Under consideration for publication in Math. Struct. in Comp. Science

Constructing Gröbner Bases for Noetherian Rings

HERVÉ PERDRY† and PETER SCHUSTER‡

† *Université Paris-Sud UMR-S 669 & INSERM U 669, Villejuif F–94817; perdry@vjf.inserm.fr*
‡ *Pure Mathematics, University of Leeds, Leeds LS2 9JT, U.K.; pschust@maths.leeds.ac.uk*

Received 13 April 2011; Revised 1 March 2013

We prove constructively that every finitely generated polynomial ideal has a Gröbner basis provided that the ring of coefficients is Noetherian in the sense of Richman and Seidenberg. That is, we give a constructive termination proof for a variant of the otherwise well-known algorithm to compute the Gröbner basis. In combination with a purely order-theoretic result we have proved in a separate paper, this yields a unified constructive proof of the Hilbert basis theorem for all Noether classes: if a ring belongs to a Noether class, then so does the polynomial ring. Our proof can be seen as a constructive rereading of one of the classical proofs, in the spirit of the partial realisation of Hilbert's programme in algebra put forward by Coquand and Lombardi. The rings under consideration need not be commutative, but are understood to be coherent, and strongly discrete: that is, they admit a membership test for every finitely generated ideal. As a complement we provide a prime decomposition for commutative rings possessing the finite-depth property.

Introduction

In this paper we complete, in constructive algebra à la Kronecker and Bishop (Edwards 2005; Lombardi and Quitté 2011; Mines *et al.* 1988),† the unified proof of several variants of the Hilbert basis theorem whose order-theoretic grounds we have set before (Perdry and Schuster 2011). The wording of this theorem is readily put: if a—not necessarily commutative—ring R is Noetherian, then so is the polynomial ring $R[X]$.

In any constructive context, however, the concept in question requires particular attention: "What is Noetherian?" (Seidenberg 1974). The definition going back to Hilbert is of little use, as recalled in (Mines *et al.* 1988, p. 193): "Standard classical proofs of the Hilbert basis theorem are constructive, if by *Noetherian* we mean that every ideal is finitely generated, but only trivial rings are Noetherian in this sense from a constructive point of view." One of these classical proofs is the one given e.g. for Theorem 69 of (Ka-

† In particular we will make use of the principle of dependent choices.

plansky 1974). A similar problem as for Hilbert's definition occurs with the condition due to Noether that every ascending chain of ideals is eventually constant.[‡]

Several constructively meaningful notions of a Noetherian ring have nonetheless allowed for a constructively provable variant of the Hilbert basis theorem (Coquand and Persson 1999; Jacobsson and Löfwall 1991; Mines *et al.* 1988; Perdry 2004; Perdry 2008; Richman 1974; Richman 2003; Schuster and Zappe 2006; Seidenberg 1974; Tennenbaum 1973). In the present paper—as in its forerunner (Perdry and Schuster 2011)—we need to add two preconditions. First, we suppose that the poset $\mathfrak{I}_R$ of the finitely generated ideals of the ring R be decidable or, equivalently, that each of these ideals have a membership test. Secondly, we assume that the ring R be coherent: that is, every finitely generated ideal have a basis of syzygies; which is automatic for the Hilbertian concept that every ideal be finitely generated.[§]

Most of those variants of "Noetherian" rely on properties of the poset $\mathfrak{I}_R$, just as Noether's ascending chain condition does. In (Perdry and Schuster 2011) we thus have abstracted from the ring context, and studied the classes of posets that correspond to these properties. Each of these classes satisfies four characteristic conditions, which define what in (Perdry and Schuster 2011) we have called a Noether class of posets. We say that a ring R is $\mathcal{C}$-Noetherian whenever $\mathfrak{I}_R$ belongs to the given Noether class $\mathcal{C}$, for which Hilbert's basis theorem reads as "if R is $\mathcal{C}$-Noetherian, then $R[X]$ is $\mathcal{C}$-Noetherian".

