thus affect the involutive divisibility. $\lhd$

An *obstruction to involution* is a polynomial $g \in \langle\mathcal{F}\rangle \setminus \langle\mathcal{F}\rangle_{L,\prec}$ possessing a (necessarily non-involutive) standard representation with respect to $\mathcal{F}$. We will later see that these elements make the difference between an involutive and an arbitrary Gröbner basis.

Example 5.10 Consider the set $\mathcal{F} = \{f_1, f_2, f_3\} \subset \mathbb{k}[x, y, z]$ with the polynomials $f_1 = z^2 - xy$, $f_2 = yz - x$ and $f_3 = y^2 - z$. For any degree compatible term order, the leading terms of f_2 and f_3 are unique. For f_1 we have two possibilities: if we use the degree lexicographic order (i. e. for $x \prec y \prec z$), it is z^2, for the degree inverse lexicographic order (i. e. for $x \succ y \succ z$) the leading term is xy.

In the first case, $\langle\mathcal{F}\rangle_{J,\prec_{\text{deglex}}} = \langle\mathcal{F}\rangle$, so that for this term order $\mathcal{F}$ is a Janet basis, i. e. an involutive basis with respect to the Janet division, although we have not yet the necessary tools to prove this fact. In the second case, $f_4 = z^3 - x^2 = zf_1 + xf_2 \in \langle\mathcal{F}\rangle$ does not possess a standard representation and $\mathcal{F}$ is not even a Gröbner basis. Adding f_4 to $\mathcal{F}$ yields a Gröbner basis $\mathcal{G}$ of $\langle\mathcal{F}\rangle$, as one may easily check. But this makes z non-multiplicative for f_2 and $f_5 = zf_2$ is now an obstruction to involution of $\mathcal{G}$, as it is not involutively reducible with respect to the Janet division. In fact, the set $\mathcal{F}' = \{f_1, f_2, f_3, f_4, f_5\}$ is the smallest Janet basis of $\mathcal{I}$ for this term order, as it is not possible to remove an element. Note that this second basis is not only larger but also contains polynomials of higher degree. $\lhd$

Remark 5.11 If $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I}$, then any element of $\mathcal{I}$ has a standard representation. But this fact does not imply that for a given division L the ideal $\mathcal{I}$ is free of obstructions to involution. In order to obtain at least a weak involutive basis, we must add further elements of $\mathcal{I}$ to $\mathcal{G}$ until $\langle\mathrm{le}_\prec \mathcal{G}\rangle_L = \mathrm{le}_\prec \mathcal{I}$. Obviously, this observation allows us to reduce the construction of a polynomial involutive basis to a Gröbner basis computation plus a monomial completion. But we will see later that better possibilities exist.

It follows that in general involutive bases are not reduced Gröbner bases, as we already observed in Example 5.10. For $\prec_{\text{deglex}}$ the set $\mathcal{F}$ was simultaneously

a Janet basis and a reduced Gröbner basis. But for $\prec_{\text{deginvlex}}$ the reduced Gröbner basis is $\mathcal{F} \cup \{f_4\}$, whereas a Janet basis requires in addition the polynomial f_5. We will see in Part II that this "redundancy" in involutive bases is the key for their use in the structure analysis of polynomial ideals and modules. $\lhd$

It often suffices, if one does not consider all terms in g but only the leading term $\mathrm{lt}_\prec\, g$: the polynomial g is *involutively head reducible*, if $\mathrm{le}_\prec\, f \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \mathrm{le}_\prec\, g$ for some $f \in \mathcal{F}$. Similarly, the set $\mathcal{F}$ is *involutively head autoreduced*, if no leading exponent of an element $f \in \mathcal{F}$ is involutively divisible by the leading exponent of another element $f' \in \mathcal{F} \setminus \{f\}$. Note that the definition of a strong involutive basis immediately implies that it is involutively head autoreduced.

As involutive reducibility is a restriction of ordinary reducibility, involutive normal forms can be determined with trivial adaptions of the familiar algorithms. The termination follows by the same argument as usual, namely that any term order is a well-order. If g' is an involutive normal form of $g \in \mathcal{P}$ with respect to the set $\mathcal{F}$ for the division L, then we write $g' = \mathrm{NF}_{\mathcal{F},L,\prec}(g)$, although involutive normal forms are in general not unique (like ordinary normal forms). Depending on the order in which reductions are applied different results are obtained.

The ordinary normal form is unique, if and only if it is computed with respect to a Gröbner basis; this property is often used as an alternative definition of Gröbner bases. The situation is somewhat different for the involutive normal form.

Lemma 5.12 *The sum in (13) is direct, if and only if the finite set $\mathcal{F} \subset \mathcal{P} \setminus \{0\}$ is involutively head autoreduced with respect to the involutive division L.*

Proof One direction is obvious. For the converse, let f_1, f_2 be two distinct elements of $\mathcal{F}$ and $X_i = X_{L,\mathcal{F},\prec}(f_i)$ their respective sets of multiplicative variables for the division L. Assume that two polynomials $P_i \in \Bbbk[X_i]$ exist with $P_1 \star f_1 = P_2 \star f_2$ and hence $\mathrm{le}_\prec\,(P_1 \star f_1) = \mathrm{le}_\prec\,(P_2 \star f_2)$. As the multiplication $\star$ respects the term order $\prec$, this implies that $\mathcal{C}_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec\, f_1) \cap \mathcal{C}_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec\, f_2) \neq \emptyset$. Thus one of the involutive cones is completely contained in the other one and either $\mathrm{le}_\prec\, f_1 \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \mathrm{le}_\prec\, f_2$ or $\mathrm{le}_\prec\, f_2 \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \mathrm{le}_\prec\, f_1$ contradicting that $\mathcal{F}$ is involutively head autoreduced. $\square$

Proposition 5.13 *If the finite set $\mathcal{F} \subset \mathcal{P} \setminus \{0\}$ is involutively head autoreduced, every polynomial $g \in \mathcal{P}$ has a unique involutive normal form* $\mathrm{NF}_{\mathcal{F},L,\prec}(g)$.

Proof If 0 is an involutive normal form of g, then obviously $g \in \langle\mathcal{F}\rangle_{L,\prec}$. Conversely, assume that $g \in \langle\mathcal{F}\rangle_{L,\prec}$, i. e. the polynomial g can be written in the form $g = \sum_{f\in\mathcal{F}} P_f \star f$ with $P_f \in \Bbbk[X_{L,\mathcal{F},\prec}(f)]$. As $\mathcal{F}$ is involutively head autoreduced, the leading terms of the summands never cancel (see the proof of Lemma 5.12). Thus $\mathrm{le}_\prec\, g = \mathrm{le}_\prec\,(P_f \star f)$ for some $f \in \mathcal{F}$ and any polynomial $g \in \langle\mathcal{F}\rangle_{L,\prec}$ is involutively head reducible with respect to $\mathcal{F}$. Each reduction step in an involutive normal form algorithm leads to a new polynomial $g' \in \langle\mathcal{F}\rangle_{L,\prec}$ with $\mathrm{le}_\prec\, g' \preceq \mathrm{le}_\prec\, g$. If the leading term is reduced, we even get $\mathrm{le}_\prec\, g' \prec \mathrm{le}_\prec\, g$. As each terminating normal form algorithm must sooner or later reduce the leading term, we eventually obtain 0 as unique involutive normal form of any $g \in \langle\mathcal{F}\rangle_{L,\prec}$.

Let g_1 and g_2 be two involutive normal forms of the polynomial g. Obviously, $g_1 - g_2 \in \langle \mathcal{F} \rangle_{L,\prec}$. By definition of a normal form, neither g_1 nor g_2 contain any term involutively reducible with respect to $\mathcal{F}$ and the same holds for $g_1 - g_2$. Hence the difference $g_1 - g_2$ is also in involutive normal form and by our considerations above we must have $g_1 - g_2 = 0$. □

The next result provides a slight generalisation of [20, Thm. 7.1] where only strongly involutive sets are treated. We modify the proof given there such that it also holds for weakly involutive sets.

Proposition 5.14 *The ordinary and the involutive normal form of any polynomial $g \in \mathcal{P}$ with respect to a finite weakly involutive set $\mathcal{F} \subset \mathcal{P} \setminus \{0\}$ are identical.*

Proof Recalling the proof of the previous proposition, we see that we used the assumption that $\mathcal{F}$ was involutively head autoreduced only for proving the existence of a generator $f \in \mathcal{F}$ such that $\mathrm{le}_\prec f \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \mathrm{le}_\prec g$ for every polynomial $g \in \langle \mathcal{F} \rangle_{L,\prec}$. But it follows immediately from Theorem 5.4 that this property also holds for any weak involutive basis. Thus by the same argument as above, we conclude that the involutive normal form with respect to a weakly involutive set is unique. For Gröbner bases the uniqueness of the ordinary normal form is a classical property and any weak involutive basis is also a Gröbner basis. As a polynomial in ordinary normal form with respect to $\mathcal{F}$ is trivially in involutive normal form with respect to $\mathcal{F}$, too, the two normal forms must coincide. □

Finally, we extend the notion of a minimal involutive basis from $\mathbb{N}_0^n$ to $\mathcal{P}$. This is done in the same manner as in the theory of Gröbner bases.

Definition 5.15 ([21, Def. 5.1]) *Let $\mathcal{I} \subseteq \mathcal{P}$ be a non-zero ideal and L an involutive division. An involutive basis $\mathcal{H}$ of $\mathcal{I}$ with respect to L is* minimal, *if $\mathrm{le}_\prec \mathcal{H}$ is the minimal involutive basis of the monoid ideal $\mathrm{le}_\prec \mathcal{I}$ for the division L.*

By Proposition 2.11, we find that for a globally defined division like the Pommaret division any involutive basis is minimal. Uniqueness requires two additional assumptions. First of all, our definition of an involutive basis requires only that it is involutively head autoreduced; for uniqueness we obviously need a full involutive autoreduction. Secondly, we must normalise the leading coefficients to one, i. e. we must take a *monic* basis.

Proposition 5.16 ([21, Thm. 5.2]) *Let $\mathcal{I} \subseteq \mathcal{P}$ be a non-zero ideal and L an involutive division. Then $\mathcal{I}$ possesses at most one monic, involutively autoreduced, minimal involutive basis for the division L.*

6 Monomial Completion

We turn to the question of the actual construction of involutive bases. Unfortunately, for arbitrary involutive division no satisfying solution is known so far. In the monomial case, one may follow a brute force approach, namely performing

a breadth first search through the tree of all possible completions. Obviously, it terminates only, if a finite basis exists. But for divisions satisfying some additional properties one can design a fairly efficient completion algorithm.

The first problem in constructing an involutive completion of a finite subset $\mathcal{N} \subset \mathbb{N}_0^n$ for a division L is to check *effectively* whether $\mathcal{N}$ is already involutive. The trouble is that we do not know a priori where obstructions to involution might lie. If we denote by $1_j \in \mathbb{N}_0^n$ the multi index where all entries are zero except the jth one which is one, then the multi indices $\nu + 1_j$ with $\nu \in \mathcal{N}$ and $j \in \bar{N}_{L,\mathcal{N}}(\nu)$ are a natural first guess.

Definition 6.1 ([20, Def. 4.7]) *The finite set $\mathcal{N} \subset \mathbb{N}_0^n$ is* locally involutive *for the involutive division L, if $\nu + 1_j \in \langle\mathcal{N}\rangle_L$ for every non-multiplicative index $j \in \bar{N}_{L,\mathcal{N}}(\nu)$ of every multi index $\nu \in \mathcal{N}$.*

Obviously, local involution is easy to check effectively. However, while (weak) involution obviously implies local involution, the converse does not necessarily hold. A concrete counterexample was given by Gerdt and Blinkov [20, Ex. 4.8]. But they also discovered that for many divisions the converse is in fact true and thus for such divisions we can effectively decide involution.

Definition 6.2 ([20, Def. 4.9]) *Let L be an involutive division and $\mathcal{N} \subset \mathbb{N}_0^n$ a finite set. Let furthermore $(\nu^{(1)}, \ldots, \nu^{(t)})$ be a finite sequence of elements of $\mathcal{N}$ where every multi index $\nu^{(k)}$ with $k < t$ has a non-multiplicative index $j_k \in \bar{N}_{L,\mathcal{N}}(\nu^{(k)})$ such that $\nu^{(k+1)} \mid_{L,\mathcal{N}} \nu^{(k)} + 1_{j_k}$. The division L is* continuous*, if any such sequence consists only of distinct elements, i. e. if $\nu^{(k)} \neq \nu^{(\ell)}$ for all $k \neq \ell$.*

Proposition 6.3 ([20, Thm. 4.10]) *For a continuous division L, any locally involutive set $\mathcal{N} \subset \mathbb{N}_0^n$ is weakly involutive.*

Proof Let the set Σ contain those obstructions to involution that are of minimal length.[3] We claim that for a continuous division L all multi indices $\sigma \in \Sigma$ are of the form $\nu + 1_j$ with $\nu \in \mathcal{N}$ and $j \in \bar{N}_{L,\mathcal{N}}(\nu)$. This observation immediately implies our proposition: since for a locally involutive set all such multi indices are contained in $\langle\mathcal{N}\rangle_L$, we must have $\Sigma = \emptyset$ and thus $\langle\mathcal{N}\rangle = \langle\mathcal{N}\rangle_L$.

In order to prove our claim, we choose a $\sigma \in \Sigma$ for which no $\nu \in \mathcal{N}$ exists with $\sigma = \nu + 1_j$. We collect in $\mathcal{N}_\sigma$ all divisors $\nu \in \mathcal{N}$ of σ of maximal length. Let $\nu^{(1)}$ be an element of $\mathcal{N}_\sigma$; by assumption the multi index $\mu^{(1)} = \sigma - \nu^{(1)}$ satisfies $|\mu^{(1)}| > 1$ and at least one non-multiplicative index $j_1 \in \bar{N}_{L,\mathcal{N}}(\nu^{(1)})$ exists with $\mu^{(1)}_{j_1} > 0$. By the definition of Σ we have $\nu^{(1)} + 1_{j_1} \in \langle\mathcal{N}\rangle_L$. Thus a multi index $\nu^{(2)} \in \mathcal{N}$ exists with $\nu^{(2)} \mid_{L,\mathcal{N}} \nu^{(1)} + 1_{j_1}$. This implies $\nu^{(2)} \mid \sigma$ and we set $\mu^{(2)} = \sigma - \nu^{(2)}$. By the definition of the set $\mathcal{N}_\sigma$ we have $|\nu^{(2)}| \leq |\nu^{(1)}|$. Hence $\nu^{(2)} + 1_j \in \langle\mathcal{N}\rangle_L$ for all j.

Choose a non-multiplicative index $j_2 \in \bar{N}_{L,\mathcal{N}}(\nu^{(2)})$ with $\mu^{(2)}_{j_2} > 0$. Such an index exists as otherwise $\sigma \in \langle\mathcal{N}\rangle_L$. By the same arguments as above, a multi

[3] The length $|\nu|$ of a multi index $\nu \in \mathbb{N}_0^n$ is the sum of its entries, i. e. the degree of the monomial x^ν.

index $\nu^{(3)} \in \mathcal{N}$ exists with $\nu^{(3)} \mid_{L,\mathcal{N}} \nu^{(2)} + 1_{j_2}$ and $|\nu^{(3)}| \leq |\nu^{(2)}|$. We can iterate this process and produce an infinite sequence $(\nu^{(1)}, \nu^{(2)}, \dots)$ where each multi index satisfies $\nu^{(i)} \in \mathcal{N}$ and $\nu^{(i+1)} \mid_{L,\mathcal{N}} \nu^{(i)} + 1_{j_i}$ with $j_i \in \bar{N}_{L,\mathcal{N}}(\nu^{(i)})$. As $\mathcal{N}$ is a finite set, the elements of the sequence cannot be all different. This contradicts our assumption that L is a continuous division: by taking a sufficiently large part of this sequence we obtain a finite sequence with all properties mentioned in Definition 6.2 but containing some identical elements. Hence a multi index $\nu \in \mathcal{N}$ must exist such that $\sigma = \nu + 1_j$. □

Lemma 6.4 ([20, Cor. 4.11]) *The Janet and the Pommaret division are continuous.*

Proof Let $\mathcal{N} \subseteq \mathbb{N}_0^n$ be a finite set and $(\nu^{(i)}, \dots, \nu^{(t)})$ a finite sequence where $\nu^{(i+1)} \mid_{L,\mathcal{N}} \nu^{(i)} + 1_j$ with $j \in \bar{N}_{L,\mathcal{N}}(\nu^{(i)})$ for $1 \leq i < t$.

We claim that for $L = J$, the Janet division, $\nu^{(i+1)} \succ_{\text{lex}} \nu^{(i)}$ implying that the sequence cannot contain any identical entries. Set $k = \max\{i \mid \mu_i \neq \nu_i\}$. Then $j \leq k$, as otherwise $j \in N_{J,\mathcal{N}}(\nu^{(i+1)})$ entails $j \in N_{J,\mathcal{N}}(\nu^{(i)})$ contradicting our assumption that j is non-multiplicative for the multi index $\nu^{(i)}$. But $j < k$ is also not possible, as then $\nu_k^{(i+1)} < \nu_k^{(i)}$ and so k cannot be multiplicative for $\nu^{(i+1)}$. There remains as only possibility $j = k$. In this case $\nu_j^{(i+1)} = \nu_j^{(i)} + 1$, as otherwise j could not be multiplicative for $\nu^{(i+1)}$. Thus we conclude that $\nu^{(i+1)} \succ_{\text{lex}} \nu^{(i)}$ and the Janet division is continuous.

The proof for the case $L = P$, the Pommaret division, is slightly more subtle.[4] The condition $j \in \bar{N}_P(\nu^{(i)})$ implies that $\operatorname{cls}(\nu^{(i)} + 1_j) = \operatorname{cls}\nu^{(i)}$ and if $\nu^{(i+1)} \mid_P \nu^{(i)} + 1_j$, then $\operatorname{cls}\nu^{(i+1)} \geq \operatorname{cls}\nu^{(i)}$, i. e. the class of the elements of the sequence is monotonously increasing. If $\operatorname{cls}\nu^{(i+1)} = \operatorname{cls}\nu^{(i)} = k$, then the involutive divisibility requires that $\nu_k^{(i+1)} \leq \nu_k^{(i)}$, i. e. among the elements of the sequence of the same class the corresponding entry is monotonously decreasing. And if finally $\nu_k^{(i+1)} = \nu_k^{(i)}$, then we must have $\nu^{(i+1)} = \nu^{(i)} + 1_j$, i. e. the length of the elements is strictly increasing. Hence all elements of the sequence are different and the Pommaret division is continuous. □

Remark 6.5 In Remark 2.9 we discussed that for a global division a weak involutive basis of the sum $\mathcal{I}_1 + \mathcal{I}_2$ of two monoid ideals is obtained by simply taking the union of (weak) involutive bases of $\mathcal{I}_1$ and $\mathcal{I}_2$. As a more theoretical application of the concept of continuity, we prove now a similar statement for the product $\mathcal{I}_1 \cdot \mathcal{I}_2$ and the intersection $\mathcal{I}_1 \cap \mathcal{I}_2$ in the special case of the Pommaret division. Let $\mathcal{N}_1$ be a (weak) Pommaret basis of $\mathcal{I}_1$ and $\mathcal{N}_2$ of $\mathcal{I}_2$. We claim that the set $\mathcal{N} = \{\mu + \nu \mid \mu \in \mathcal{N}_1, \nu \in \mathcal{N}_2\}$ is a weak Pommaret basis of $\mathcal{I}_1 \cdot \mathcal{I}_2$ and that the set $\hat{\mathcal{N}} = \{\operatorname{lcm}(\mu, \nu) \mid \mu \in \mathcal{N}_1, \nu \in \mathcal{N}_2\}$ is a weak Pommaret basis of $\mathcal{I}_1 \cap \mathcal{I}_2$.

[4] It is tempting to tackle the Pommaret division in the same manner as the Janet division using $\prec_{\text{revlex}}$ instead of $\prec_{\text{lex}}$; in fact, such a "proof" can be found in the literature. Unfortunately, it is not correct: if $\nu^{(i+1)} = \nu^{(i)} + 1_j$, then $\nu^{(i+1)} \prec_{\text{revlex}} \nu^{(i)}$ although the latter multi index is a divisor of the former one ($\prec_{\text{revlex}}$ is *not* a term order!). Thus the sequences considered in the application of Definition 6.2 to the Pommaret division are in general not strictly ascending with respect to $\prec_{\text{revlex}}$.

By Proposition 6.3, it suffices to show that the sets $\mathcal{N}$ and $\hat{\mathcal{N}}$, respectively, are locally involutive for the Pommaret division. Thus we take a generator $\mu+\nu \in \mathcal{N}$, where we assume for definiteness that $\operatorname{cls}\mu \leq \operatorname{cls}\nu$, and a non-multiplicative index $j_1 > \operatorname{cls}(\mu+\nu) = \operatorname{cls}\mu$ of it. Then j_1 is also non-multiplicative for $\mu \in \mathcal{N}_1$ alone and the Pommaret basis $\mathcal{N}_1$ must contain a multi index $\mu^{(1)}$ which involutively divides $\mu + 1_{j_1}$. If we are lucky, then the generator $\mu^{(1)} + \nu \in \mathcal{N}$ is an involutive divisor of $\mu + \nu + 1_{j_1}$, too, and we are done.

Otherwise, there exists an index $k_1 > \operatorname{cls}\nu$ such that $(\mu - \mu^{(1)})_{k_1} > 0$. In this case the Pommaret basis $\mathcal{N}_2$ must contain a multi index $\nu^{(1)}$ which involutively divides $\nu+1_{k_1}$. Again, if we are lucky, then $\mu^{(1)}+\nu^{(1)} \in \mathcal{N}$ is an involutive divisor of $\mu+\nu+1_{j_1}$ and we are done. Otherwise, there are two possibilities. There could be an index $j_2 > \operatorname{cls}\mu^{(1)}$ such that $(\mu+\nu+1_{j_1}-\mu^{(1)}+\nu^{(1)})_{j_2} > 0$ entailing the existence of a further generator $\mu^{(2)} \in \mathcal{N}_1$ which involutively divides $\mu^{(1)}+1_{j_2}$. Or there could exist an index $k_2 > \operatorname{cls}\nu^{(1)}$ such that $(\mu+\nu+1_{j_1}-\mu^{(1)}+\nu^{(1)})_{k_2} > 0$ implying that there is a multi index $\nu^{(2)} \in \mathcal{N}_2$ involutively dividing $\nu^{(1)} + 1_{k_2}$.

Continuing in this manner, one easily sees that we build up two sequences $\big(\mu, \mu^{(1)}, \mu^{(2)}, \dots\big) \subseteq \mathcal{N}_1$ and $\big(\nu, \nu^{(1)}, \nu^{(2)}, \dots\big) \subseteq \mathcal{N}_2$ as in the definition of a continuous division. Since both Pommaret bases are finite by definition and the Pommaret division is continuous by Lemma 6.4, no sequence may become infinite and the above described process must stop with an involutive divisor of $\mu+\nu+1_{j_1}$. Hence $\mathcal{N}$ is locally involutive and a weak Pommaret basis of $\mathcal{I}_1 \cdot \mathcal{I}_2$. The proof for $\hat{\mathcal{N}}$ goes completely analogously replacing at appropriate places the sum of two multi indices by their least common multiple. $\lhd$

Definition 6.6 ([20, Def. 4.12]) *Let L be a continuous involutive division and $\mathcal{N} \subset \mathbb{N}_0^n$ a finite set of multi indices. Choose a multi index $\nu \in \mathcal{N}$ and a non-multiplicative index $j \in \bar{N}_{L,\mathcal{N}}(\nu)$ such that:*

(i) $\nu + 1_j \notin \langle\mathcal{N}\rangle_L$*;*
(ii) *if there exists $\mu \in \mathcal{N}$ and $k \in \bar{N}_{L,\mathcal{N}}(\mu)$ such that $\mu + 1_k \mid \nu + 1_j$ but $\mu + 1_k \neq \nu + 1_j$, then $\mu + 1_k \in \langle\mathcal{N}\rangle_L$.*

The division L is constructive*, if for any such set $\mathcal{N}$ and any such multi index $\nu + 1_j$ no multi index $\rho \in \langle\mathcal{N}\rangle_L$ with $\nu + 1_j \in \mathcal{C}_{L,\mathcal{N}\cup\{\rho\}}(\rho)$ exists.*

In words, constructivity may roughly be explained as follows. The conditions imposed on ν and j ensure a kind of minimality: no proper divisor of $\nu + 1_j$ is of the form $\mu + 1_k$ for a $\mu \in \mathcal{N}$ and not contained in the involutive span $\langle\mathcal{N}\rangle_L$. The conclusion implies that it is useless to add multi indices to $\mathcal{N}$ that lie in some involutive cone, as none of them can be an involutive divisor of $\nu + 1_j$. An efficient completion algorithm for a constructive division should consider only non-multiplicative indices.

Lemma 6.7 ([20, Prop. 4.13]) *Any globally defined division (and thus the Pommaret division) is constructive. The Janet division is constructive, too.*

We present now an algorithm for determining weak involutive completions of finite sets $\mathcal{N} \subset \mathbb{N}_0^n$. As mentioned above, for arbitrary involutive divisions,

nobody has so far been able to find a reasonable approach. But if we assume that the division is constructive, then a very simple completion algorithm exists (given first in the proof of [20, Thm. 4.14]), the basic ideas of which go back to Janet.

Algorithm 2 Completion in $(\mathbb{N}_0^n, +)$

Input: a finite set $\mathcal{N} \subset \mathbb{N}_0^n$, an involutive division L
Output: a weak involutive completion $\bar{\mathcal{N}}$ of $\mathcal{N}$
/1/ $\bar{\mathcal{N}} \leftarrow \mathcal{N}$
/2/ **loop**
/3/ $\mathcal{S} \leftarrow \big\{\nu + 1_j \mid \nu \in \bar{\mathcal{N}},\, j \in \bar{N}_{L,\bar{\mathcal{N}}}(\nu),\, \nu + 1_j \notin \langle \bar{\mathcal{N}} \rangle_L\big\}$
/4/ **if** $\mathcal{S} = \emptyset$ **then**
/5/ **return** $\bar{\mathcal{N}}$
/6/ **else**
/7/ choose $\mu \in \mathcal{S}$ such that $\mathcal{S}$ does not contain a proper divisor of it
/8/ $\bar{\mathcal{N}} \leftarrow \bar{\mathcal{N}} \cup \{\mu\}$
/9/ **end_if**
/10/ **end_loop**

The strategy behind Algorithm 2 is fairly natural given the results above. It collects in a set $\mathcal{S}$ all obstructions to local involution. For a continuous division L, the set $\mathcal{N}$ is weakly involutive, if and only if $\mathcal{S} = \emptyset$. Furthermore, for a constructive division L it does not make sense to add elements of $\langle \mathcal{N} \rangle_L$ to $\mathcal{N}$ in order to complete. Thus we add in Line /8/ an element of $\mathcal{S}$ which is minimal in the sense that the set $\mathcal{S}$ does not contain a proper divisor of it. The following termination and correctness proof is essentially due to Gerdt and Blinkov [20, Thm. 4.14].

Proposition 6.8 *Let the finite set $\mathcal{N} \subset \mathbb{N}_0^n$ possess a finite (weak) involutive completion with respect to the constructive division L. Then Algorithm 2 terminates with a weak involutive completion $\bar{\mathcal{N}}$ of $\mathcal{N}$.*

Proof If Algorithm 2 terminates, its correctness is obvious under the made assumptions. The criterion for its termination, $\mathcal{S} = \emptyset$, is equivalent to local involution of $\bar{\mathcal{N}}$. By Proposition 6.3, local involution implies for a continuous division weak involution. Thus the result $\bar{\mathcal{N}}$ is a weak involutive completion of $\mathcal{N}$, as by construction $\mathcal{N} \subseteq \bar{\mathcal{N}} \subset \langle \mathcal{N} \rangle$.

If the input set $\mathcal{N}$ is already involutive, Algorithm 2 leaves it unchanged and thus obviously terminates. Let us assume that $\mathcal{N}$ is not yet involutive. In the first iteration of the `loop` a multi index of the form $\mu = \nu + 1_j$ is added to $\mathcal{N}$. It is not contained in $\langle \mathcal{N} \rangle_L$ and $\mathcal{S}$ does not contain a proper divisor of it. If $\mathcal{N}_L$ is an arbitrary involutive completion of $\mathcal{N}$, it must contain a multi index $\lambda \notin \mathcal{N}$ such that $\lambda \,|_{L,\mathcal{N}_L}\, \mu$. We claim that $\lambda = \mu$.

Assume on the contrary that $\lambda \neq \mu$. Since $\mathcal{N}_L \subset \langle \mathcal{N} \rangle$, the multi index λ must lie in the cone of a generator $\nu^{(1)} \in \mathcal{N}$. We will show that, because of the continuity of L, $\lambda \in \langle \mathcal{N} \rangle_L$, contradicting the constructivity of L. If $\nu^{(1)} \,|_{L,\mathcal{N}}\, \lambda$, we are done. Otherwise we write $\lambda = \nu^{(1)} + \rho^{(1)}$ for some multi index $\rho^{(1)} \in \mathbb{N}_0^n$. By construction, a non-multiplicative index $j_1 \in \bar{N}_{L,\mathcal{N}}(\nu^{(1)})$ with $\rho_{j_1}^{(1)} > 0$ must

exist. Consider the multi index $\nu^{(1)}+1_{j_1}$. Because of $\nu^{(1)}+1_{j_1} \mid \lambda$, the multi index $\nu^{(1)}+1_{j_1}$ is a proper divisor of μ. Since the set $\mathcal{S}$ does not contain any proper divisor of μ, we must have $\nu^{(1)}+1_{j_1} \in \langle\mathcal{N}\rangle_L$. Thus a multi index $\nu^{(2)} \in \mathcal{N}$ exists such that $\nu^{(2)} \mid_{L,\mathcal{N}} \nu^{(1)}+1_{j_1}$.

By iteration of this argument, we obtain a sequence $\left(\nu^{(1)}, \nu^{(2)}, \ldots\right)$ where each element $\nu^{(i)} \in \mathcal{N}$ is a divisor of λ and where $\nu^{(i+1)} \mid_{L,\mathcal{N}} \nu^{(i)}+1_{j_i}$ with a non-multiplicative index $j_i \in \bar{N}_{L,\mathcal{N}}(\nu^{(i)})$. This sequence cannot become infinite for a continuous division, as λ possesses only finitely many different divisors and all the multi indices $\nu^{(i)}$ in arbitrary finite pieces of the sequence must be different. But the sequence will only stop, if some $\nu^{(i)} \in \mathcal{N}$ exists such that $\nu^{(i)} \mid_{L,\mathcal{N}} \lambda$ and hence we must have that $\lambda \in \langle\mathcal{N}\rangle_L$.

Thus *every* weak involutive completion $\mathcal{N}_L$ of the given set $\mathcal{N}$ must contain the multi index $\nu+1_j$. In the next iteration of the `loop`, Algorithm 2 treats the enlarged set $\mathcal{N}_1 = \mathcal{N} \cup \{\nu+1_j\}$. It follows from our considerations above that any weak involutive completion $\mathcal{N}_L$ of $\mathcal{N}$ is also a weak involutive completion of $\mathcal{N}_1$ and hence we may apply the same argument again. As a completion $\mathcal{N}_L$ is by definition a finite set, we must reach after a finite number k of iterations a weak involutive basis $\mathcal{N}_k$ of $\langle\mathcal{N}\rangle$. □

Note the crucial difference between this result and the termination proof of Buchberger's algorithm for the construction of Gröbner bases. In the latter case, we can show the termination for arbitrary input, i. e. the theorem provides a constructive proof for the existence of such a basis. Here we are only able to prove the termination under the assumption that a finite (weak) involutive basis exists; the existence has to be shown separately. For example, Lemma 2.15 guarantees us that any monoid ideal possesses a finite weak Janet basis.

Recall that by Proposition 2.8 any weak involutive basis can be made strongly involutive by simply eliminating some redundant elements. Thus we obtain an algorithm for the construction of a strong involutive basis of $\langle\mathcal{N}\rangle$ by adding an involutive autoreduction as last step to Algorithm 2. Alternatively, we could perform the involutive autoreduction as first step. Indeed, if the input set $\mathcal{N}$ is involutively autoreduced, then all intermediate sets $\bar{\mathcal{N}}$ constructed by Algorithm 2 are also involutively autoreduced. This fact is a simple consequence of the second condition in Definition 2.1 of an involutive division that involutive cones may only shrink, if we add elements to the set $\mathcal{N}$.

Remark 6.9 [5] While we just stated that it suffices to perform an involutive autoreduction as either first or last step in Algorithm 2, we now analyse for later use what happens, if we involutively autoreduce $\bar{\mathcal{N}}$ every time a new element has been added to it. The termination argument given in the proof of Proposition 6.8 does not remain valid after this modification and we must provide an alternative proof.

Let again $\mathcal{N}_L = \left\{\mu^{(1)}, \ldots, \mu^{(r)}\right\}$ be a weak involutive completion of the input set $\mathcal{N}$. If we denote by $\bar{\mathcal{N}}_i$ the value of $\bar{\mathcal{N}}$ after the ith iteration of the `loop`, then it was shown in the proof of Proposition 6.8 that $\mathcal{N}_L$ is also a weak involutive completion of any set $\bar{\mathcal{N}}_i$. As by definition $\mathcal{N}_L$ is finite and each $\bar{\mathcal{N}}_i$ is a subset

[5] The following considerations are joint work with Vladimir Gerdt.

of it, the only possibility for non-termination is the appearance of a cycle, i. e. the existence of values k_0, ℓ such that $\bar{\mathcal{N}}_{k+\ell} = \bar{\mathcal{N}}_k$ for all $k \geq k_0$.

Assume that in some iteration of the `loop` the multi index $\mu^{(k)}$ is added to $\bar{\mathcal{N}}$ and that in the subsequent involutive autoreduction some elements of $\bar{\mathcal{N}}$ are eliminated (in order to have a cycle this must indeed happen). The first step in the autoreduction must be that some multi index $\mu^{(\ell)}$ is eliminated, because $\mu^{(k)}$ is an involutive divisor of it. Indeed, by Condition (ii) in Definition 2.1, any other reduction would have been possible already before the insertion of $\mu^{(k)}$ and thus the previous involutive autoreduction would not have been finished.

Since $\mu^{(k)}$ has been added to $\bar{\mathcal{N}}$, there must exist some multi index $\mu^{(a_1)} \in \mathcal{N}$ such that $\mu^{(k)} = \mu^{(a_1)} + \rho$. Furthermore, we know that $\mu^{(\ell)} = \mu^{(k)} + \tilde{\sigma}$ for some multi index $\tilde{\sigma}$ with $|\tilde{\sigma}| > 0$ and thus $\mu^{(\ell)} = \mu^{(a_1)} + \sigma$ with $\sigma = \tilde{\sigma} + \rho$ and $|\sigma| > 1$. As we are in a cycle, the multi index $\mu^{(\ell)}$ must have been added to $\bar{\mathcal{N}}$ in a previous iteration of the `loop`, say when analysing $\bar{\mathcal{N}}_i$. Thus $\mu^{(\ell)}$ cannot be involutively divisible by $\mu^{(a_1)}$ and we must have $\sigma_{j_1} > 0$ for a non-multiplicative index $j_1 \in \bar{N}_{L,\bar{\mathcal{N}}_i}(\mu^{(a_1)})$. It cannot be that $\mu^{(a_1)} + 1_{j_1} = \mu^{(\ell)}$, as $|\sigma| > 1$, and therefore $\mu^{(a_1)} + 1_{j_1}$ is a proper divisor of $\mu^{(\ell)}$. Hence $\bar{\mathcal{N}}_i$ must contain an involutive divisor $\mu^{(a_2)}$ of $\mu^{(a_1)} + 1_{j_1}$, as otherwise this multi index would have been added to $\bar{\mathcal{N}}$ instead of $\mu^{(\ell)}$.

Obviously, $\mu^{(a_2)} \mid \mu^{(k)}$ and, decomposing $\mu^{(k)} = \mu^{(a_2)} + \pi$, we conclude by the same reasoning as above that $\pi_{j_2} > 0$ for some non-multiplicative index $j_2 \in \bar{N}_{L,\bar{\mathcal{N}}_i}(\mu^{(a_2)})$. Iteration of this argument yields an infinite sequence $\big(\mu^{(a_1)}, \mu^{(a_2)}, \dots\big)$ as in Definition 6.2 of a continuous division. However, since L is a continuous division and $\mathcal{N}_L$ a finite set, we arrive at a contradiction. Thus even with involutive autoreductions after each step Algorithm 2 terminates. $\lhd$

In some sense our description of Algorithm 2 is not complete, as we have not specified how one should choose the multi index μ in Line /7/, if several choices are possible. One would expect that different involutive completions are obtained for different choices. However, an interesting aspect of our proof of Proposition 6.8 is that it shows that this is not the case. The choice affects only the order in which multi indices are added but not which or how many multi indices are added during the completion. A simple method for choosing μ consists of taking an arbitrary term order $\prec$ (which also could be changed in each iteration of the `loop`) and setting $\mu = \min_{\prec} \mathcal{S}$. The following two corollaries expand [20, Cor. 4.15].

Corollary 6.10 *If Algorithm 2 terminates, its output $\bar{\mathcal{N}}$ is independent of the manner in which μ is chosen. Furthermore, if $\mathcal{N}_L$ is any weak involutive completion of $\mathcal{N}$ with respect to the division L, then $\bar{\mathcal{N}} \subseteq \mathcal{N}_L$.*

Proof Consider the set $\mathcal{L}(\mathcal{N})$ of all weak involutive completions of $\mathcal{N}$ with respect to the division L and define

$$\tilde{\mathcal{N}} = \bigcap_{\mathcal{N}_L \in \mathcal{L}(\mathcal{N})} \mathcal{N}_L \,. \tag{15}$$

We claim that Algorithm 2 determines this set $\tilde{\mathcal{N}}$ independent of the used term order. Obviously, this implies our corollary.