The perhaps best known constructively meaningful property of $\mathfrak{I}_R$ is the chain condition used by Richman and Seidenberg (Richman 1974; Seidenberg 1974): every descending sequence $a_0 \geqslant a_1 \geqslant \dots$ halts, i.e. there is n with $a_n = a_{n+1}$. The posets which possess this property form the prime example of a Noether class, the Richman-Seidenberg class $\mathcal{RS}$, which also is the largest Noether class (Perdry and Schuster 2011). (We follow (Perdry 2004) and reverse the natural inclusion order on $\mathfrak{I}_R$; whence we consider descending rather than ascending chains of finitely generated ideals.) Richman and Seidenberg's condition is both meaningful and useful: plenty of rings are $\mathcal{RS}$-Noetherian (Mines *et al.* 1988); and that $K[X_1, \dots, X_n]$ is $\mathcal{RS}$-Noetherian for any (discrete) field K suffices (Perdry 2004) for a constructive termination proof of Buchberger's algorithm.

In the vein of a partial realisation of Hilbert's programme in algebra (Coquand and Lombardi 2006) we reread constructively one of the classical proofs of the Hilbert basis theorem: e.g., the first proof of Theorem 1 in (Zariski and Samuel 1958, IV). In this type of proof one first notices that the ascending chain condition propagates from the poset of ideals to the poset of ascending chains of ideals. Given a chain of polynomial ideals $I_0 \subseteq I_1 \subseteq \cdots$ one next considers for each k the ascending chain of ideals $\ell_0(I_k) \subseteq \ell_1(I_k) \subseteq \cdots$ where each $\ell_n(I_k)$ consists of the leading coefficients of the $f \in I_k$ with $\deg(f) \leqslant n$. The double-indexed sequence of the $\ell_n(I_k)$ can then be seen as an ascending chain of ascending chains of ideals, which—as noticed before—is eventually constant. To conclude it suffices to verify that if $I \subseteq J$ and $\ell_n(I) = \ell_n(J)$ for all n, then $I = J$.

[‡] Both customary notions of a Noetherian ring are in fact too strong in a recursive interpretation already for $R = \mathbb{F}_2$, the two-element field, for which either of them would solve the halting problem.

[§] Strong discreteness, or coherence, can be relaxed for some of the variants listed above, see e.g. (Coquand and Persson 1999; Mines *et al.* 1988; Perdry 2008; Richman 2003; Tennenbaum 1973).

By thus passing from infinite sequences of ideals to infinite sequences of such sequences, the complexity of the objects under consideration is increased during the proof. A constructive rereading therefore seems hardly possible; and in fact the constructive proofs listed earlier on all follow different lines. Our key observation however (Perdry and Schuster 2011, Theorem 3.1) was that the method of this classical proof works with finite chains as well: if a poset E is in a Noether class $\mathcal{C}$, then the poset $E^\star$ of the eventually constant descending chains in E is also in $\mathcal{C}$. We further need to invoke one of the conditions we have imposed on the Noether classes (Perdry and Schuster 2011): if a poset G is in a Noether class $\mathcal{C}$, then every poset F is in $\mathcal{C}$ that can be embedded into G along a strictly increasing mapping. To apply this to the posets $E = \mathfrak{I}_R$, $F = \mathfrak{I}_R^\star$, and $G = \mathfrak{I}_{R[X]}$, and thus to complete the desired unified constructive proof of the Hilbert basis theorem (Theorem 3.1 below), it suffices to give a strictly increasing mapping from $\mathfrak{I}_{R[X]}$ to $\mathfrak{I}_R^\star$. The latter is done—mimicking the classical proof recalled above—by assigning (Lemma 3.1) every $I \in \mathfrak{I}_{R[X]}$ to the sequence $\ell_0(I) \geqslant \ell_1(I) \geqslant \cdots$ in $\mathfrak{I}_R$.

From the constructive angle, an important ingredient is to see that this mapping is well-defined, which could well be done with some material already present in the literature (Mines *et al.* 1988); see Appendix 5.1. However, we prefer to do it with a variant of the notion of a Gröbner basis, which approach we find more natural. More precisely we prove constructively (Theorem 2.1) that if the ring R is $\mathcal{RS}$-Noetherian, then R is a Gröbner ring by which we mean that every finitely generated ideal of $R[X]$ has a Gröbner basis in the sense of Definition 2.4 below. It is noteworthy that to prove Theorem 2.1 we apply (Perdry and Schuster 2011, Theorem 3.1) once more, this time to the class $\mathcal{RS}$.