In the proof of Proposition 6.8 we showed that the multi indices added in Algorithm 2 are contained in *every* weak involutive completion of $\mathcal{N}$. Thus all these multi indices are elements of $\tilde{\mathcal{N}}$. As Algorithm 2 terminates with a weak involutive completion, its output is also an element of $\mathcal{L}(\mathcal{N})$ and hence must be $\tilde{\mathcal{N}}$. □

Corollary 6.11 *If the monoid ideal $\mathcal{I} \subseteq \mathbb{N}_0^n$ possesses an involutive basis for the constructive division L, then $\mathcal{I}$ has a unique minimal involutive basis.*

Proof If we apply Algorithm 2 to the unique minimal basis $\mathcal{N}$ of $\mathcal{I}$ in the usual sense, then it follows trivially from Corollary 6.10 that the output is a minimal involutive basis of $\mathcal{I}$ and that no other involutive basis of $\mathcal{I}$ can be minimal, as it is necessarily an involutive completion of $\mathcal{N}$. □

7 Polynomial Completion

An obvious way to compute an involutive basis for an ideal $\mathcal{I}$ in a polynomial algebra $(\mathcal{P}, \star, \prec)$ of solvable type goes as follows: we determine first a Gröbner basis $\mathcal{G}$ of $\mathcal{I}$ and then with Algorithm 2 an involutive completion of $\mathrm{le}_\prec \mathcal{G}$. In fact, a similar method is proposed by Sturmfels and White [56] for the construction of Stanley decompositions (cf. Part II). However, we prefer to extend the ideas behind Algorithm 2 to a direct completion algorithm for polynomial ideals, as we believe that this approach is more efficient.

First, we need two subalgorithms: *involutive normal forms* and *involutive head autoreductions*. The design of an algorithm $\mathtt{NormalForm}_{L,\prec}(g, \mathcal{H})$ determining an involutive normal form of the polynomial g with respect to the finite set $\mathcal{H} \subset \mathcal{P}$ is trivial. We may use the standard algorithm for normal forms in the Gröbner theory, if we replace the ordinary divisibility by its involutive version. Obviously, this modification does not affect the termination. Actually, for our purposes it is not even necessary to compute a full normal form; we may stop as soon as we have obtained a polynomial that is not involutively head reducible.

The design of an algorithm $\mathtt{InvHeadAutoReduce}_{L,\prec}(\mathcal{F})$ for an involutive head autoreduction of a finite set $\mathcal{F}$ is also obvious.[6] Again one may use the standard algorithm with the ordinary divisibility replaced by involutive divisibility.

Based on these two subalgorithms, we propose Algorithm 3 for the computation of involutive bases in $\mathcal{P}$.[7] It follows the same strategy as the monomial algorithm. We multiply each generator by its non-multiplicative variables. Then we decide whether or not the result is already contained in the involutive span of the basis; if not, it is added. This decision is effectively made via an involutive normal form computation: the involutive normal form of a polynomial is zero, if and only if the polynomial lies in the involutive span. As our goal is a strong involutive basis, we take care that our set is always involutively head autoreduced.

[6] [20, Sect. 5] contains explicit pseudocode for both needed subalgorithms. Note, however, that there always a full autoreduction and not only a head autoreduction is performed.

[7] We present here only the basic form of the involutive completion algorithm, as it makes the simple underlying ideas more transparent. Gerdt and Blinkov [20, Sect. 8] provide an optimised form of this algorithm which is, however, more involved.

Algorithm 3 Completion in $(\mathcal{P}, \star, \prec)$

Input: a finite set $\mathcal{F} \subset \mathcal{P}$, an involutive division L
Output: an involutive basis $\mathcal{H}$ of $\mathcal{I} = \langle \mathcal{F} \rangle$ with respect to L and $\prec$
/1/ $\mathcal{H} \leftarrow \mathtt{InvHeadAutoReduce}_{L,\prec}(\mathcal{F})$
/2/ **loop**
/3/ $\quad \mathcal{S} \leftarrow \{x_j \star h \mid h \in \mathcal{H},\, x_j \in \bar{X}_{L,\mathcal{H},\prec}(h),\, x_j \star h \notin \langle \mathcal{H} \rangle_{L,\prec}\}$
/4/ $\quad$ **if** $\mathcal{S} = \emptyset$ **then**
/5/ $\quad\quad$ **return** $\mathcal{H}$
/6/ $\quad$ **else**
/7/ $\quad\quad$ choose $\bar{g} \in \mathcal{S}$ such that $\mathrm{le}_\prec\, \bar{g} = \min_\prec \mathcal{S}$
/8/ $\quad\quad$ $g \leftarrow \mathtt{NormalForm}_{L,\prec}(\bar{g}, \mathcal{H})$
/9/ $\quad\quad$ $\mathcal{H} \leftarrow \mathtt{InvHeadAutoReduce}_{L,\prec}(\mathcal{H} \cup \{g\})$
/10/ $\quad$ **end_if**
/11/ **end_loop**

The manner in which we choose in Line /7/ the next polynomial $\bar{g}$ to be treated (we briefly write $\min_\prec \mathcal{S}$ for the minimal leading exponent of an element of $\mathcal{S}$) corresponds to the normal selection strategy in the theory of Gröbner bases. There, this strategy is known to work very well for degree compatible term orders but not so well for other orders like the purely lexicographic one. Whereas for Gröbner bases the selection strategy concerns only the efficiency of the computation, we will see below that here the use of this particular strategy is important for the termination proof. With more refined and optimised versions of the basic completion Algorithm 3 one can circumvent this restriction [5, 14, 19], but we will not discuss this highly technical question here.

Definition 7.1 *A finite set $\mathcal{F} \subset \mathcal{P}$ is* locally involutive *for the division L, if for every polynomial $f \in \mathcal{F}$ and for every non-multiplicative variable $x_j \in \bar{X}_{L,\mathcal{F},\prec}(f)$ the product $x_j \star f$ has an involutive standard representation with respect to $\mathcal{F}$.*

If the set $\mathcal{F}$ is involutively head autoreduced, then we may equivalently demand that $x_j \star f \in \langle \mathcal{F} \rangle_{L,\prec}$. Because of Lemma 5.12, this condition automatically implies the existence of an involutive standard representation. In fact, the criterion appears in this form in Line /3/ of Algorithm 3. In any case, local involution may be effectively verified by computing an involutive normal form of $x_j \star f$ in the usual manner, i. e. always performing head reductions.

Our next result is similar to one direction of [20, Thm. 6.5] and its proof uses essentially the same techniques. It is more general with respect to its assumptions, as it does not require that the set $\mathcal{F}$ is involutively autoreduced. As a consequence we obtain only a weaker conclusion (see, however, the subsequent corollary).

Proposition 7.2 *If the finite set $\mathcal{F} \subset \mathcal{P}$ is locally involutive for the continuous division L, then $\langle \mathcal{F} \rangle_{L,\prec} = \langle \mathcal{F} \rangle$.*

Proof We claim that if the set $\mathcal{F}$ is locally involutive (with respect to the continuous division L), then every product $x^\mu \star f_1$ of an arbitrary term x^μ with a polynomial $f_1 \in \mathcal{F}$ possesses an involutive standard representation. This claim

trivially entails our proposition, as any polynomial in $\langle \mathcal{F} \rangle$ consists of a finite linear combination of such products: adding the corresponding involutive standard representations shows that the polynomial is contained in $\langle \mathcal{F} \rangle_{L,\prec}$.

In order to prove our claim, it suffices to show the existence of a representation

$$x^\mu \star f_1 = \sum_{f \in \mathcal{F}} \Big(P_f \star f + \sum_{\nu \in \mathbb{N}_0^n} c_{\nu,f} x^\nu \star f \Big) \tag{16}$$

where $P_f \in \Bbbk[X_{L,\mathcal{F},\prec}(f)]$ and $\mathrm{le}_\prec (P_f \star f) = \mathrm{le}_\prec (x^\mu \star f_1)$ (or $P_f = 0$) and where the coefficients $c_{\nu,f} \in \Bbbk$ vanish for all multi indices $\nu \in \mathbb{N}_0^n$ such that $\mathrm{le}_\prec (x^\nu \star f) \succeq \mathrm{le}_\prec (x^\mu \star f_1)$. Our claim follows then by an obvious induction.

If $x^\mu \in \Bbbk[X_{L,\mathcal{F},\prec}(f_1)]$, i. e. it contains only variables that are multiplicative for $\mathrm{le}_\prec f_1$, nothing has to be shown. Otherwise we choose a non-multiplicative index $j_1 \in \bar{N}_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec f_1)$ such that $\mu_{j_1} > 0$. As $\mathcal{F}$ is locally involutive, an involutive standard representation $x_{j_1} \star f_1 = \sum_{f \in \mathcal{F}} P_f^{(1)} \star f$ exists. Let $\mathcal{F}_2 \subseteq \mathcal{F}$ contain all polynomials f_2 such that $\mathrm{le}_\prec (P_{f_2}^{(1)} \star f_2) = \mathrm{le}_\prec (x_{j_1} \star f_1)$. If we have $x^{\mu - 1_{j_1}} \in \Bbbk[X_{L,\mathcal{F},\prec}(f_2)]$ for all polynomials $f_2 \in \mathcal{F}_2$, then we are done, as at least $\mathrm{lm}_\prec (x^{\mu - 1_{j_1}} \star P_{f_2}^{(1)}) \in \Bbbk[X_{L,\mathcal{F},\prec}(f_2)]$.

Otherwise we consider the subset $\mathcal{F}_2' \subseteq \mathcal{F}_2$ of polynomials f_2 for which $x^{\mu - 1_{j_1}} \notin \Bbbk[X_{L,\mathcal{F},\prec}(f_2)]$ and iterate over it. For each polynomial $f_2 \in \mathcal{F}_2'$ we choose a non-multiplicative index $j_2 \in \bar{N}_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec f_2)$ such that $(\mu - 1_{j_1})_{j_2} > 0$. Again the local involution of the set $\mathcal{F}$ implies the existence of an involutive standard representation $x_{j_2} \star f_2 = \sum_{f \in \mathcal{F}} P_f^{(2)} \star f$. We collect in $\mathcal{F}_3 \subseteq \mathcal{F}$ all polynomials f_3 such that $\mathrm{le}_\prec (P_{f_3}^{(2)} \star f_3) = \mathrm{le}_\prec (x_{j_2} \star f_2)$. If we introduce the multi index $\nu = \mathrm{le}_\prec (x_{j_1} \star f_1) - \mathrm{le}_\prec f_2$, then $\mathrm{le}_\prec (x^\mu \star f_1) = \mathrm{le}_\prec (x^{\mu + \nu - 1_{j_1} - 1_{j_2}} \star f_3)$ for all $f_3 \in \mathcal{F}_3$. If $x^{\mu + \nu - 1_{j_1} - 1_{j_2}} \in \Bbbk[X_{L,\mathcal{F},\prec}(f_3)]$ for all $f_3 \in \mathcal{F}_3$, we are done.

Otherwise we continue in the same manner: we collect in a subset $\mathcal{F}_3' \subseteq \mathcal{F}_3$ all polynomials f_3 which are multiplied by non-multiplicative variables, for each of them we choose a non-multiplicative index $j_3 \in \Bbbk[X_{L,\mathcal{F},\prec}(f_3)]$ such that $(\mu - 1_{j_1} - 1_{j_2})_{j_3} > 0$, determine an involutive standard representation of $x_{j_3} \star f_3$ and analyse the leading terms. If they are still multiplied with non-multiplicative variables, this leads to sets $\mathcal{F}_4' \subseteq \mathcal{F}_4$ and so on. This process yields a whole tree of cases and each branch leads to a sequence $\big(\nu^{(1)} = \mathrm{le}_\prec f_1, \nu^{(2)} = \mathrm{le}_\prec f_2, \dots\big)$ where all contained multi indices $\nu^{(k)}$ are elements of the finite set $\mathrm{le}_\prec \mathcal{F}$ and where to each $\nu^{(k)}$ a non-multiplicative index $j_k \in \bar{N}_{L,\mathrm{le}_\prec \mathcal{F}}(\nu^{(k)})$ exists such that $\nu^{(k+1)} \,|_{L,\mathrm{le}_\prec \mathcal{F}}\, \nu^{(k)} + 1_{j_k}$. By the definition of a continuous division, this sequence cannot become infinite and thus each branch must terminate. But this implies that we may construct for each polynomial $f_1 \in \mathcal{F}$ and each non-multiplicative variables $x_j \in \bar{X}_{L,\mathcal{F},\prec}(f_1)$ a representation of the claimed form (16). □

Note that the proposition only asserts that the involutive span equals the normal span. It does *not* say that $\mathcal{F}$ is weakly involutive (indeed, the set $\mathcal{F}$ studied in Example 5.6 would be a simple counterexample). If $g = \sum_{\mu \in \mathbb{N}_0^n} \sum_{f \in \mathcal{F}} c_{\mu,f} x^\mu \star f$ is an arbitrary polynomial in $\langle \mathcal{F} \rangle$, then adding the involutive standard representations of all the products $x^\mu \star f$ for which $c_{\mu,f} \neq 0$ yields a representation

$g = \sum_{f\in\mathcal{F}} P_f \star f$ where $P_f \in \mathbb{k}[X_{L,\mathcal{F},\prec}(f)]$. But in general it will not satisfy the condition $\mathrm{le}_\prec(P_f \star f) \preceq \mathrm{le}_\prec g$ for all $f \in \mathcal{F}$, as we cannot assume that we started with an ordinary standard representation of g. The satisfaction of this condition is guaranteed only for involutively head autoreduced sets, as there it is impossible that the leading terms cancel (Lemma 5.12). For such sets the above proof simplifies, as all the sets $\mathcal{F}_i$ consist of precisely one element and thus no branching is necessary.

Corollary 7.3 *For a continuous division L an involutively head autoreduced set $\mathcal{F} \subset \mathcal{P}$ is involutive, if and only if it is locally involutive.*

As in the proof of Proposition 6.8, local involution of $\mathcal{H}$ is obviously equivalent to the termination condition $\mathcal{S} = \emptyset$ of the `loop` in Algorithm 3. Thus we are now in the position to prove the following result.

Theorem 7.4 *Let L be a constructive Noetherian involutive division and $(\mathcal{P}, \star, \prec)$ a polynomial algebra of solvable type. Then Algorithm 3 terminates for any finite input set $\mathcal{F}$ with an involutive basis of the ideal $\mathcal{I} = \langle\mathcal{F}\rangle$.*

Proof We begin by proving the *correctness* of the algorithm under the assumption that it terminates. The relation $\mathcal{I} = \langle\mathcal{H}\rangle$ remains valid throughout, although $\mathcal{H}$ changes. But the only changes are the addition of further elements of $\mathcal{I}$ and involutive head autoreductions; both operations do not affect the ideal generated by $\mathcal{H}$. When the algorithm terminates, we have $\mathcal{S} = \emptyset$ and thus the output $\mathcal{H}$ is locally involutive and by Corollary 7.3 involutive.

There remains the problem of *termination*. Algorithm 3 produces a sequence $(\mathcal{H}_1, \mathcal{H}_2, \dots)$ with $\langle\mathcal{H}_i\rangle = \mathcal{I}$. The set $\mathcal{H}_{i+1}$ is determined from $\mathcal{H}_i$ in Line /9/. We distinguish two cases, namely whether or not during the computation of the involutive normal form in Line /8/ the leading exponent changes. If $\mathrm{le}_\prec \bar{g} = \mathrm{le}_\prec g$, then $\langle\mathrm{le}_\prec \mathcal{H}_i\rangle = \langle\mathrm{le}_\prec \mathcal{H}_{i+1}\rangle$, as $\mathrm{le}_\prec g = \mathrm{le}_\prec h + 1_j$ for some $h \in \mathcal{H}_i$. Otherwise we claim that $\langle\mathrm{le}_\prec \mathcal{H}_i\rangle \subsetneq \langle\mathrm{le}_\prec \mathcal{H}_{i+1}\rangle$.

By construction, g is in involutive normal form with respect to the set $\mathcal{H}_i$ implying that $\mathrm{le}_\prec g \in \langle\mathrm{le}_\prec \mathcal{H}_i\rangle \setminus \langle\mathrm{le}_\prec \mathcal{H}_i\rangle_L$. If we had $\langle\mathrm{le}_\prec \mathcal{H}_i\rangle = \langle\mathrm{le}_\prec \mathcal{H}_{i+1}\rangle$, a polynomial $h \in \mathcal{H}_i$ would exist such that $\mathrm{le}_\prec g = \mathrm{le}_\prec h + \mu$ where the multi index μ has a non-vanishing entry μ_j for at least one non-multiplicative index $j \in \bar{N}_{L,\mathrm{le}_\prec \mathcal{H}_i}(h)$. This implies that $\mathrm{le}_\prec h + 1_j \preceq \mathrm{le}_\prec g \prec \mathrm{le}_\prec \bar{g}$. But we choose the polynomial $\bar{g}$ in Line /7/ such that its leading exponent is minimal among all non-multiplicative products $x_k \star h$ with $h \in \mathcal{H}_i$; hence $\mathrm{le}_\prec \bar{g} \preceq \mathrm{le}_\prec h + 1_j$. As this is a contradiction, we must have $\langle\mathrm{le}_\prec \mathcal{H}_i\rangle \subsetneq \langle\mathrm{le}_\prec \mathcal{H}_{i+1}\rangle$.

So the `loop` of Algorithm 3 generates an ascending chain of monoid ideals $\langle\mathrm{le}_\prec \mathcal{H}_1\rangle \subseteq \langle\mathrm{le}_\prec \mathcal{H}_2\rangle \subseteq \cdots \subseteq \mathrm{le}_\prec \mathcal{I}$. As $\mathbb{N}_0^n$ is Noetherian, the chain must become stationary at some index N. It follows from the considerations above that in all iterations of the `loop` after the Nth one $\mathrm{le}_\prec \bar{g} = \mathrm{le}_\prec g$ in Line /8/. At this stage Algorithm 3 reduces to an involutive completion of the monomial set $\mathrm{le}_\prec \mathcal{H}_N$ using Algorithm 2—but with additional involutive autoreductions after each appearance of a new element. Indeed, in Line /7/ we choose the polynomial $\bar{g}$ such that $\mathrm{le}_\prec \bar{g}$ is a possible choice for the multi index μ Algorithm 2 adds in Line /8/. Since

we assume that our division is Noetherian, it follows now from Proposition 6.8 together with Remark 6.9 that Algorithm 3 terminates (and the correctness proof above implies that in fact $\langle \mathrm{le}_\prec \mathcal{H}_N \rangle = \mathrm{le}_\prec \mathcal{I}$). □

Remark 7.5 If the division L is not Noetherian, then it may happen that, even when the ideal $\mathcal{I} = \langle \mathcal{F} \rangle$ does possess a finite involutive basis with respect to L, Algorithm 3 does not terminate for the input $\mathcal{F}$. We will see concrete examples for this phenomenon in Part II for the Pommaret division.

The problem is that the existence of an involutive basis for $\mathrm{le}_\prec \mathcal{I}$ does not imply that all subideals of it have also an involutive basis (as a trivial counterexample consider $\langle xy \rangle \subset \langle xy, y^2 \rangle$ with the Pommaret division). In such a case it may happen that at some stage of Algorithm 3 we encounter a basis $\mathcal{H}_i$ such that $\langle \mathrm{le}_\prec \mathcal{H}_i \rangle$ does not possess an involutive basis and then it is possible that the algorithm iterates endlessly in an attempt to complete $\mathrm{le}_\prec \mathcal{H}_i$.