With Theorem 2.1 we thus give a constructive termination proof for a variant of the otherwise well-known algorithm to compute the Gröbner basis. Our approach is related to the customary theory of Gröbner bases over a ring, which in turn resembles the one of Gröbner bases over a field (Buchberger 1965); see e.g. (Adams and Loustaunau 1994).[¶] In particular, Lemmas 2.6 and 2.7, and Proposition 2.6 below are related to the Buchberger criterion by which one can tell whether any given finite set of generators is a Gröbner basis. The main difference is that we prove constructively that the aforementioned algorithm terminates in a finite number of steps. Also, we focus on the case of polynomials in a single variable; the case of polynomials in several variables with lexicographic monomial ordering can be obtained by iteration, and is left to the interested reader.

On the road to Theorem 2.1 we prove that if R is a Gröbner ring, and I a finitely generated ideal of $R[X]$, then $\ell_k(I)$ is finitely generated for every $k \in \mathbb{N}$ (Proposition 2.5); in particular (Corollary 2.2) the ideal $\mathrm{LC}(I)$ of R that consists of the leading coefficients of the elements of I is finitely generated as well. In view of this our notion of a Gröbner ring is to be contrasted with the one coined by Yengui (Yengui 2006), for whom a Gröbner ring R is such that, for every $n \geqslant 1$ and every finitely generated ideal I of $R[X_1, \ldots, X_n]$ with a fixed monomial order, the ideal $\mathrm{LT}(I)$ of $R[X]$ that is generated by the leading terms of the elements of I is finitely generated. See also (Lombardi *et al.* 2012).

Another example of a Noether class of posets is the one defined by the finite-depth

[¶] In the case of polynomials over a ring yet another approach—the so-called dynamical Gröbner bases—has proved successful (Yengui 2006; Hajd Kacem and Yengui 2010).

property (Perdry and Schuster 2011): every finitely branching tree labelled by the poset under consideration has finite depth. This property defines the finite-depth class of posets $\mathcal{FD}$, which coincides with $\mathcal{RS}$ precisely when (Perdry and Schuster 2011) a fairly general form of Brouwer's fan theorem holds, the classical contrapositive of which is König's lemma. As a complement we provide in Appendix 5.3 a prime decomposition for commutative $\mathcal{FD}$-Noetherian rings, and thus generalise a result from (Perdry 2004).

1. Preliminaries

1.1. *Posets and chains*

We first recollect and enrich some material from (Perdry and Schuster 2011), which in parts goes back to (Mines *et al.* 1988). Let every partially ordered set $(E, \leqslant)$ have a *decidable order* and thus be a *discrete set*: that is, $x \leqslant y$ and thus $x = y$ are decidable relations between the elements of E. By $x < y$ we denote the conjunction of $x \leqslant y$ and $x \neq y$, where the latter stands for the negation of $x = y$.

Let E and F be posets. A mapping $\varphi : E \to F$ is *increasing* (respectively, *strictly increasing*) if

$$a \leqslant b \implies \varphi(a) \leqslant \varphi(b) \quad (\text{respectively, } a < b \implies \varphi(a) < \varphi(b))$$

for all $a, b \in E$. Any $\varphi : E \to F$ is strictly increasing precisely when it is increasing and

$$a \leqslant b \wedge \varphi(a) = \varphi(b) \implies a = b$$

for all $a, b \in E$.

Let $(E_i, \leqslant_i)_{i \in I}$ be a family of posets indexed by a poset $(I, \leqslant)$. By $\sum_{i \in I} E_i$ we denote the disjoint union $\{(i, x) \,:\, i \in I,\ x \in E_i\}$ ordered by

$$(i, x) \leqslant (j, y) \iff i < j \vee (i = j \wedge x \leqslant_i y)\,.$$

Since the partial orders on I and on the E_i with $i \in I$ are decidable, so is $\leqslant$ on $\sum_{i \in I} E_i$. If $E_i = E$ for all $i \in I$, then $\sum_{i \in I} E_i$ is nothing but the lexicographic product $I \cdot E$.

To replace the eventually constant descending sequences with a concept of finite character, we consider the set of descending finite sequences in a poset E: that is,

$$E^\star = \bigcup_{n \in \mathbb{N}} \{(a_0, \ldots, a_n) \in E^{n+1} \,:\, a_0 \geqslant a_1 \geqslant \cdots \geqslant a_n\}\,.$$

Every $(a_0, \ldots, a_n) \in E^\star$ can be extended, by setting $a_m = a_n$ for $m > n$, to a descending infinite sequence, with which we often identify it. With this convention we define

$$a \leqslant b \iff \forall m \in \mathbb{N}\,(a_m \leqslant b_m)$$

for any two $a, b \in E^\star$. Note that $\leqslant$ on $E^\star$ is decidable for so is $\leqslant$ on E.

The *Richman-Seidenberg class* $\mathcal{RS}$ consists of the posets E for which

$$\text{if } a_0 \geqslant a_1 \geqslant \cdots \text{ in } E, \text{ then there is } n \in \mathbb{N} \text{ such that } a_n = a_{n+1}.$$

A class $\mathcal{C}$ of posets is a *Noether class* if it satisfies the following four conditions:

1 $\mathcal{C} \subseteq \mathcal{RS}$.

2 $\mathbb{N} \in \mathcal{C}$.
3 If there is a strictly increasing mapping from E to F, then $E \in \mathcal{C}$ whenever $F \in \mathcal{C}$.
4 Let I be a poset in $\mathcal{C}$. If $(E_i)_{i\in I}$ is a family of posets in $\mathcal{C}$, then $\sum_{i\in I} E_i$ is in $\mathcal{C}$.

The class $\mathcal{RS}$ is a Noether class; by condition 1 above it is the largest one. More examples of Noether classes are given in (Perdry and Schuster 2011). The following (Perdry and Schuster 2011, Theorem 3.1) will be crucial for this paper.

Theorem 1.1. Let $\mathcal{C}$ be a Noether class. If a poset E is in $\mathcal{C}$, then so is $E^\star$.

1.2. *Rings and ideals*

In the whole paper, R denotes a—not necessarily commutative—ring with unit. Following (Perdry 2004) we write $\mathfrak{I}_R$ for the poset of finitely generated left ideals of R ordered by reverse inclusion:

$$I \leqslant J \iff I \supseteq J\,.$$

By $\langle S\rangle$ we denote the left ideal of R that is generated by a finite subset S of R. We sometimes identify a finite family $a = (a_1, \ldots, a_n)$ of elements of R with the set of its elements, and write $\langle a\rangle$ or $\langle a_1, \ldots, a_n\rangle$ for the left ideal generated by them.

Recall that a *syzygy* of a finite family $a = (a_1, \ldots, a_n)$ of elements of R is an element of $\ker(\eta_a)$ where η_a is defined by

$$\begin{array}{rcl} \eta_a : R^n & \to & \langle a_1, \ldots, a_n\rangle \\ (\alpha_1, \ldots, \alpha_n) & \mapsto & \alpha_1 a_1 + \cdots + \alpha_n a_n\,. \end{array}$$

A *basis of syzygies* of a is a finite set of non-zero elements of R^n which generates $\ker(\eta_a)$ as a left R-module.

It has been indicated (Lombardi and Quitté 2011, 4.1) that if two finite families of elements of R generate the same left ideal, then one of these families has a basis of syzygies if and only if so does the other. For completeness's sake we give a detailed proof of this in Section 2.6 below (Lemma 2.9). In particular, it is licit to say that a finitely generated left ideal I *has a basis of syzygies* if so does any finite set of generators: that is, $\ker(\eta_a)$ is finitely generated whenever $I = \langle a\rangle$.

Recall that a ring R is *coherent* if every finitely generated left ideal is *finitely presented*: that is, it has a basis of syzygies. Also, a ring R is *strongly discrete* if every finitely generated left ideal I is *detachable* from R: that is, for each $r \in R$ it is decidable whether $r \in I$. A strongly discrete ring is *discrete*: that is, for each $r \in R$ it is decidable whether $r = 0$. If a ring R is discrete, then the degree $\deg(f)$ of any $f \in R[X]$ with $f \neq 0$ is defined as usual; we further set $\deg(0) = -\infty$.

Now let $\mathcal{C}$ be a Noether class of posets.

Definition 1.1. We say that a coherent and strongly discrete ring R is $\mathcal{C}$*-Noetherian* if $\mathfrak{I}_R$ belongs to $\mathcal{C}$.

By the definition of a Noether class, if R is $\mathcal{C}$-Noetherian, then R is $\mathcal{RS}$-Noetherian: that is, if $I_0 \subseteq I_1 \subseteq \cdots$ are finitely generated ideals of R, then there is $n \in \mathbb{N}$ such that $I_n = I_{n+1}$.

2. Gröbner Bases for Noetherian Rings

We assume throughout that the ring R under consideration is strongly discrete and coherent. Also, all ideals of R are thought to be left ideals.