This observation entails that variations of Theorem 7.4 hold also for divisions which are not Noetherian. For example, we could assume instead that all subideals of $\mathrm{le}_\prec \mathcal{I}$ possess an involutive basis. Alternatively, we could restrict to term orders of type ω. Then it suffices to assume that $\mathrm{le}_\prec \mathcal{I}$ has an involutive basis. Indeed, now it is not possible that Algorithm 3 iterates endlessly within $\mathrm{le}_\prec \mathcal{H}_i$, as sooner or later an element $\bar{g}$ must be selected in Line /7/ with $\mathrm{le}_\prec \bar{g} \notin \mathrm{le}_\prec \mathcal{H}_i$. ◁

Corollary 7.6 *For a constructive Noetherian division L every ideal $\mathcal{I} \subseteq \mathcal{P}$ possesses a finite involutive basis.*

Example 7.7 Now we are finally in the position to prove the claims made in Example 5.10. With respect to the degree reverse lexicographic term order the Janet (and the Pommaret) division assigns the polynomial $f_1 = z^2 - xy$ the multiplicative variables $\{x, y, z\}$ and the polynomials $f_2 = yz - x$ and $f_3 = y^2 - z$ the multiplicative variables $\{x, y\}$. Thus we must check the two non-multiplicative products: $zf_2 = yf_1 + xf_3$ and $zf_3 = yf_2 - f_1$. As both possess an involutive standard representation, the set $\mathcal{S}$ in Line /3/ of Algorithm 3 is empty in the first iteration and thus $\mathcal{F}$ is a Janet (and a Pommaret) basis of the ideal it generates.

The situation changes, if we use the degree inverse lexicographic term order, as then $\mathrm{lt}_\prec f_1 = xy$. Now $X_{J,\mathcal{F},\prec}(f_1) = \{x\}$, $X_{J,\mathcal{F},\prec}(f_2) = \{x, y, z\}$ and $X_{J,\mathcal{F},\prec}(f_3) = \{x, y\}$. In the first iteration we find $\mathcal{S} = \{zf_1\}$. Its involutive normal form is $f_4 = z^3 - x^2$ and we add this polynomial to $\mathcal{F}$ to obtain $\mathcal{H}_1 = \{f_1, f_2, f_3, f_4\}$ (the involutive head autoreduction does not change the set). For f_4 all variables are multiplicative; for the other generators there is one change: z is no longer multiplicative for f_2. Thus in the second iteration $\mathcal{S} = \{zf_2\}$. It is easy to check that this polynomial is already in involutive normal form with respect to $\mathcal{H}_1$ and we obtain $\mathcal{H}_2$ by adding $f_5 = yz^2 - xz$ to $\mathcal{H}_1$. In the next iteration $\mathcal{S}$ is empty, so that $\mathcal{H}_2$ is indeed the Janet basis of $\langle \mathcal{F} \rangle$ for the degree inverse lexicographic term order. ◁

The proof of Theorem 7.4 has an interesting consequence which was first discovered by Apel [3] for the special case of the Pommaret division (see also [21, Prop. 5.4] where for arbitrary divisions the case of degree compatible orders is considered). Assume that the term order $\prec$ is of type ω, i. e. for any two

multi indices μ, ν with $\mu \prec \nu$ only finitely many multi indices $\rho^{(i)}$ exist with $\mu \prec \rho^{(1)} \prec \rho^{(2)} \prec \cdots \prec \nu$. Then even if Algorithm 3 does *not* terminate, it determines in a finite number of steps a Gröbner basis of the ideal $\mathcal{I}$.

Proposition 7.8 *Let the term order $\prec$ be of type ω. Then Algorithm 3 determines for any finite input set $\mathcal{F} \subset \mathcal{P}$ and any involutive division L in a finite number of steps a Gröbner basis of the ideal $\mathcal{I} = \langle \mathcal{F} \rangle$.*

Proof Above we introduced the set $\mathcal{H}_N$ such that $\langle \mathrm{le}_\prec \mathcal{H}_{N+\ell} \rangle = \langle \mathrm{le}_\prec \mathcal{H}_N \rangle$ for all $\ell > 0$. We claim that $\mathcal{H}_N$ is a Gröbner basis of $\mathcal{I}$.

Let $f \in \mathcal{I}$ be an arbitrary element of the ideal. As $\mathcal{H}_N$ is a basis of $\mathcal{I}$, we find for each $h \in \mathcal{H}_N$ a polynomial $g_h \in \mathcal{P}$ such that

$$f = \sum_{h \in \mathcal{H}_N} g_h \star h \; . \tag{17}$$

$\mathcal{H}_N$ is a Gröbner basis, if and only if we can choose the coefficients g_h such that $\mathrm{le}_\prec (g_h \star h) \preceq \mathrm{le}_\prec f$. Assume that for f no such standard representation exists and let $\mu = \max_{h \in \mathcal{H}_N} \{ \mathrm{le}_\prec g_h + \mathrm{le}_\prec h \} \succ \mathrm{le}_\prec f$. If we denote by $\bar{\mathcal{H}}_N$ the set of all polynomials $\bar{h} \in \mathcal{H}_N$ for which $\mathrm{le}_\prec g_{\bar{h}} + \mathrm{le}_\prec \bar{h} = \mu$, then the identity $\sum_{\bar{h} \in \bar{\mathcal{H}}_N} \mathrm{lc}_\prec (g_{\bar{h}} \star \bar{h}) = 0$ must hold and hence $\bar{\mathcal{H}}_N$ contains at least two elements. For each element $\bar{h} \in \bar{\mathcal{H}}_N$ we have $\mu \in \mathcal{C}(\mathrm{le}_\prec \bar{h})$. As by construction the set $\mathcal{H}_N$ is involutively head autoreduced, the involutive cones of the leading exponents do not intersect and there must be at least one generator $\bar{h} \in \bar{\mathcal{H}}_N$ such that some non-multiplicative variable $x_j \in \bar{X}_{L,\mathcal{H}_N}(\bar{h})$ divides $\mathrm{lt}_\prec g_{\bar{h}}$.

As $\prec$ is of type ω, after a finite number of steps the non-multiplicative product $x_j \star \bar{h}$ is analysed in Algorithm 3. Thus for some $n_1 \geq 0$ the set $\mathcal{H}_{N+n_1}$ contains an element $\bar{h}'$ with $\mathrm{le}_\prec \bar{h}' = \mathrm{le}_\prec (x_j \star \bar{h})$. Let $\mu = \mathrm{le}_\prec g_{\bar{h}}$, $x^{\mu - 1_j} \star x_j = c x^\mu + r_1$ and $\bar{h}' = d x_j \star \bar{h} + r_2$. Then we may rewrite

$$g_{\bar{h}} \star \bar{h} = \frac{\mathrm{lc}_\prec g_{\bar{h}}}{cd} \Big[x^{\mu - 1_j} \star (\bar{h}' - r_2) - d r_1 \star \bar{h} \Big] + \big(g_{\bar{h}} - \mathrm{lm}_\prec g_{\bar{h}} \big) \star \bar{h} \; . \tag{18}$$

As $\bar{h}'$ was determined via an involutive normal form computation applied to the product $x_j \star \bar{h}$ and as we know that at this stage of the algorithm the leading exponent does not change during the computation, the leading exponent on the right hand side of (18) is $\mathrm{le}_\prec (x^{\mu - 1_j} \star \bar{h}')$. If the term $x^{\mu - 1_j}$ contains a non-multiplicative variable $x_k \in \bar{X}_{L,\mathcal{H}_{N+n_1}}(\bar{h}')$, we repeat the argument obtaining a polynomial $\bar{h}'' \in \mathcal{H}_{N+n_1+n_2}$ such that $\mathrm{le}_\prec \bar{h}'' = \mathrm{le}_\prec (x_k \star \bar{h}')$.

Obviously, this process terminates after a finite number of steps, even if we do it for each $\bar{h} \in \bar{\mathcal{H}}_N$. Thus after ℓ further iterations we obtain a set $\mathcal{H}_{N+\ell}$ such that, after applying all the found relations (18), f can be expressed in the form $f = \sum_{h \in \mathcal{H}_{N+\ell}} \tilde{g}_h \star h$ where still $\mu = \max_{h \in \mathcal{H}_{N+\ell}} \{ \mathrm{le}_\prec \tilde{g}_h + \mathrm{le}_\prec h \}$. Denote again by $\bar{\mathcal{H}}_{N+\ell} \subseteq \mathcal{H}_{N+\ell}$ the set of all polynomials $\bar{h}$ achieving this maximum.

By construction, no term $\mathrm{lt}_\prec \tilde{g}_{\bar{h}}$ with $\bar{h} \in \bar{\mathcal{H}}_{N+\ell}$ contains a variable that is non-multiplicative for $\bar{h}$. Thus we must now have $\mu \in \mathcal{C}_{\mathrm{le}_\prec (\mathcal{H}_{N+\ell}),L}(\mathrm{le}_\prec \bar{h})$ for each $\bar{h} \in \bar{\mathcal{H}}_{N+\ell}$ implying that $\bar{\mathcal{H}}_{N+\ell}$ contains at most one element. But then it is not possible that $\mu \succ \mathrm{le}_\prec f$. Hence each polynomial $f \in \mathcal{P}$ possesses a standard representation already with respect to $\mathcal{H}_N$ and this set is a Gröbner basis. □

Note that in the given form this result is only of theoretical interest, as in general no efficient method exists for checking whether the current basis is already a Gröbner basis. Using standard criteria would destroy all potential advantages of the involutive algorithm. For the special case of Pommaret bases, Apel [3] found a simple criterion that allows us to use a variant of Algorithm 3 for the construction of Gröbner bases independent of the existence of a finite involutive basis.

In contrast to the monomial case, one does not automatically obtain a minimal involutive basis by making some minor modifications of Algorithm 3. In particular, it does not suffice to apply it to a minimal basis in the ordinary sense. Gerdt and Blinkov [21, Sect. 5] presented an algorithm that always returns a minimal involutive basis provided a finite involutive basis exists. While it still follows the same basic strategy of study all products with non-multiplicative variables, it requires a more complicated organisation of the algorithm. We omit here the details.

8 Right and Two-Sided Bases

We now briefly discuss the relation between left and right involutive bases and the computation of bases for two-sided ideals. We use in this section the following notations: the left ideal generated by $\mathcal{F} \subset \mathcal{P}$ is denoted by $\langle \mathcal{F} \rangle^{(l)}$, the right ideal by $\langle \mathcal{F} \rangle^{(r)}$ and the two-sided ideal by $\langle\langle \mathcal{F} \rangle\rangle$ and corresponding notations for the left, right and two-sided involutive span.

Recall from Remark 4.8 that even with a coefficient field $\Bbbk$ it is not guaranteed that $\mathcal{P}$ is also right Noetherian and hence generally the existence of right Gröbner bases for right ideals is not clear. However, we also noted that the ring $\mathcal{P}$ is always right Noetherian, if we assume that the maps $\rho_i : \Bbbk \to \Bbbk$ in (8a) are automorphisms. In the sequel of this section we will always make this assumption.

From a computational point of view, the theory of right ideals is almost identical to the corresponding theory for left ideals. The left-right asymmetry in our definition of polynomial algebras of solvable type leads only to one complication. Suppose that we want to perform a right reduction of a term ax^ν with respect to another term cx^μ with $\mu \mid \nu$. This requires to find a coefficient $b \in \Bbbk$ such that $\mathrm{lc}_\prec (cx^\mu \star bx^{\nu-\mu}) = c\rho_\mu(b) r_{\mu,\nu-\mu} = a$. Since, according to the above made assumption, all the maps ρ_μ are automorphisms, such a b always exists. It turns out [42, Sect. 4.11] that under the made assumption the results of Kandry-Rodi and Weispfenning [41, Sects. 4/5] remain valid for our larger class of non-commutative algebras and can be straightforwardly extended to involutive bases.

Lemma 8.1 *A polynomial $f \in \mathcal{P}$ is (involutively) left reducible modulo a finite set $\mathcal{F} \subset \mathcal{P}$ (with respect to an involutive division L), if and only if it is (involutively) right reducible (with respect to L).*

Proof Because of the made assumptions on the maps ρ_μ, reducibility depends solely on the leading exponents. □

Proposition 8.2 *Let $\mathcal{H}_l$ be a monic, involutively left autoreduced, minimal left involutive set and $\mathcal{H}_r$ a monic, involutively right autoreduced, minimal right involutive set for an involutive division L. If $\langle \mathcal{H}_l \rangle^{(l)} = \langle \mathcal{H}_r \rangle^{(r)} = \mathcal{I}$, then $\mathcal{H}_l = \mathcal{H}_r$.*

Proof By definition of a minimal basis, the sets $\mathrm{le}_\prec \mathcal{H}_l$ and $\mathrm{le}_\prec \mathcal{H}_r$ are both minimal involutive bases of the monoid ideal $\mathrm{le}_\prec \mathcal{I}$ and thus are identical. Assume that $(\mathcal{H}_l \setminus \mathcal{H}_r) \cup (\mathcal{H}_r \setminus \mathcal{H}_l) \neq \emptyset$ and let f be an element of this set with minimal leading exponent with respect to $\prec$. Without loss of generality, we assume that $f \in \mathcal{H}_l \setminus \mathcal{H}_r$. Because of the condition $\langle \mathcal{H}_l \rangle^{(l)} = \langle \mathcal{H}_r \rangle^{(r)}$, we have $f \in \langle \mathcal{H}_r \rangle^{(r)}_{L,\prec}$. Thus the (by Proposition 5.13 unique) right involutive normal form of f with respect to $\mathcal{H}_r$ is 0. This implies in particular that f is right involutively reducible with respect to some $h \in \mathcal{H}_r$ with $\mathrm{le}_\prec h \preceq \mathrm{le}_\prec f$.

If $\mathrm{le}_\prec h \prec \mathrm{le}_\prec f$, then $h \in \mathcal{H}_l$, too, as f was chosen as a minimal element of the symmetric difference of $\mathcal{H}_l$ and $\mathcal{H}_r$. Hence, by Lemma 8.1, f is also left involutively reducible with respect to h (because of $\mathrm{le}_\prec \mathcal{H}_l = \mathrm{le}_\prec \mathcal{H}_r$ the multiplicative variables of h are the same in both cases). But this contradicts the assumption that $\mathcal{H}_l$ is involutively left autoreduced.

If $\mathrm{le}_\prec h = \mathrm{le}_\prec f = \mu$, then we consider the difference $g = f - h \in \mathcal{I}$: both the left involutive normal form of g with respect to $\mathcal{H}_l$ and the right involutive normal form with respect to $\mathcal{H}_r$ must vanish. By construction, $\mathrm{le}_\prec g \prec \mu$ and $\operatorname{supp} g \subseteq (\operatorname{supp} f \cup \operatorname{supp} h) \setminus \{\mu\}$. Since both $\mathcal{H}_l$ and $\mathcal{H}_r$ are assumed to be involutively autoreduced, no term in this set is involutively reducible by $\mathrm{le}_\prec \mathcal{H}_l = \mathrm{le}_\prec \mathcal{H}_r$ and hence we must have $\operatorname{supp} g = \emptyset$, i. e. $g = 0$, a contradiction. □

A direct derivation of a theory of two-sided involutive bases along the lines of Section 5 fails, as two-sided linear combinations are rather unwieldy objects. A general polynomial $f \in \langle\langle \mathcal{H} \rangle\rangle$ for some finite set $\mathcal{H} \subset \mathcal{P}$ is of the form

$$f = \sum_{h \in \mathcal{H}} \sum_{i=1}^{n_h} \ell_i \star h \star r_i \tag{19}$$

with polynomials $\ell_i, r_i \in \mathcal{P}$, i. e. we must allow several summands with the same generator h. The definition of a unique involutive standard representation would require control over the numbers n_h which seems rather difficult. Therefore we will take another approach and construct left involutive bases even for two-sided ideals. The following proposition is an involutive version of [41, Thm. 5.4].

Proposition 8.3 *Let $\mathcal{H} \subset (\mathcal{P}, \star, \prec)$ be a finite set and L an involutive division. Then the following five statements are equivalent.*

(i) *$\mathcal{H}$ is a left involutive basis and $\langle \mathcal{H} \rangle^{(l)} = \langle\langle \mathcal{H} \rangle\rangle$.*
(ii) *$\mathcal{H}$ is a right involutive basis and $\langle \mathcal{H} \rangle^{(r)} = \langle\langle \mathcal{H} \rangle\rangle$.*
(iii) *$\mathcal{H}$ is a left involutive basis of $\langle \mathcal{H} \rangle^{(l)}$ and both $h \star x_i \in \langle \mathcal{H} \rangle^{(l)}$ and $h \star c \in \langle \mathcal{H} \rangle^{(l)}$ for all generators $h \in \mathcal{H}$, all variables x_i and all coefficients $c \in \Bbbk$.*
(iv) *$\mathcal{H}$ is a right involutive basis of $\langle \mathcal{H} \rangle^{(r)}$ and both $x_i \star h \in \langle \mathcal{H} \rangle^{(r)}$ and $c \star h \in \langle \mathcal{H} \rangle^{(r)}$ for all generators $h \in \mathcal{H}$, all variables x_i and all coefficients $c \in \Bbbk$.*
(v) *A unique generator $h \in \mathcal{H}$ exists for every polynomial $f \in \langle\langle \mathcal{H} \rangle\rangle$ such that $\mathrm{le}_\prec h \,|_{L, \mathrm{le}_\prec \mathcal{H}}\, \mathrm{le}_\prec f$.*

Proof We begin with the equivalence of the first two statements. (i) implies that $\langle \mathcal{H} \rangle^{(l)}_{L,\prec} = \langle \mathcal{H} \rangle^{(l)} = \langle\langle \mathcal{H} \rangle\rangle$ and hence trivially $\langle \mathcal{H} \rangle^{(r)} \subseteq \langle \mathcal{H} \rangle^{(l)}$. The same argument as in the proof of Proposition 8.2 shows that we have in fact an equality and thus $\langle \mathcal{H} \rangle^{(r)}_{L,\prec} = \langle \mathcal{H} \rangle^{(r)} = \langle\langle \mathcal{H} \rangle\rangle$, i. e. (ii). The converse goes analogously.

Next we consider the equivalence of (i) and (iii); the equivalence of (ii) and (iv) follows by the same argument. (iii) is a trivial consequence of (i). For the converse, we note that (iii) implies that $f \star (ct) \in \langle\mathcal{H}\rangle^{(l)}$ for all $f \in \langle\mathcal{H}\rangle^{(l)}$, all terms $t \in \mathbb{T}$ and all constants $c \in \Bbbk$. Indeed, we may rewrite the monomial ct as a polynomial in the "terms" $x_{i_1} \star x_{i_2} \star \cdots \star x_{i_q}$ with $i_1 \leq i_2 \leq \cdots \leq i_q$ and then apply repeatedly our assumptions. Obviously, this entails (i).

The equivalence of (i) or (ii), respectively, with (v) is a trivial consequence of the definition of an involutive basis. □

We would like to exploit Statement (iii) for the construction of a left involutive basis for the two-sided ideal $\langle\!\langle\mathcal{F}\rangle\!\rangle$. However, if the field $\Bbbk$ is infinite, then it contains an infinite number of conditions. We make now one further assumption about the algebra $\mathcal{P}$. Let $\Bbbk_0 = \{c \in \Bbbk \mid \forall f \in \mathcal{P} : c \star f = f \star c\}$ be the constant part of the centre of $\mathcal{P}$. By analysing the products $x_i \star c^{-1} \star c$ for an arbitrary element $c \in \Bbbk_0^\times$, one easily proves that $\Bbbk_0$ is even a subfield of $\Bbbk$ [42, Sect. 4.11].

We make now the assumption that either $\Bbbk^\times = \{c_1, \ldots, c_\ell\}$ is finite or that the field extension $\Bbbk/\Bbbk_0$ is finite, i. e. that $\Bbbk$ is a finite-dimensional vector space over $\Bbbk_0$ with basis $\{c_1, \ldots, c_\ell\}$. In the latter case, it is easy to see that it suffices in (iii) to require that only all products $h \star c_j$ lie in $\langle\mathcal{H}\rangle^{(l)}$, as for $c = \sum_{j=1}^{\ell} \lambda_j c_j$ with $\lambda_j \in \Bbbk_0$ we have $h \star c = \sum_{j=1}^{\ell} \lambda_j (h \star c_j)$.

These considerations lead to the simple Algorithm 4 below. It first constructs in Line /1/ a left involutive basis $\mathcal{H}$ of the left ideal $\langle\mathcal{F}\rangle^{(l)}$ (using Algorithm 3). The `while` loop in Lines /2–19/ extends the set $\mathcal{H}$ to a left generating set of the two-sided ideal $\langle\!\langle\mathcal{F}\rangle\!\rangle$ according to our simplified version of Proposition 8.3 (iii). Finally, we complete in Line /20/ this set to an involutive basis. In Line /1/ it is not really necessary to compute a left involutive basis; any left Gröbner basis would suffice as well. Similarly, an ordinary left normal form could be used in Lines /6/ and /12/, respectively; the use of $\texttt{InvLeftNormalForm}_{L,\prec}$ anticipates the final involutive basis computation in Line /20/.

The termination of the `while` loop follows from the fact that under the made assumptions $\mathcal{P}$ is Noetherian and hence a finite generating set of $\langle\!\langle\mathcal{F}\rangle\!\rangle$ exists. In principle, we perform here a simple breadth-first search for it. The termination of the involutive bases computations in Lines /1/ and /20/, respectively, depends on the conditions discussed in the last section. Thus the termination is guaranteed, if the division L is constructive and Noetherian.

9 Involutive Bases for Semigroup Orders

For many applications it is of interest to compute involutive or Gröbner bases with respect to more general orders, namely *semigroup orders* (see Appendix A). This generalisation does not affect the basic properties of polynomial algebras of solvable type as discussed in Section 3, but if 1 is no longer the smallest term, then normal form computations do no longer terminate for all inputs. So we can no longer apply Algorithm 3 directly for the determination of involutive bases.

Algorithm 4 Left Involutive basis for two-sided ideal in $(\mathcal{P}, \star, \prec)$

Input: finite set $\mathcal{F} \subset \mathcal{P}$, involutive division L
Output: left involutive basis $\mathcal{H}$ of $\langle\langle \mathcal{F} \rangle\rangle$
/1/ $\mathcal{H} \leftarrow \mathtt{LeftInvBasis}_{L,\prec}(\mathcal{F})$; $\mathcal{S} \leftarrow \mathcal{H}$
/2/ **while** $\mathcal{S} \neq \emptyset$ **do**
/3/ $\mathcal{T} \leftarrow \emptyset$
/4/ **for all** $f \in \mathcal{S}$ **do**
/5/ **for** i **from** 1 **to** n **do**
/6/ $h \leftarrow \mathtt{InvLeftNormalForm}_{L,\prec}(f \star x_i, \mathcal{H})$
/7/ **if** $h \neq 0$ **then**
/8/ $\mathcal{H} \leftarrow \mathcal{H} \cup \{h\}$; $\mathcal{T} \leftarrow \mathcal{T} \cup \{h\}$
/9/ **end_if**
/10/ **end_for**
/11/ **for** j **from** 1 **to** ℓ **do**
/12/ $h \leftarrow \mathtt{InvLeftNormalForm}_{L,\prec}(f \star c_j, \mathcal{H})$
/13/ **if** $h \neq 0$ **then**
/14/ $\mathcal{H} \leftarrow \mathcal{H} \cup \{h\}$; $\mathcal{T} \leftarrow \mathcal{T} \cup \{h\}$
/15/ **end_if**
/16/ **end_for**
/17/ **end_for**
/18/ $\mathcal{S} \leftarrow \mathcal{T}$
/19/ **end_while**
/20/ **return** $\mathtt{LeftInvBasis}_{L,\prec}(\mathcal{H})$

Example 9.1 The *Weyl algebra* $\mathbb{W}_n$ is the polynomial algebra in the $2n$ variables $x_1, \ldots, x_n$ and $\partial_1, \ldots, \partial_n$ with the following non-commutative product $\star$: for all $1 \leq i \leq n$ we have $\partial_i \star x_i = x_i \partial_i + 1$ and $\star$ is the normal commutative product in all other cases. It is easy to see that $\mathbb{W}_n$ is a polynomial algebra of solvable type for any monoid order. A semigroup order respects the multiplication $\star$ only, if $1 \prec x_i \partial_i$ for all i. In [54] such orders are called *multiplicative monomial orders*.

An important class of semigroup orders is defined via real weight vectors. Let $(\xi, \zeta) \in \mathbb{R}^n \times \mathbb{R}^n$ be such that $\xi + \zeta \in \mathbb{R}^n$ is non-negative and let $\prec$ be an arbitrary monoid order. Then we define $x^\mu \partial^\nu \prec_{(\xi,\zeta)} x^\sigma \partial^\tau$, if either $\mu \cdot \xi + \nu \cdot \zeta < \sigma \cdot \xi + \tau \cdot \zeta$ or $\mu \cdot \xi + \nu \cdot \zeta = \sigma \cdot \xi + \tau \cdot \zeta$ and $x^\mu \partial^\nu \prec x^\sigma \partial^\tau$. This yields a monoid order, if and only if both ξ and ζ are non-negative. A special case are the orders with weight vectors $(\xi, -\xi)$ arising from the action of the algebraic torus $(\mathbb{k}^*)^n$ on the Weyl algebra. They have numerous applications in the theory of $\mathcal{D}$-modules [54]. $\lhd$

As normal form computations do not necessarily terminate for semigroup orders, we must slightly modify our definitions of (weak) involutive or Gröbner bases. The proof of Theorem 5.4 (and consequently also the one of Corollary 5.5 showing that a weak involutive basis of an ideal $\mathcal{I}$ is indeed a basis of $\mathcal{I}$) requires normal form computations and thus this theorem is no longer valid. The same problem occurs for Gröbner bases. Therefore we must explicitly include this condition in our definition.

Definition 9.2 *Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type where $\prec$ is an arbitrary semigroup order. Let furthermore $\mathcal{I} \subseteq \mathcal{P}$ be a left ideal. A* Gröbner

basis *of $\mathcal{I}$ is a finite set $\mathcal{G}$ such that $\langle\mathcal{G}\rangle = \mathcal{I}$ and $\langle \mathrm{le}_\prec \mathcal{G}\rangle = \mathrm{le}_\prec \mathcal{I}$. The set $\mathcal{G}$ is a* weak involutive basis *of $\mathcal{I}$ for the involutive division L, if in addition the set $\mathrm{le}_\prec \mathcal{G}$ is weakly involutive for L. It is a* (strong) involutive basis, *if it is furthermore involutively head autoreduced.*

In the case of Gröbner bases, a classical trick due to Lazard [43] consists of homogenising the input and lifting the semigroup order to a monoid order on the homogenised terms. One can show that computing first a Gröbner basis for the ideal spanned by the homogenised input and then dehomogenising yields a Gröbner basis with respect to the semigroup order. Note, however, that in general we cannot expect that *reduced* Gröbner bases exist.

We extend now this approach to involutive bases. Here we encounter the additional difficulty that we must lift not only the order but also the used involutive division. In particular, we must show that properties like being Noetherian or continuity are preserved by the lift which is non-trivial. For the special case of involutive bases in the Weyl algebra, this problem was first solved in [35]. As most arguments are independent of the actually used algebra of solvable type, we recall here the results of [35] without proofs (all details can be found in [55, Sect. 4.5]).

Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type where $\prec$ is any semigroup order that respects the multiplication $\star$. We set $\tilde{\mathcal{P}} = \Bbbk[x_0, x_1, \ldots, x_n]$ and extend the multiplication $\star$ to $\tilde{\mathcal{P}}$ by defining that x_0 commutes with all other variables and the elements of the field $\Bbbk$. For a polynomial $f = \sum c_\mu x^\mu \in \mathcal{P}$ of degree q, we introduce as usual its *homogenisation* $f^{(h)} = \sum c_\mu x_0^{q-|\mu|} x^\mu \in \tilde{\mathcal{P}}$. Conversely, for a polynomial $\tilde{f} \in \tilde{\mathcal{P}}$ we denote its projection to $\mathcal{P}$ as $f = \tilde{f}|_{x_0=1}$.

We denote by $\tilde{\mathbb{T}}$ the set of terms in $\tilde{\mathcal{P}}$; obviously, it is in one-to-one correspondence to the multi indices in $\mathbb{N}_0^{n+1}$. We use in the sequel the following convention. Multi indices in $\mathbb{N}_0^{n+1}$ always carry a tilde: $\tilde{\mu} = [\mu_0, \ldots, \mu_n]$. The projection to $\mathbb{N}_0^n$ defined by dropping the first entry (i. e. the exponent of the homogenisation variable x_0) is signalled by omitting the tilde; thus $\mu = [\mu_1, \ldots, \mu_n]$. For subsets $\tilde{\mathcal{N}} \subset \mathbb{N}_0^{n+1}$ we also simply write $\mathcal{N} = \{\nu \mid \tilde{\nu} \in \tilde{\mathcal{N}}\} \subset \mathbb{N}_0^n$.

We lift the semigroup order $\prec$ on $\mathbb{T}$ to a monoid order $\prec_h$ on $\tilde{\mathbb{T}}$ by defining $x^{\tilde{\mu}} \prec_h x^{\tilde{\nu}}$, if either $|\tilde{\mu}| < |\tilde{\nu}|$ or both $|\tilde{\mu}| = |\tilde{\nu}|$ and $x^\mu \prec x^\nu$. It is trivial to check that this yields indeed a monoid order and that $(\tilde{\mathcal{P}}, \star, \prec_h)$ is again a polynomial algebra of solvable type. For lifting the involutive division, we proceed somewhat similarly to the definition of the Janet division: the homogenisation variable x_0 is multiplicative only for terms which have maximal degree in x_0.

Proposition 9.3 ([35, Prop. 5.1]) *Let L be an involutive division on $\mathbb{N}_0^n$. For any finite set $\tilde{\mathcal{N}} \subset \mathbb{N}_0^{n+1}$ and every multi index $\tilde{\mu} \in \tilde{\mathcal{N}}$, we define $N_{\tilde{L},\tilde{\mathcal{N}}}(\tilde{\mu})$ by:*

- *$0 \in N_{\tilde{L},\tilde{\mathcal{N}}}(\tilde{\mu})$, if and only if $\mu_0 = \max_{\tilde{\nu}\in\tilde{\mathcal{N}}}\{\nu_0\}$,*
- *$0 < i \in N_{\tilde{L},\tilde{\mathcal{N}}}(\tilde{\mu})$, if and only if $i \in N_{L,\mathcal{N}}(\mu)$.*

This determines an involutive division $\tilde{L}$ on $\mathbb{N}_0^{n+1}$.

Now we must check to what extent the properties of L are inherited by the lifted division $\tilde{L}$. As the definition of $\tilde{L}$ is very similar to the one of the Janet division, the proofs of the following results reuse many techniques from the corresponding proofs for the Janet division.

Proposition 9.4 ([35, Prop. 5.2]) *If L is a Noetherian division, then so is $\tilde{L}$.*

Proposition 9.5 ([35, Prop. 5.3]) *If L is a continuous division, then so is $\tilde{L}$.*

Unfortunately, it is much harder to show that constructivity is preserved. So far, a proof is known only for globally defined divisions and the Janet division.

Proposition 9.6 ([35, Prop. 5.4]) *If the continuous division L is either globally defined or the Janet division, then the lifted division $\tilde{L}$ is constructive.*

Based on these results, Algorithm 3 can be extended to semigroup orders. Given a finite set $\mathcal{F} \in \mathcal{P}$, we first determine its homogenisation $\mathcal{F}^{(h)} \in \tilde{\mathcal{P}}$ and then compute an involutive basis of $\langle F^{(h)} \rangle$ with respect to $\tilde{L}$ and $\prec_h$. What remains to be done is first to show that the existence of a finite involutive basis is preserved under the lifting to $\tilde{\mathcal{P}}$ and then to study the properties of the dehomogenisation of this basis.

Proposition 9.7 ([35, Prop. 6.1]) *If the left ideal $\mathcal{I} = \langle \mathcal{F} \rangle \subseteq \mathcal{P}$ possesses an involutive basis with respect to the Noetherian division L and the semigroup order $\prec$, then the left ideal $\tilde{\mathcal{I}} = \langle \mathcal{F}^{(h)} \rangle \subseteq \tilde{\mathcal{P}}$ generated by the homogenisations of the elements in the finite set $\mathcal{F}$ possesses an involutive basis with respect to the lifted division $\tilde{L}$ and the monoid order $\prec_h$.*

Hence our lifting leads to a situation where we can apply Theorem 7.4. Unfortunately, the dehomogenisation of the strong involutive basis computed in $\tilde{\mathcal{P}}$ does not necessarily lead to a *strong* involutive basis in $\mathcal{P}$, but we obtain always at least a weak involutive basis and thus in particular a Gröbner basis. Note also that the dehomogenised basis is in general smaller than the basis in $\tilde{\mathcal{P}}$, as some elements of the latter one may differ only in powers of the homogenisation variable x_0.

Theorem 9.8 ([35, Thm. 6.1]) *Let $\tilde{\mathcal{H}}$ be a strong involutive basis of the left ideal $\tilde{\mathcal{I}} \subseteq \tilde{\mathcal{P}}$ with respect to $\tilde{L}$ and $\prec_h$. Then the dehomogenisation $\mathcal{H}$ is a weak involutive basis of the left ideal $\mathcal{I} \subseteq \mathcal{P}$ with respect to L and $\prec$.*

Remark 9.9 For the Pommaret division P the situation is considerably simpler. There is no need to define a lifted division $\tilde{P}$ according to Proposition 9.3. Instead we renumber x_0 to x_{n+1} and then use the standard Pommaret division on $\mathbb{N}_0^{n+1}$. This approach implies that for all multi indices $\tilde{\mu} \in \mathbb{N}_0^{n+1}$ with $\mu \neq 0$ the equality $N_P(\tilde{\mu}) = N_P(\mu)$ holds, as obviously $n+1$ is multiplicative only for multi indices of the form $\tilde{\mu} = \ell_{n+1}$, i. e. for which $\mu = 0$. One easily sees that the above proof of Theorem 9.8 is not affected by this change of the division used in $\mathbb{N}_0^{n+1}$ and hence remains true. ◁

It is not a shortcoming of our proof that in general we do not get a strong involutive basis, but actually some ideals do not possess strong involutive bases. In particular, there is no point in invoking Proposition 5.7 for obtaining a strong basis. While we may surely obtain by elimination a subset $\mathcal{H}' \subseteq \mathcal{H}$ such that $\mathrm{le}_\prec \mathcal{H}'$ is a strong involutive basis of $\langle \mathrm{le}_\prec \mathcal{H} \rangle$, in general $\langle \mathcal{H}' \rangle \subsetneq \mathcal{I}$.

Example 9.10 Consider in the Weyl algebra $\mathbb{W}_2 = \mathbb{k}[x, y, \partial_x, \partial_y]$ the left ideal generated by the set $\mathcal{F} = \{\underline{1} + x + y, \underline{\partial_y} - \partial_x\}$. We take the semigroup order induced by the weight vector $(-1, -1, 1, 1)$ and refined by a term order for which $\partial_y \succ \partial_x \succ y \succ x$. Then the underlined terms are the leading ones. One easily checks that $\mathcal{F}$ is a Gröbner basis for this order. Furthermore, all variables are multiplicative for each generator with respect to the Pommaret division and thus $\mathcal{F}$ is a weak Pommaret basis, too.

Obviously, the set $\mathcal{F}$ is neither a reduced Gröbner basis nor a strong Pommaret basis, as 1 is a (multiplicative) divisor of ∂_y. However, it is easy to see that the left ideal $\mathcal{I} = \langle \mathcal{F} \rangle$ does not possess a reduced Gröbner basis or a strong Pommaret basis. Indeed, we have $\mathrm{le}_\prec \mathcal{I} = \mathbb{N}_0^4$ and thus such a basis had to consist of only a single generator; but $\mathcal{I}$ is not a principal ideal. $\lhd$

A special situation arises for the Janet division. Recall from Remark 2.6 that any finite set $\mathcal{N} \subset \mathbb{N}_0^n$ is automatically involutively autoreduced with respect to the Janet division. Thus any weak Janet basis is a strong basis, if all generators have different leading exponents. If we follow the above outlined strategy of applying Algorithm 3 to a homogenised basis and then dehomogenising the result, we cannot generally expect this condition to be satisfied. However, with a minor modification of the algorithm we can achieve this goal.

Theorem 9.11 ([35, Thm. 6.2]) *Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type where $\prec$ is an arbitrary semigroup order. Then every left ideal $\mathcal{I} \subseteq \mathcal{P}$ possesses a strong Janet basis for $\prec$.*

Proof Assume that at some intermediate stage of Algorithm 3 the basis $\tilde{\mathcal{H}}$ contains two polynomials $\tilde{f}$ and $\tilde{g}$ such that $\mathrm{le}_{\prec_h}(\tilde{g}) = \mathrm{le}_{\prec_h}(\tilde{f}) + 1_0$, i. e. the leading exponents differ only in the first entry. If $\tilde{g} = x_0 \tilde{f}$, we will find $f = g$ after dehomogenisation and no obstruction to a strong basis appears. Otherwise we note that, by definition of the lifted Janet division J_h, the homogenisation variable x_0 is non-multiplicative for $\tilde{f}$. Thus at some later stage the algorithm must consider the non-multiplicative product $x_0 \tilde{f}$ (if it was already treated, $\tilde{\mathcal{H}}$ would not be involutively head autoreduced).

In the usual algorithm, we then determine the involutive normal form of the polynomial $x_0 \tilde{f}$; the first step of this computation is to replace $x_0 \tilde{f}$ by $x_0 \tilde{f} - \tilde{g}$. Alternatively, we may proceed instead as follows. The polynomial $\tilde{g}$ is removed from the basis $\tilde{\mathcal{H}}$ and replaced by $x_0 \tilde{f}$. Then we continue by analysing the involutive normal form of $\tilde{g}$ with respect to the new basis. Note that this modification concerns only the situation that a multiplication by x_0 has been performed and that the basis $\tilde{\mathcal{H}}$ contains already an element with the same leading exponent as the obtained polynomial.

If the final output $\tilde{\mathcal{H}}$ of the thus modified completion algorithm contains two polynomials $\tilde{g}$ and $\tilde{f}$ such that $\mathrm{le}_{\prec_h}(\tilde{g})$ and $\mathrm{le}_{\prec_h}(\tilde{f})$ differ only in the first entry, then either $\tilde{g} = x_0^k \tilde{f}$ or $\tilde{f} = x_0^k \tilde{g}$ for some $k \in \mathbb{N}$. Thus the dehomogenisation yields a basis $\mathcal{H}$ where all elements possess different leading exponents and $\mathcal{H}$ is a strong Janet basis. Looking at the proof of Theorem 7.4, it is easy to see that this modification does not affect the correctness and the termination of the

algorithm. As the Janet division is Noetherian, these considerations prove together with Proposition 9.4 the assertion. □

Note that our modification only achieves its goal, if we really restrict in Algorithm 3 to head reductions. Otherwise some other terms than the leading term in $x_0\tilde{f}$ might be reducible but not the corresponding terms in $\tilde{f}$. Then we could still find after dehomogenisation two generators with the same leading exponent.

Example 9.12 Consider in the Weyl algebra $\mathbb{W}_3$ with the three variables x, y, z the left ideal generated by the set $\mathcal{F} = \{\partial_z - y\partial_x,\, \partial_y\}$. If we apply the usual involutive completion Algorithm 3 (to the homogenisation $\mathcal{F}^{(h)}$), we obtain for the weight vector $(-1,0,0,1,0,0)$ refined by the degree reverse lexicographic order and the Janet division the following weak basis with nine generators:

$$\mathcal{H}_1 = \left\{ \partial_x,\, \partial_y,\, \partial_z,\, \partial_x\partial_z,\, \partial_y\partial_z,\, y\partial_x,\, y\partial_x + \partial_z,\, y\partial_x\partial_z,\, y\partial_x\partial_z + \partial_z^2 \right\}. \quad (20)$$

As one easily sees from the last four generators, it is not a strong basis.

Applying the modified algorithm for the Janet division yields the following basis with only seven generators:

$$\mathcal{H}_2 = \left\{ \partial_x + \partial_y\partial_z,\, \partial_y,\, \partial_z,\, \partial_x\partial_z,\, \partial_y\partial_z,\, y\partial_x + \partial_z,\, y\partial_x\partial_z + \partial_z^2 \right\}. \quad (21)$$

Obviously, we now have a strong basis, as all leading exponents are different.

This example also demonstrates the profound effect of the homogenisation. A strong Janet or Pommaret basis of $\langle\mathcal{F}\rangle$ is simply given by $\mathcal{H} = \{\partial_x,\, \partial_y,\, \partial_z\}$ which is simultaneously a reduced Gröbner basis. In $\langle\mathcal{F}^{(h)}\rangle$ many reductions are not possible because the terms contain different powers of t. However, this is a general problem of all approaches to Gröbner bases for semigroup orders using homogenisation and not specific for the involutive approach.

In this particular case, one could have applied the involutive completion algorithm directly to the original set $\mathcal{F}$ and it would have terminated with the minimal basis $\mathcal{H}$, although we are using an order which is not a monoid order. Unfortunately, it is not clear how to predict when infinite reduction chains appear in normal form computations with respect to such orders, so that one does not know in advance whether one may dispense with the homogenisation. ◁

10 Involutive Bases for Semigroup Orders II: Mora's Normal Form

One computational disadvantage of the approach outlined in the previous section is that the basis $\tilde{\mathcal{H}}$ in the homogenised algebra $\tilde{\mathcal{P}}$ is often much larger than the final basis $\mathcal{H}$ in the original algebra $\mathcal{P}$, as upon dehomogenisation generators may become identical. Furthermore, we have seen that it is difficult to prove the constructivity of the lifted division L_h which limits the applicability of this technique. Finally, for most divisions we are not able to determine strong bases.

An alternative approach for Gröbner bases computations in the ordinary polynomial ring was proposed first by Greuel and Pfister [29] and later independently by Gräbe [27,28]; extensive textbook discussions are contained in [16, Chapt. 4]

and [30, Sect. 1.6]. It allows us to dispense completely with computing in the homogenised algebra $\tilde{\mathcal{P}}$. Two ideas are the core of this approach: we modify the normal form algorithm using ideas developed by Mora [49] for the computation of tangent cones and we work over a ring of fractions of $\mathcal{P}$. We will now show that a generalisation to arbitrary polynomial algebras of solvable type and to involutive normal forms is possible and removes all the mentioned problems.

The central problem in working with semigroup orders is that they are no longer well-orders and hence normal form computations in the classical form do not necessarily terminate. Mora [49] introduced the notion of the *écart* of a polynomial f as the difference between the lowest and the highest degree of a term in f and based a new normal form algorithm on it which always terminates. The main differences between it and the usual algorithm lie in the possibility to reduce also with respect to intermediate results (see Line /9/ in Algorithm 5 below) and that it computes only a "weak" normal form (cf. Proposition 10.1 below).

Mora's approach is valid only for tangent cone orders where the leading term is always of minimal degree. Greuel and Pfister [29] noticed that a slight modification of the definition of the écart allows us to use it for arbitrary semigroup orders. So we set for any polynomial $f \in \mathcal{P} \setminus \{0\}$ and any semigroup order $\prec$

$$\text{écart}\, f = \deg f - \deg \mathrm{lt}_{\prec} f \ . \tag{22}$$

The extension of the Mora normal form to an involutive normal form faces one problem. As already mentioned, one allows here also reductions with respect to some intermediate results and thus one must decide on the assignment of multiplicative variables to these. However, it immediately follows from the proof of the correctness of the Mora algorithm how this assignment must be done in order to obtain in the end an involutive standard representation with respect to the set $\mathcal{G}$ (one should stress that this assignment is *not* performed according to some involutive division in the sense of Definition 2.1).

In Algorithm 5 below we use the following approach. To each member g of the set $\hat{\mathcal{G}}$ with respect to which we reduce we assign a set $N[g]$ of multiplicative indices. We write $\mathrm{le}_{\prec} g \,|_N\, \mathrm{le}_{\prec} h$, if the multi index $\mathrm{le}_{\prec} h$ lies in the restricted cone of $\mathrm{le}_{\prec} g$ defined by $N[g]$. The set $\mathcal{S}$ collects all generators $g \in \mathcal{G}$ which have already been used for reductions and the set $\mathcal{N}$ is the intersection of the corresponding sets of multiplicative indices. If a new polynomial h is added to $\hat{\mathcal{G}}$, it is assigned as multiplicative indices the current value of $\mathcal{N}$.

Proposition 10.1 *Algorithm 5 always terminates. Let $(\mathcal{P} = \mathbb{k}[X], \star, \prec)$ be a polynomial algebra of solvable type (for an arbitrary semigroup order $\prec$) such that $\mathbb{k}[X']$ is a subring of $\mathcal{P}$ for any subset $X' \subset X$. Then the output h is a* weak involutive normal form *of the input f with respect to the set $\mathcal{G}$ in the sense that there exists a polynomial $u \in \mathcal{P}$ with $\mathrm{le}_{\prec} u = 0$ such that the difference $u \star f - h$ possesses an involutive standard representation*

$$u \star f - h = \sum_{g \in \mathcal{G}} P_g \star g \tag{23}$$

and none of the leading exponents $\mathrm{le}_{\prec} g$ involutively divides $\mathrm{le}_{\prec} h$. If $\prec$ is a monoid order, then $u = 1$ and h is an involutive normal form in the usual sense.

Algorithm 5 Involutive Mora normal form for a semigroup order $\prec$ on $\mathcal{P}$

Input: polynomial $f \in \mathcal{P}$, finite set $\mathcal{G} \subset \mathcal{P}$, involutive division L
Output: involutive Mora normal form h of f with respect to $\mathcal{G}$
/1/ $h \leftarrow f$; $\hat{\mathcal{G}} \leftarrow \mathcal{G}$
/2/ **for all** $g \in \mathcal{G}$ **do**
/3/ $N[g] \leftarrow N_{L,\mathrm{le}_\prec \mathcal{G}}(\mathrm{le}_\prec g)$
/4/ **end_for**
/5/ $\mathcal{N} \leftarrow \{1,\dots,n\}$; $\mathcal{S} \leftarrow \emptyset$
/6/ **while** $(h \neq 0) \wedge (\exists\, g \in \hat{\mathcal{G}} : \mathrm{le}_\prec g \,|_N\, \mathrm{le}_\prec h)$ **do**
/7/ choose g with écart g minimal among all $g \in \hat{\mathcal{G}}$ such that $\mathrm{le}_\prec g \,|_N\, \mathrm{le}_\prec h$
/8/ **if** $(g \in \mathcal{G}) \wedge (g \notin \mathcal{S})$ **then**
/9/ $\mathcal{S} \leftarrow \mathcal{S} \cup \{g\}$; $\mathcal{N} \leftarrow \mathcal{N} \cap N[g]$
/10/ **end_if**
/11/ **if** écart $g >$ écart h **then**
/12/ $\hat{\mathcal{G}} \leftarrow \hat{\mathcal{G}} \cup \{h\}$; $N[h] \leftarrow \mathcal{N}$
/13/ **end_if**
/14/ $\mu \leftarrow \mathrm{le}_\prec h - \mathrm{le}_\prec g$; $h \leftarrow h - \frac{\mathrm{lc}_\prec h}{\mathrm{lc}_\prec (x^\mu \star g)} x^\mu \star g$
/15/ **end_while**
/16/ **return** h

Proof As the proof is almost identical to the one for the non-involutive version of the Mora normal form given by Greuel and Pfister [29,30], we only sketch the required modifications; full details are given in [55, Sect. 4.51]. For the termination proof no modifications are needed. For the existence of the involutive standard representation one uses the same induction as in the non-involutive case and keeps track of the multiplicative variables. The key point is that if a reduction with respect to a polynomial $\hat{g} \in \hat{\mathcal{G}} \setminus \mathcal{G}$ is performed, then it is multiplied only with terms which are multiplicative for all $g \in \mathcal{G}$ appearing in $\hat{g}$. This fact ensures that in the end indeed each non-zero coefficient P_g is contained in $\Bbbk[X_{L,\mathcal{G},\prec}(g)]$. □

Remark 10.2 The assumption about $\mathcal{P}$ in Proposition 10.1 is necessary, because the coefficients P_g in (23) are the result of multiplications. While the above considerations ensure that each factor lies in $\Bbbk[X_{L,\mathcal{G},\prec}(g)]$, it is unclear in a general polynomial algebra whether this remains true for their product. Simple examples for polynomial algebras of solvable type satisfying the made assumption are rings of linear difference or differential operators. In the case of the Pommaret division, the assumption can be weaken a bit and every iterated polynomial algebra of solvable type in the sense of Definition 4.1 is permitted, too. ◁

We move now to a larger ring of fractions where all polynomials with leading exponent 0 are units. In such a ring it really makes sense to call h a (weak) normal form of f, as we multiply f only by a unit.

Proposition 10.3 *Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type where $\prec$ is a semigroup order. Then the subset*

$$\mathcal{S}_\prec = \{f \in \mathcal{P} \mid \mathrm{le}_\prec f = 0\}\,. \tag{24}$$

is multiplicatively closed and the left localisation $\mathcal{P}_\prec = \mathcal{S}_\prec^{-1} \star \mathcal{P}$ is a well defined ring of left fractions.

Proof Obviously, $1 \in \mathcal{S}_\prec$. If $1 + f$ and $1 + g$ are two elements in $\mathcal{S}_\prec$, then the compatibility of the order $\prec$ with the multiplication $\star$ ensures that their product is of the form $(1 + f) \star (1 + g) = 1 + h$ with $\mathrm{le}_\prec h \prec 0$. Hence the set $\mathcal{S}_\prec$ is multiplicatively closed.

As polynomial algebras of solvable type do not possess zero divisors, a sufficient condition for the existence of the ring of left fractions $\mathcal{S}_\prec^{-1} \star \mathcal{P}$ is that for all $f \in \mathcal{S}_\prec$ and $g \in \mathcal{P}$ the intersection $(\mathcal{P} \star f) \cap (\mathcal{S}_\prec \star g)$ is not empty [15, Sect. 12.1]. But this fact can be shown using minor modifications of our proof of Proposition 3.5 on the existence of Ore multipliers.

We first choose coefficients $r_0, s_0 \in \mathcal{R}$ such that in $\bar{h}_1 = r_0 g \star f - s_0 f \star g$ the leading terms cancel, i. e. we have $\mathrm{le}_\prec \bar{h}_1 \prec \mathrm{le}_\prec f + \mathrm{le}_\prec g = \mathrm{le}_\prec g$. Then we compute with (the non-involutive form of) Algorithm 5 a weak normal form h_1 of $\bar{h}_1$ with respect to the set $\mathcal{F}_0 = \{f, g\}$. By Proposition 10.1 this yields a standard representation $u_1 \star \bar{h}_1 - h_1 = \phi_0 \star f + \psi_0 \star g$ where $\mathrm{le}_\prec u_1 = 0$. Assume that $\mathrm{le}_\prec \psi_0 \succeq 0$. Then we arrive at the contradiction $\mathrm{le}_\prec (\psi_0 \star g) \succeq \mathrm{le}_\prec g \succ \mathrm{le}_\prec \bar{h}_1 = \mathrm{le}_\prec (u_1 \star \bar{h}_1)$. Thus $\mathrm{le}_\prec \psi_0 \prec 0$. If $h_1 = 0$, then $(u_1 \star r_0 g - \phi_0) \star f = (u_1 \star s_0 f + \psi_0) \star g$ and by the considerations above on the leading exponents $u_1 \star s_0 f + \psi_0 \in \mathcal{S}_\prec$ so that indeed $(\mathcal{P} \star f) \cap (\mathcal{S}_\prec \star g) \neq \emptyset$.

If $h_1 \neq 0$, we proceed as in the proof of Proposition 3.5. We introduce $\mathcal{F}_1 = \mathcal{F}_0 \cup \{h_1\}$ and choose $r_1, s_1 \in \mathcal{R}$ such that in $\bar{h}_2 = r_1 h_1 \star f - s_1 f \star h_1$ the leading terms cancel. If we compute a weak Mora normal form h_2 of $\bar{h}_2$, then we obtain a standard representation $u_2 \star \bar{h}_2 - h_2 = \phi_1 \star f + \psi_1 \star g + \rho_1 \star h_1$ where again $\mathrm{le}_\prec u_2 = 0$. The properties of a standard representation imply now that $\mathrm{le}_\prec \psi_1 + \mathrm{le}_\prec g \preceq \mathrm{le}_\prec \bar{h}_2$ and $\mathrm{le}_\prec \rho_1 + \mathrm{le}_\prec h_1 \preceq \mathrm{le}_\prec \bar{h}_2$. Together with the inequalities $\mathrm{le}_\prec \bar{h}_2 \prec \mathrm{le}_\prec f + \mathrm{le}_\prec h_1 = \mathrm{le}_\prec h_1 \prec \mathrm{le}_\prec g$ this entails that both $\mathrm{le}_\prec \psi_1 \prec 0$ and $\mathrm{le}_\prec \rho_1 \prec 0$. Thus for $h_2 = 0$ we have found $\phi \in \mathcal{P}$ and $\psi \in \mathcal{S}_\prec$ such that $\phi \star f = \psi \star g$. If $h_2 \neq 0$, similar inequalities in the subsequent iterations ensure that we always have $\psi \in \mathcal{S}_\prec$. □

As any localisation of a Noetherian ring is again Noetherian, $\mathcal{P}_\prec$ is Noetherian, if $\mathcal{P}$ is so. One sees immediately that the units in $\mathcal{P}_\prec$ are all those fractions where not only the denominator but also the numerator is contained in $\mathcal{S}_\prec$. Given an ideal $\mathcal{I} \subseteq \mathcal{P}_\prec$, we may always assume without loss of generality that it is generated by a set $\mathcal{F} \subset \mathcal{P}$ of polynomials, as multiplication of a generator by a unit does not change the span. Hence in all computations we will exclusively work with polynomials and not with fractions.

As all elements of $\mathcal{S}_\prec$ are units in $\mathcal{P}_\prec$, we may extend the notions of leading term, monomial or exponent: if $f \in \mathcal{P}_\prec$, then we can choose a unit $u \in \mathcal{S}_\prec$ with $\mathrm{lc}_\prec u = 1$ such that $u \star f \in \mathcal{P}$ is a polynomial; now we define $\mathrm{le}_\prec f = \mathrm{le}_\prec (u \star f)$ etc. One easily verifies that this definition is independent of the choice of u.

Following Greuel and Pfister [30], one can now construct a complete theory of involutive bases over $\mathcal{P}_\prec$. Definition 9.2 of Gröbner and involutive bases can be extended without changes from the ring $\mathcal{P}$ to the localisation $\mathcal{P}_\prec$. Theorem 4.7 on the existence of Gröbner bases generalises to $\mathcal{P}_\prec$, as its proof is only based on the

leading exponents and a simple normal form argument remaining valid due to our considerations above.

Note that even if the set $\mathcal{G}$ is involutively head autoreduced, we cannot conclude in analogy to Proposition 5.13 that the involutive Mora normal form is unique, as we only consider the leading term in Algorithm 5 and hence the lower terms in h may still be involutively divisible by the leading term of some generator $g \in \mathcal{G}$. However, Theorem 5.4 remains valid.

Theorem 10.4 *Let $(\mathcal{P} = \mathbb{k}[X], \star, \prec)$ be a polynomial algebra of solvable type (for an arbitrary semigroup order $\prec$) such that $\mathbb{k}[X']$ is a subring of $\mathcal{P}$ for any subset $X' \subset X$. Furthermore, let L be a constructive Noetherian division. For a finite set $\mathcal{F} \subset \mathcal{P}$ of polynomials, let $\mathcal{I} = \langle \mathcal{F} \rangle$ be the left ideal generated by it in the localisation $\mathcal{P}_\prec$. If we apply Algorithm 3 with the involutive Mora normal form instead of the usual one to the set $\mathcal{F}$, then it terminates with an involutive basis of the ideal $\mathcal{I}$.*

Proof The termination of Algorithm 3 under the made assumptions was shown in Proposition 7.2 and Theorem 7.4. One easily verifies that their proofs are not affected by the substitution of the normal form algorithm, as they rely mainly on Theorem 5.4 and on the fact that the leading term of the normal form is not involutively divisible by the leading term of any generator. Both properties remain valid for the Mora normal form. □

Remark 10.5 Note that Theorem 10.4 guarantees the existence of *strong* involutive bases. Due to the extension to $\mathcal{P}_\prec$, Example 9.10 is no longer a valid counterexample. As the first generator in $\mathcal{F}$ is now a unit, we find that $\langle \mathcal{F} \rangle = \mathcal{P}_\prec$ and $\{1\}$ is a trivial strong Pommaret basis. ◁

Example 10.6 We continue Example 9.12. Following the approach given by Theorem 10.4, we immediately compute as Janet basis of $\langle \mathcal{F} \rangle$ (over $\mathcal{P}_\prec$) the minimal basis $\mathcal{H}_3 = \{\partial_x, \partial_y, \partial_z\}$. Obviously, it is considerably smaller than the bases obtained with Lazard's approach (over $\mathcal{P}$). This effect becomes even more profound, if we look at the sizes of the bases in the homogenised Weyl algebra: both $\tilde{\mathcal{H}}_1$ and $\tilde{\mathcal{H}}_2$ consist of 21 generators. ◁

11 Involutive Bases over Rings

Finally, we consider the case that $\mathcal{P} = \mathcal{R}[x_1, \ldots, x_n]$ is a polynomial algebra of solvable type over a (left) Noetherian ring $\mathcal{R}$. For commutative products, Gröbner bases for such algebras have been studied in [25,59] (see [1, Chapt. 4] for a more extensive textbook discussion); for PBW extensions a theory of Gröbner bases was developed in [26]. We will follow the basic ideas developed in these references and assume that linear equations are solvable in the coefficient ring $\mathcal{R}$ which means that the following two operations can be effectively performed:

(i) given elements $s, r_1, \ldots, r_k \in \mathcal{R}$, we can decide whether $s \in \langle r_1, \ldots, r_k \rangle_\mathcal{R}$ (the left ideal in $\mathcal{R}$ generated by $r_1, \ldots, r_k$);

(ii) given elements $r_1, \ldots, r_k \in \mathcal{R}$, we can construct a finite basis of the module $\mathrm{Syz}(r_1, \ldots, r_k)$ of left syzygies $s_1 r_1 + \cdots + s_k r_k = 0$.

The first operation is obviously necessary for the algorithmic reduction of polynomials with respect to a set $\mathcal{F} \subset \mathcal{P}$. The necessity of the second operation will become evident later. Compared with the commutative case, reduction is a more complicated process, in particular due to the possibility that in the commutation relations (5) for the multiplication in $\mathcal{P}$ the maps ρ_μ may be different from the identity on $\mathcal{R}$ and the coefficients $r_{\mu\nu}$ unequal one.

Let $\mathcal{G} \subset \mathcal{P}$ be a finite set. We introduce for any polynomial $f \in \mathcal{P}$ the sets $\mathcal{G}_f = \{g \in \mathcal{G} \mid \mathrm{le}_\prec g \mid \mathrm{le}_\prec f\}$ and

$$\bar{\mathcal{G}}_f = \left\{x^\mu \star g \mid g \in \mathcal{G}_f \wedge \mu = \mathrm{le}_\prec f - \mathrm{le}_\prec g \wedge \mathrm{le}_\prec (x^\mu \star g) = \mathrm{le}_\prec f\right\} \tag{25}$$

Note that the last condition in the definition of $\bar{\mathcal{G}}_f$ is redundant only, if the coefficient ring $\mathcal{R}$ is an integral domain. Otherwise it may happen that $|\bar{\mathcal{G}}_f| < |\mathcal{G}_f|$, namely if $\rho_\mu(r) r_{\mu\nu} = 0$ where $\mathrm{lm}_\prec g = r x^\nu$. The polynomial f is *head reducible* with respect to $\mathcal{G}$, if $\mathrm{lc}_\prec g \in \langle \mathrm{lc}_\prec \bar{\mathcal{G}}_f \rangle_\mathcal{R}$ (note that we use $\bar{\mathcal{G}}_f$ here so that the reduction comes only from the leading terms and is not due to some zero divisors as leading coefficients). *Involutive head reducibility* is defined analogously via sets $\mathcal{G}_{f,L}$ and $\bar{\mathcal{G}}_{f,L}$ where only involutive divisors with respect to the division L on $\mathbb{N}_0^n$ are taken into account, i. e. we set

$$\mathcal{G}_{f,L} = \{g \in \mathcal{G} \mid \mathrm{le}_\prec f \in \mathcal{C}_{L,\mathrm{le}_\prec \mathcal{G}}(\mathrm{le}_\prec g)\} \,. \tag{26}$$

Thus the set $\mathcal{G}$ is *involutively head autoreduced*, if $\mathrm{lc}_\prec g \notin \langle \mathrm{lc}_\prec (\bar{\mathcal{G}}_{g,L} \setminus \{g\}) \rangle_\mathcal{R}$ for all polynomials $g \in \mathcal{G}$. This notion is now much weaker than before; in particular, Lemma 5.12 is no longer valid.

Definition 11.1 *Let $\mathcal{I} \subseteq \mathcal{P}$ be a left ideal in the polynomial algebra $(\mathcal{P}, \star, \prec)$ of solvable type over a ring $\mathcal{R}$ in which linear equations can be solved. A finite set $\mathcal{G} \subset \mathcal{P}$ is a* Gröbner basis *of $\mathcal{I}$, if for every polynomial $f \in \mathcal{I}$ the condition $\mathrm{lc}_\prec f \in \langle \mathrm{lc}_\prec \bar{\mathcal{G}}_f \rangle_\mathcal{R}$ is satisfied. The set $\mathcal{G}$ is a* weak involutive basis *for the involutive division L, if for every polynomial $f \in \mathcal{I}$ the condition $\mathrm{lc}_\prec f \in \langle \mathrm{lc}_\prec \bar{\mathcal{G}}_{f,L} \rangle_\mathcal{R}$ is satisfied. A weak involutive basis is a* strong involutive basis, *if every set $\bar{\mathcal{G}}_{f,L}$ contains precisely one element.*

It is easy to see that the characterisation of (weak) involutive bases via the existence of involutive standard representations (Theorem 5.4) remains valid. Indeed, only the first part of the proof requires a minor change: the polynomial f_1 is now of the form $f_1 = f - \sum_{h \in \mathcal{H}_{f,L}} r_h h$ where the coefficients $r_h \in \mathcal{R}$ are chosen such that $\mathrm{le}_\prec f_1 \prec \mathrm{le}_\prec f$.

Clearly, a necessary condition for the existence of Gröbner and thus of (weak) involutive bases for arbitrary left ideals $\mathcal{I} \subset \mathcal{P}$ is that the algebra $\mathcal{P}$ is a (left) Noetherian ring. As we have seen in Section 4, this assumption becomes nontrivial, if the coefficient ring $\mathcal{R}$ is not a field. In this section, we will assume throughout that $\mathcal{P}$ is a polynomial algebra of solvable type over a left Noetherian ring $\mathcal{R}$ with centred commutation relations (cf. Definition 4.3) so that Theorem 4.4

asserts that $\mathcal{P}$ is left Noetherian, too.[8] A very useful side effect of this assumption is that the scalars appearing in the commutation relations (5) are units and thus not zero divisors which is important for some arguments.

Example 11.2 As in the previous two sections, we cannot generally expect strong involutive bases to exist. As a simple concrete example, also demonstrating the need of the second assumption on $\mathcal{R}$, we consider in $\mathbb{k}[x,y][z]$ (with the ordinary multiplication) the ideal $\mathcal{I}$ generated by the set $\mathcal{F} = \{x^2z-1, y^2z+1\}$. Obviously, both generators have the same leading exponent $[1]$; nevertheless none is reducible by the other one due to the relative primeness of the coefficients. Furthermore, the syzygy $\mathbf{S} = x^2\mathbf{e}_2 - y^2\mathbf{e}_1 \in \mathbb{k}[x,y]^2$ connecting the leading coefficients leads to the polynomial $x^2 + y^2 \in \mathcal{I}$. It is easy to see that a Gröbner and weak Janet basis of $\mathcal{I}$ is obtained by adding it to $\mathcal{F}$. A strong Janet basis does not exist, as none of these generators may be removed from the basis. $\lhd$

This example shows that simply applying the completion Algorithm 3 will generally not suffice. Obviously, with respect to the Janet division z is multiplicative for both elements of $\mathcal{F}$ so that no non-multiplicative variables exist and thus it is not possible to generate the missing generator by multiplication with a non-multiplicative variable. We must substitute in Algorithm 3 the involutive head autoreduction by a more comprehensive operation.[9]

Definition 11.3 *Let $\mathcal{F} \subset \mathcal{P}$ be a finite set and L an involutive division. We consider for each $f \in \mathcal{F}$ the syzygies $\sum_{\bar{f}\in\bar{\mathcal{F}}_{f,L}} s_{\bar{f}}\, \mathrm{lc}_\prec\, \bar{f} = 0$ connecting the leading coefficients of the elements of the set $\bar{\mathcal{F}}_{f,L}$. The set $\mathcal{F}$ is* involutively $\mathcal{R}$-saturated *for the division L, if for any such syzygy $\mathbf{S}$ the polynomial $\sum_{\bar{f}\in\bar{\mathcal{F}}_{f,L}} s_{\bar{f}}\bar{f}$ possesses an involutive standard representation with respect to $\mathcal{F}$.*

For checking involutive $\mathcal{R}$-saturation, it obviously suffices to consider a finite basis of each of the finitely many syzygy modules $\mathrm{Syz}(\mathrm{lc}_\prec \bar{\mathcal{F}}_{f,L})$ so that such a check can easily be performed effectively. An element $f \in \mathcal{F}$ is involutively head reducible by the other elements of $\mathcal{F}$, if and only if $\mathrm{Syz}(\mathrm{lc}_\prec \bar{\mathcal{F}}_{f,L})$ contains a syzygy with $s_f = 1$. For this reason it is easy to combine an involutive $\mathcal{R}$-saturation with an involutive head autoreduction leading to Algorithm 6.

[8] The case of an iterated polynomial algebra of solvable type (cf. Definition 4.1) will be considered in Part II, after we have developed a syzygy theory for involutive bases.

[9] In the classical case of commutative variables over a coefficient field, it is not difficult to show that for any finite set $\mathcal{F}$ the syzygy module $\mathrm{Syz}(\mathrm{lm}_\prec \mathcal{F})$ of the leading *monomials* can be spanned by binomial generators corresponding to the S-polynomials in the Buchberger algorithm. In Part II we will show that in any such syzygy at least one component contains a non-multiplicative variable, so that implicitly the involutive completion algorithm also runs over a generating set of this syzygy module. When we move on to coefficient rings, it is well-known that additional, more complicated syzygies coming from the coefficients must be considered. For these we can no longer assume that one component contains a non-multiplicative variable. Hence *partially* we must follow the same approach as in the generalisation of the Buchberger algorithm and this leads to the notion of $\mathcal{R}$-saturation where some syzygies not reachable via non-multiplicative variables are explicitly considered.

The `for` loop in Lines /5-13/ takes care of the involutive head autoreduction (the call $\texttt{HeadReduce}_{L,\prec}(f,\mathcal{H})$ involutively head reduces f with respect to the set $\mathcal{H}\setminus\{f\}$ but with multiplicative variables determined with respect to the full set $\mathcal{H}$—cf. Remark 5.9). The `for` loop in Lines /17-22/ checks the involutive $\mathcal{R}$-saturation. Each iteration of the outer `while` loop analyses from the remaining polynomials (collected in $\mathcal{S}$) those with the highest leading exponent. The set $\mathcal{S}$ is reset to the full basis, whenever a new element has been put into $\mathcal{H}$; this ensures that all new reduction possibilities are taken into account. In Line /15/ it does not matter which element $f\in\mathcal{S}_\nu$ we choose, as the set $\mathcal{H}'_{f,L}$ depends only on $\mathrm{le}_\prec f$ and all elements of $\mathcal{S}_\nu$ possess by construction the same leading exponent ν.

Algorithm 6 Involutive $\mathcal{R}$-saturation (and head autoreduction)

Input: finite set $\mathcal{F}\subset\mathcal{P}$, involutive division L on $\mathbb{N}_0^n$
Output: involutively $\mathcal{R}$-saturated and head autoreduced set $\mathcal{H}$ with $\langle\mathcal{H}\rangle=\langle\mathcal{F}\rangle$

/1/ $\mathcal{H}\leftarrow\mathcal{F}$; $\mathcal{S}\leftarrow\mathcal{F}$
/2/ **while** $S\neq\emptyset$ **do**
/3/ $\nu\leftarrow\max_\prec \mathrm{le}_\prec\mathcal{S}$; $\mathcal{S}_\nu\leftarrow\{f\in\mathcal{H}\mid\mathrm{le}_\prec f=\nu\}$
/4/ $\mathcal{S}\leftarrow\mathcal{S}\setminus\mathcal{S}_\nu$; $\mathcal{H}'\leftarrow\mathcal{H}$
/5/ **for all** $f\in\mathcal{S}_\nu$ **do**
/6/ $h\leftarrow\texttt{HeadReduce}_{L,\prec}(f,\mathcal{H})$
/7/ **if** $f\neq h$ **then**
/8/ $\mathcal{S}_\nu\leftarrow\mathcal{S}_\nu\setminus\{f\}$; $\mathcal{H}'\leftarrow\mathcal{H}'\setminus\{f\}$
/9/ **if** $h\neq 0$ **then**
/10/ $\mathcal{H}'\leftarrow\mathcal{H}'\cup\{h\}$
/11/ **end_if**
/12/ **end_if**
/13/ **end_for**
/14/ **if** $\mathcal{S}_\nu\neq\emptyset$ **then**
/15/ choose $f\in\mathcal{S}_\nu$ and determine the set $\bar{\mathcal{H}}'_{f,L}$
/16/ compute basis $\mathcal{B}$ of $\mathrm{Syz}(\mathrm{lc}_\prec\bar{\mathcal{H}}'_{f,L})$
/17/ **for all** $\mathbf{S}=\sum_{\bar f\in\bar{\mathcal{H}}'_{f,L}} s_{\bar f}\mathbf{e}_{\bar f}\in\mathcal{B}$ **do**
/18/ $h\leftarrow\texttt{NormalForm}_{L,\prec}(\sum_{\bar f\in\bar{\mathcal{H}}'_{f,L}} s_{\bar f}\bar f,\mathcal{H}')$
/19/ **if** $h\neq 0$ **then**
/20/ $\mathcal{H}'\leftarrow\mathcal{H}'\cup\{h\}$
/21/ **end_if**
/22/ **end_for**
/23/ **end_if**
/24/ **if** $\mathcal{H}'\neq\mathcal{H}$ **then**
/25/ $\mathcal{H}\leftarrow\mathcal{H}'$; $\mathcal{S}\leftarrow\mathcal{H}$
/26/ **end_if**
/27/ **end_while**
/28/ **return** $\mathcal{H}$

Proposition 11.4 *Under the made assumptions about the polynomial algebra $\mathcal{P}$, Algorithm 6 terminates for any finite input set $\mathcal{F}\subset\mathcal{P}$ with an involutively $\mathcal{R}$-saturated and head autoreduced set $\mathcal{H}$ such that $\langle\mathcal{H}\rangle=\langle\mathcal{F}\rangle$.*

Proof The correctness of the algorithm is trivial. The termination follows from the fact that both $\mathcal{R}$ and $\mathbb{N}_0^n$ are Noetherian. Whenever we add a new polynomial h to the set $\mathcal{H}'$, we have either that $\mathrm{le}_\prec h \notin \langle \mathrm{le}_\prec \mathcal{H}' \rangle_{\mathbb{N}_0^n}$ or $\mathrm{lc}_\prec h \notin \langle \mathrm{lc}_\prec \mathcal{H}'_{h,L} \rangle_{\mathcal{R}}$. As neither in $\mathbb{N}_0^n$ nor in $\mathcal{R}$ infinite ascending chains of ideals are possible, the algorithm must terminate after a finite number of steps. □

An obvious idea is now to substitute in the completion Algorithm 3 the involutive head autoreduction by an involutive $\mathcal{R}$-saturation. Recall that Proposition 7.2 (and Corollary 7.3) was the crucial step for proving the correctness of Algorithm 3. Our next goal is thus to show that under the made assumptions for involutively $\mathcal{R}$-saturated sets local involution implies weak involution.

Proposition 11.5 *Under the made assumptions about the polynomial algebra $\mathcal{P}$, a finite, involutively $\mathcal{R}$-saturated set $\mathcal{F} \subset \mathcal{P}$ is weakly involutive, if and only if it is locally involutive.*

Proof We first note that Proposition 7.2 remains true under the made assumptions. Its proof only requires a few trivial modifications, as all appearing coefficients (for example, when we rewrite $x^\mu \to x^{\mu - 1_j} \star x_j$) are units in the case of centred commutation relations and thus we may proceed as for a field. Hence if $\mathcal{F}$ is locally involutive, then $\mathcal{I} = \langle \mathcal{F} \rangle = \langle \mathcal{F} \rangle_{L,\prec}$ implying that any polynomial $g \in \mathcal{I}$ may be written in the form $g = \sum_{f \in \mathcal{F}} P_f \star f$ with $P_f \in \mathcal{R}[X_{L,\mathcal{F},\prec}(f)]$. Furthermore, it follows from this proof that for centred commutation relations we may assume that the polynomials P_f satisfy $\mathrm{le}_\prec (P_f \star f) = \mathrm{le}_\prec P_f + \mathrm{le}_\prec f$. We are done, if we can show that they can be chosen such that additionally $\mathrm{le}_\prec (P_f \star f) \preceq \mathrm{le}_\prec g$, i. e. such that we obtain an involutive standard representation of g.

If the representation coming out of the proof of Proposition 7.2 already satisfies this condition on the leading exponents, nothing has to be done. Otherwise we set $\nu = \max_\prec \{\mathrm{le}_\prec (P_f \star f) \mid f \in \mathcal{F}\}$ and $\mathcal{F}_\nu = \{f \in \mathcal{F} \mid \mathrm{le}_\prec (P_f \star f) = \nu\}$. As by construction $\nu \in \bigcap_{f \in \mathcal{F}_\nu} \mathcal{C}_{L,\mathrm{le}_\prec \mathcal{F}}(\mathrm{le}_\prec f)$, the properties of an involutive division imply that we can write $\mathcal{F}_\nu = \{f_1, \ldots, f_k\}$ with $\mathrm{le}_\prec f_1 \mid \mathrm{le}_\prec f_2 \mid \cdots \mid \mathrm{le}_\prec f_k$ and hence $\mathcal{F}_\nu \subseteq \mathcal{F}_{f_k,L}$. Since we have assumed that $\mathrm{le}_\prec (P_f \star f) = \mathrm{le}_\prec P_f + \mathrm{le}_\prec f$, we even find $\mathcal{F}_\nu \subseteq \bar{\mathcal{F}}_{f_k,L}$.

By construction, the equality $\sum_{f \in \mathcal{F}_\nu} \mathrm{lc}_\prec (P_f \star f) = 0$ holds. If we now set $\mathrm{lm}_\prec f = r_f x^{\nu_f}$ and $\mathrm{lm}_\prec P_f = s_f x^{\mu_f}$, then we obtain under the made assumptions: $\mathrm{lc}_\prec (P_f \star f) = s_f \rho_{\mu_f}(r_f) r_{\mu_f \nu_f} = \big[s_f \bar{\rho}_{\mu_f}(r_f) r_{\mu_f \nu_f}\big] r_f$ and hence the above equality corresponds to a syzygy of the set $\mathrm{lc}_\prec \mathcal{F}_{f_k,L}$. As the set $\mathcal{F}$ is involutively $\mathcal{R}$-saturated, there exists an involutive standard representation

$$\sum_{i=1}^{k} \big[s_{f_i} \bar{\rho}_{\mu_{f_i}}(r_{f_i}) r_{\mu_{f_i} \nu_{f_i}}\big] \bar{f}_i = \sum_{f \in \mathcal{F}} Q_f \star f \tag{27}$$

with $Q_f \in \Bbbk[X_{L,\mathcal{F},\prec}(f)]$ and $\mathrm{le}_\prec (Q_f \star f) = \mathrm{le}_\prec Q_f + \mathrm{le}_\prec f \prec \nu_{f_k}$.

Introducing now the polynomials $Q'_f = Q_f - \big[s_f \bar{\rho}_{\mu_f}(r_f) r_{\mu_f \nu_f}\big] x^{\nu_{f_k} - \nu_f}$ for $f \in \mathcal{F}_\nu$ and $Q'_f = Q_f$ otherwise, we get the syzygy $\sum_{f \in \mathcal{F}} Q'_f \star f = 0$. If we set $P'_f = P_f - c_f^{-1} x^{\nu - \nu_{f_k}} \star Q'_f$ with $c_f = \bar{\rho}_{\nu - \nu_{f_k}}\big(s_f \bar{\rho}_{\mu_f}(r_f) r_{\mu_f \nu_f}\big) \bar{\rho}_{\mu_f}(r_f) r_{\mu_f \nu_f}$,

then, by construction, $g = \sum_{f\in\mathcal{F}} P'_f \star f$ is another involutive representation of the polynomial g with $\nu' = \max_\prec\{\mathrm{le}_\prec (P'_f \star f) \mid f \in \mathcal{F}\} \prec \nu$.

Repeating this procedure for a finite number of times obviously yields an involutive standard representation of the polynomial g. As g was an arbitrary element of the ideal $\mathcal{I} = \langle\mathcal{F}\rangle$, this implies that $\mathcal{F}$ is indeed weakly involutive. □

Theorem 11.6 *Let $\mathcal{P}$ be a polynomial algebra of solvable type satisfying the made assumptions. If the subalgorithm* `InvHeadAutoReduce`$_{L,\prec}$ *is substituted in Algorithm 3 by Algorithm 6, then the completion will terminate with a weak involutive basis of $\mathcal{I} = \langle\mathcal{F}\rangle$ for any finite input set $\mathcal{F} \subset \mathcal{P}$ such that the monoid ideal $\mathrm{le}_\prec \mathcal{I}$ possesses a weak involutive basis.*

Proof The correctness of the modified algorithm follows immediately from Proposition 11.5. For the termination we may use the same argument as in the proof of Theorem 7.4, as it depends only on the leading exponents. □

12 Conclusions

We studied involutive bases for a rather general class of non-commutative polynomial algebras. Our approach was closely modelled on that of Kandry-Rody and Weispfenning [41] and subsequently Kredel [42]. We believe that the third condition in Definition 3.1 (compatibility between term order $\prec$ and non-commutative product $\star$) is more natural than the stricter axioms in [41]. It is unclear where Kandry-Rody and Weispfenning actually needed these stricter conditions, as all their main results hold in our more general situation, as shown by Kredel.

Comparing with [2,13,42,45], one must say that the there used approach is more constructive than ours. More precisely, all these authors specify the non-commutative product via commutation relations and thus have automatically a concrete algorithm for evaluating any product. As we have seen in the proof of Proposition 3.4, the same data suffices to fix our axiomatically described product, but it does not provide us with an algorithm. However, we showed that we can always map to their approach via a basis transformation.

We showed that the polynomial algebras of solvable type form a natural framework for involutive bases. This fact does not come as a surprise, if one takes into account that the main part of the involutive theory happens in the monoid $\mathbb{N}_0^n$ and the decisive third condition in Definition 3.1 of a polynomial algebra of solvable type ensures that its product $\star$ does not interfere with the leading exponents.

We extended the theory of involutive bases to semigroup orders and to polynomials over coefficient rings. It turned out that the novel concept of a *weak* involutive basis is crucial for such generalisations, as in both cases strong bases rarely exist. These weak bases are still Gröbner bases and involutive standard representations still exist (though they are no longer unique). It seems that in such computations the Janet division has a distinguished position, as by Theorem 9.11 strong Janet bases always exist. If one is only interested in using Algorithm 3 as an alternative to Buchberger's algorithm, weak bases are sufficient. However, most of

the more advanced applications of involutive bases studied in Part II will require strong involutive bases.

Concerning involutive bases over rings, we will study in Part II the special case that the coefficient ring is again a polynomial algebra of solvable type. Using the syzygy theory that will be developed there, we will be able to obtain stronger results and a "purely involutive" completion algorithm. The current approach contains hidden in the concept of $\mathcal{R}$-saturation parts of the Buchberger algorithm for the construction of Gröbner bases over rings.

Definition 2.1 represents the currently mainly used definition of an involutive division. While it appears quite natural, one problem is that in some sense too many involutive divisions exist, in particular rather weird ones with unpleasant properties (a concrete example can be found in [20, Ex. 4.8]). This effect has lead to the introduction of such technical concepts like continuity and constructivity. One could imagine that there should exist a stricter definition of involutive divisions that automatically ensures that Algorithm 2 terminates without having to resort to these technicalities.

Most of these weird divisions are globally defined and multiplicative indices are assigned only to finitely many multi indices. Such divisions are obviously of no interest, as more or less no monoid ideal possesses an involutive basis for them. One way to eliminate these divisions would be to require that for every degree $q \in \mathbb{N}_0$ the monoid ideal $(\mathbb{N}_0^n)_{\geq q} = \{\nu \in \mathbb{N}_0^n \mid q \leq |\nu|\}$ has an involutive basis. All the involutive divisions used in practice satisfy this condition, but it is still a long way from this simple condition to the termination of Algorithm 2.

We did not discuss the efficiency of the here presented algorithms. Much of the literature on involutive bases is concerned with their use as an alternative approach to the construction of Gröbner bases. In particular, experiments by Gerdt et al. [23] comparing a specialised `C/C++` program for the construction of Janet bases with the Gröbner bases package of SINGULAR [31] indicate that the involutive approach is highly competitive. This fact is quite remarkable, if one takes into account that SINGULAR is based on the results of many years of intensive research on Gröbner bases by many groups, whereas involutive bases are still very young and only a few researchers have actively worked on them. The results in Part II will offer some heuristic explanations for this observation.

Finally, we mention that most of the algorithms discussed in this article have been implemented (for general polynomial algebras of solvable type) by M. Hausdorf [33, 34] in the computer algebra system *MuPAD*.[10] The implementation does not use the simple completion Algorithm 3 but a more optimised version yielding minimal bases developed by Gerdt and Blinkov [21]. It also includes the modified algorithm for determining strong Janet bases in local rings.

A Term Orders

We use in this article non-standard definitions of some basic term orders. More precisely, we revert the order of the variables: our definitions become the standard

[10] For more information see `www.mupad.de`.

ones, if one transforms $(x_1, \ldots, x_n) \to (x_n, \ldots, x_1)$. The reason for this reversal is that this way the definitions fit better to the conventions in the theory of involutive systems of differential equations. Furthermore, they appear more natural in some applications like the determination of the depth in Part II.

A *term order* $\prec$ is for us a total order on the set $\mathbb{T}$ of all terms x^μ satisfying the following two conditions: (i) $1 \preceq t$ for all terms $t \in \mathbb{T}$ and (ii) $s \preceq t$ implies $r \cdot s \preceq r \cdot t$ for all terms $r, s, t \in \mathbb{T}$. If a term order fulfils in addition the condition that $s \prec t$ whenever $\deg s < \deg t$, it is called *degree compatible*. As $\mathbb{T}$ and $\mathbb{N}_0^n$ are isomorphic as monoids, we may also speak of term orders on $\mathbb{N}_0^n$. In fact, most term orders are defined via multi indices.

A more appropriate name for term orders might be *monoid orders*, as the two conditions above say nothing but that these orders respect the monoid structure of $\mathbb{T}$. A more general class of (total) orders are *semigroup orders* where we skip the first condition, i. e. we only take the semigroup structure of $\mathbb{T}$ into account. It is a well-known property of such orders that they are no longer well-orders. This implies in particular the existence of infinite descending sequences so that normal form algorithms do not necessarily terminate.

The *lexicographic* order is defined by $x^\mu \prec_{\text{lex}} x^\nu$, if the last non-vanishing entry of $\mu - \nu$ is negative. Thus $x_2^2 x_3 \prec_{\text{lex}} x_1 x_3^2$. With respect to the *reverse lexicographic* order $x^\mu \prec_{\text{revlex}} x^\nu$, if the first non-vanishing entry of $\mu - \nu$ is positive. Now we have $x_1 x_3^2 \prec_{\text{revlex}} x_2^2 x_3$. However, $\prec_{\text{revlex}}$ is only a semigroup order, as it violates the first condition: $x_1 \prec_{\text{revlex}} 1$. Degree compatible versions of these orders exist, too. $x^\mu \prec_{\text{deglex}} x^\nu$, if $|\mu| < |\nu|$ or if $|\mu| = |\nu|$ and $x^\mu \prec_{\text{lex}} x^\nu$. Similarly, $x^\mu \prec_{\text{degrevlex}} x^\nu$, if $|\mu| < |\nu|$ or if $|\mu| = |\nu|$ and $x^\mu \prec_{\text{revlex}} x^\nu$. Obviously $\prec_{\text{degrevlex}}$ is a term order. It possesses the following useful characterisation which is easy to prove.

Lemma A.1 *Let $\prec$ be a degree compatible term order such that the condition $\operatorname{lt}_\prec f \in \langle x_1, \ldots, x_k \rangle$ is equivalent to $f \in \langle x_1, \ldots, x_k \rangle$ for every homogeneous polynomial $f \in \mathcal{P}$. Then $\prec$ is the degree reverse lexicographic order $\prec_{\text{degrevlex}}$.*

We say that a term order *respects classes*, if for multi indices μ, ν of the same length $\operatorname{cls}\mu < \operatorname{cls}\nu$ implies $x^\mu \prec x^\nu$. It is now easy to see that by Lemma A.1 on terms of the same degree any class respecting term order on $\mathbb{T}$ coincides with the degree reverse lexicographic order. If we consider free polynomial modules, class respecting orders have the same relation to TOP lifts [1] of $\prec_{\text{degrevlex}}$.

Acknowledgements The author would like to thank V.P. Gerdt for a number of interesting discussions on involutive bases. M. Hausdorf and R. Steinwandt participated in an informal seminar at Karlsruhe University where most ideas of this article were presented and gave many valuable comments. The constructive remarks of the anonymous referees were also very helpful. This work received partial financial support by Deutsche Forschungsgemeinschaft, INTAS grant 99-1222 and NEST-Adventure contract 5006 (*GIFT*).

References

1. W.W. Adams and P. Loustaunau. *An Introduction to Gröbner Bases*. Graduate Studies in Mathematics 3. American Mathematical Society, Providence, 1994.
2. J. Apel. *Gröbnerbasen in Nichtkommutativen Algebren und ihre Anwendung*. PhD thesis, Universität Leipzig, 1988.
3. J. Apel. The computation of Gröbner bases using an alternative algorithm. In M. Bronstein, J. Grabmeier, and V. Weispfenning, editors, *Symbolic Rewriting Techniques*, Progress in Computer Science and Applied Logic 15, pages 35–45. Birkhäuser, Basel, 1998.
4. J. Apel. Theory of involutive divisions and an application to Hilbert function computations. *J. Symb. Comp.*, 25:683–704, 1998.
5. J. Apel and R. Hemmecke. Detecting unnecessary reductions in an involutive basis computation. *J. Symb. Comp.*, 40:1131–1149, 2005.
6. Th. Becker and V. Weispfenning. *Gröbner Bases*. Graduate Texts in Mathematics 141. Springer-Verlag, New York, 1993.
7. A.D. Bell and K.R. Goodearl. Uniform rank over differential operator rings and Poincaré-Birkhoff-Witt extensions. *Pacific J. Math.*, 131:13–37, 1988.
8. R. Berger. The quantum Poincaré-Birkhoff-Witt theorem. *Comm. Math. Phys.*, 143:215–234, 1992.
9. J.E. Björk. *Rings of Differential Operators*. North-Holland Mathematical Library 21. North-Holland, Amsterdam, 1979.
10. Yu.A. Blinkov. Method of separative monomials for involutive divisions. *Prog. Comp. Software*, 27:139–141, 2001.
11. J.L. Bueso, J. Gómez-Torrecillas, and F.J. Lobillo. Homological computations in PBW modules. *Alg. Represent. Theo.*, 4:201–218, 2001.
12. J.L. Bueso, J. Gómez-Torrecillas, F.J. Lobillo, and F.J. Castro-Jiménez. An introduction to effective calculus in quantum groups. In S. Caenepeel and A. Verschoren, editors, *Rings, Hopf Algebras, and Brauer Groups*, Lecture Notes in Pure and Applied Mathematics 197, pages 55–83. Marcel Dekker, New York, 1998.
13. J.L. Bueso, J. Gómez-Torrecillas, and A. Verschoren. *Algorithmic Methods in Non-Commutative Algebra*. Mathematical Modelling: Theory and Applications 17. Kluwer, Dordrecht, 2003.
14. Y.F. Chen and X.S. Gao. Involutive directions and new involutive divisions. *Comp. Math. Appl.*, 41:945–956, 2001.
15. P.M. Cohn. *Algebra II*. John Wiley, London, 1977.
16. D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics 185. Springer-Verlag, New York, 1998.
17. V.G. Drinfeld. Hopf algebras and the quantum Yang-Baxter equations. *Sov. Math. Dokl.*, 32:254–258, 1985.
18. V.P. Gerdt. Completion of linear differential systems to involution. In V.G. Ghanza, E.W. Mayr, and E.V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing — CASC '99*, pages 115–137. Springer-Verlag, Berlin, 1999.
19. V.P. Gerdt. On an algorithmic optimization in computation of involutive bases. *Prog. Comp. Softw.*, 28:62–65, 2002.
20. V.P. Gerdt and Yu.A. Blinkov. Involutive bases of polynomial ideals. *Math. Comp. Simul.*, 45:519–542, 1998.
21. V.P. Gerdt and Yu.A. Blinkov. Minimal involutive bases. *Math. Comp. Simul.*, 45:543–560, 1998.
22. V.P. Gerdt, Yu.A. Blinkov, and D.A. Yanovich. Construction of Janet bases I: Monomial bases. In Ghanza et al. [24], pages 233–247.

23. V.P. Gerdt, Yu.A. Blinkov, and D.A. Yanovich. Construction of Janet bases II: Polynomial bases. In Ghanza et al. [24], pages 249–263.
24. V.G. Ghanza, E.W. Mayr, and E.V. Vorozhtsov, editors. *Computer Algebra in Scientific Computing — CASC 2001*. Springer-Verlag, Berlin, 2001.
25. P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symb. Comp.*, 6:149–167, 1988.
26. M. Giesbrecht, G.J. Reid, and Y. Zhang. Non-commutative Gröbner bases in Poincaré-Birkhoff-Witt extensions. In V.G. Ghanza, E.W. Mayr, and E.V. Vorozhtsov, editors, *Computer Algebra in Scientific Computing — CASC 2002*. Fakultät für Informatik, Technische Universität München, 2002.
27. H.-G. Gräbe. The tangent cone algorithm and homogenization. *J. Pure Appl. Alg.*, 97:303–312, 1994.
28. H.-G. Gräbe. Algorithms in local algebra. *J. Symb. Comp.*, 19:545–557, 1995.
29. G.-M. Greuel and G. Pfister. Advances and improvements in the theory of standard bases and syzygies. *Arch. Math.*, 66:163–176, 1996.
30. G.-M. Greuel and G. Pfister. *A* SINGULAR *Introduction to Commutative Algebra*. Springer-Verlag, Berlin, 2002.
31. G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 2.0 — A computer algebra system for polynomial computations. Technical report, Centre for Computer Algebra, University of Kaiserslautern, 2001. `www.singular.uni-kl.de`.
32. M. Hausdorf and W.M. Seiler. An efficient algebraic algorithm for the geometric completion to involution. *Appl. Alg. Eng. Comm. Comp.*, 13:163–207, 2002.
33. M. Hausdorf and W.M. Seiler. Involutive bases in *MuPAD* I: Involutive divisions. *mathPAD*, 11:51–56, 2002.
34. M. Hausdorf and W.M. Seiler. Involutive bases in *MuPAD* II: Polynomial algebras of solvable type. *mathPAD*, to appear.
35. M. Hausdorf, W.M. Seiler, and R. Steinwandt. Involutive bases in the Weyl algebra. *J. Symb. Comp.*, 34:181–198, 2002.
36. W. Hereman. Review of symbolic software for the computation of Lie symmetries of differential equations. *Euromath Bull.*, 2:45–82, 1994.
37. M. Janet. Sur les systèmes d'équations aux dérivées partielles. *J. Math. Pure Appl.*, 3:65–151, 1920.
38. M. Janet. Les modules de formes algébriques et la théorie générale des systèmes différentiels. *Ann. École Norm. Sup.*, 41:27–65, 1924.
39. M. Janet. *Leçons sur les Systèmes d'Équations aux Dérivées Partielles*. Cahiers Scientifiques, Fascicule IV. Gauthier-Villars, Paris, 1929.
40. M. Jimbo. A q-difference analogue of $U(\mathfrak{g})$ and the Yang-Baxter equations. *Lett. Math. Phys.*, 10:63–69, 1985.
41. A. Kandry-Rody and V. Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. *J. Symb. Comp.*, 9:1–26, 1990.
42. H. Kredel. *Solvable Polynomial Rings*. Verlag Shaker, Aachen, 1993.
43. D. Lazard. Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In J.A. van Hulzen, editor, *Proc. EUROCAL '83*, Lecture Notes in Computer Science 162, pages 146–156. Springer-Verlag, Berlin, 1983.
44. V. Levandovskyy. On Gröbner bases for non-commutative G-algebras. In J. Calmet, M. Hausdorf, and W.M. Seiler, editors, *Proc. Under- and Overdetermined Systems of Algebraic or Differential Equations*, pages 99–118. Fakultät für Informatik, Universität Karlsruhe, 2002.
45. V. Levandovskyy. *Non-commutative Computer Algebra for Polynomial Algebras: Gröbner Bases, Applications and Implementation*. PhD thesis, Fachbereich Mathematik, Universität Kaiserslautern, 2005.

46. J.C. McConnell and J.C. Robson. *Non-commutative Noetherian Rings*. Wiley, 1987.
47. C. Méray and C. Riquier. Sur la convergence des développements des intégrales ordinaires d'un système d'équations différentielles partielles. *Ann. Sci. Ec. Norm. Sup.*, 7:23–88, 1890.
48. E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra*. Graduate Texts in Mathematics 227. Springer-Verlag, New York, 2005.
49. T. Mora. An algorithm to compute the equations of tangent cones. In J. Calmet, editor, *Proc. EUROCAM '82*, Lecture Notes in Computer Science 144, pages 158–165. Springer-Verlag, Berlin, 1982.
50. E. Noether and W. Schmeidler. Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzausdrücken. *Math. Zeit.*, 8:1–35, 1920.
51. O. Ore. Linear equations in non-commutative fields. *Ann. Math.*, 32:463–477, 1931.
52. O. Ore. Theory of non-commutative polynomials. *Ann. Math.*, 34:480–508, 1933.
53. C. Riquier. *Les Systèmes d'Équations aux Derivées Partielles*. Gauthier-Villars, Paris, 1910.
54. M. Saito, B. Sturmfels, and N. Takayama. *Gröbner Deformations of Hypergeometric Differential Equations*. Algorithms and Computation in Mathematics 6. Springer-Verlag, Berlin, 2000.
55. W.M. Seiler. *Involution — The Formal Theory of Differential Equations and its Applications in Computer Algebra*. Algorithms and Computation in Mathematics 24. Springer-Verlag, Berlin, 2009 (to appear).
56. B. Sturmfels and N. White. Computing combinatorial decompositions of rings. *Combinatorica*, 11:275–293, 1991.
57. J.M. Thomas. *Differential Systems*. Colloquium Publications XXI. American Mathematical Society, New York, 1937.
58. A. Tresse. Sur les invariants différentiels des groupes continus de transformations. *Acta Math.*, 18:1–88, 1894.
59. W. Trinks. Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen. *J. Num. Th.*, 10:475–488, 1978.
60. V.S. Varadarajan. *Lie Groups, Lie Algebras, and Their Representations*. Graduate Texts in Mathematics 102. Springer-Verlag, New York, 1984.
61. W.T. Wu. On the construction of Gröbner basis of a polynomial ideal based on Riquier-Janet theory. *Syst. Sci. Math. Sci.*, 4:194–207, 1991.
62. A.Yu. Zharkov and Yu.A. Blinkov. Involution approach to solving systems of algebraic equations. In G. Jacob, N.E. Oussous, and S. Steinberg, editors, *Proc. Int. IMACS Symp. Symbolic Computation*, pages 11–17. Lille, 1993.