2.1. *Leading coefficients*

Let $\mathrm{LT}(h)$ and $\mathrm{LC}(h)$ denote the *leading term* and the *leading coefficient*, respectively, of $h \in R[X]$ with $h \neq 0$. In other words, if

$$h = c_n X^n + \cdots + c_1 X + c_0$$

with $c_n \neq 0$, then $\mathrm{LT}(h) = c_n X^n$ and $\mathrm{LC}(h) = c_n$.

In the following let $S = \{f_1, \ldots, f_s\}$ be a finite subset of $R[X]$. For any such S we set

$$\mathrm{LC}(S) = \{\mathrm{LC}(f) : f \in S, f \neq 0\},$$

which equally is a finite subset of R. We also define

$$S_k = \{X^n f : n + \deg(f) = k,\ n \in \mathbb{N},\ f \in S, f \neq 0\}$$

for $k \in \mathbb{N}$. Note that S_k is a finite subset of $\langle S \rangle$. If $h \in S_k$, then $\deg(h) = k$ and $k \geqslant \min_{f \in S \setminus \{0\}} \deg(f)$; whence $S_k = \varnothing$ whenever $k < \min_{f \in S \setminus \{0\}} \deg(f)$. Moreover,

$$\mathrm{LC}(S_1) \subseteq \mathrm{LC}(S_2) \subseteq \cdots \subseteq \mathrm{LC}(S_d) = \mathrm{LC}(S_{d+1}) = \ldots = \mathrm{LC}(S) \tag{1}$$

where $d = \max_{f \in S \setminus \{0\}} \deg(f)$, for which if $k \geqslant d$, then

$$S_k = X^{k-d} S_d = \{X^{k-d} h : h \in S_d\}.$$

Remark 2.1. If $S_k = \{h_1, \ldots, h_\ell\}$, and $\beta = (\beta_1, \ldots, \beta_\ell) \in R^\ell$, then β is a syzygy of $\langle \mathrm{LC}(S_k) \rangle$ precisely when $\sum_j \beta_j h_j$ has degree $< k$.

2.2. *Reductions of polynomials*

In this subsection, $S = \{f_1, \ldots, f_s\}$ is a finite subset of $R[X]$.

Definition 2.1. Let $g \in R[X]$. We say that

— g is *reducible* by S if $g \neq 0$ and there are $\alpha_1, \ldots, \alpha_s \in R$ and $n_1, \ldots, n_s \in \mathbb{N}$ with

$$\mathrm{LT}(g) = \sum_{i=1}^{s} \alpha_i X^{n_i} \mathrm{LT}(f_i), \tag{2}$$

$$\alpha_i \neq 0 \Rightarrow \alpha_i \mathrm{LC}(f_i) \neq 0 \ \&\ n_i + \deg(f_i) = \deg(g); \tag{3}$$

— g is *irreducible* by S if g is not reducible by S: that is, either $g = 0$ or else there are no $\alpha_1, \ldots, \alpha_s \in R$ and $n_1, \ldots, n_s \in \mathbb{N}$ satisfying both (2) and (3).

The following lemma is readily verified.

Lemma 2.1. The following are equivalent for each $g \in R[X]$ with $g \neq 0$:

1 g is reducible by S.

2 There are $\alpha_1, \ldots, \alpha_s \in R$ with

$$\mathrm{LC}(g) = \sum_{i=1}^{s} \alpha_i \,\mathrm{LC}(f_i)\,, \tag{4}$$

$$\alpha_i \neq 0 \Rightarrow \alpha_i \,\mathrm{LC}(f_i) \neq 0 \;\&\; \deg(f_i) \leqslant \deg(g)\,. \tag{5}$$

3 $\mathrm{LC}(g)$ belongs to the left ideal $\langle \mathrm{LC}(S_k) \rangle$ with $k = \deg(g)$.

Corollary 2.1. For each $g \in R[X]$ it is decidable whether g is reducible by S.

Proof. Decide first whether $g = 0$. In case $g \neq 0$, decide next whether the third equivalent of Lemma 2.1 holds; this can be done because R is strongly discrete. □

Proposition 2.1. For each $g \in R[X]$ there is $\widetilde{g} \in R[X]$ with

$$g = \sum_{i=1}^{s} \alpha_i X^{n_i} f_i + \widetilde{g}$$

for suitable $\alpha_1, \ldots, \alpha_s \in R$ and $n_1, \ldots, n_s \in \mathbb{N}$ satisfying (3) such that

— if g is reducible by S, then $\deg(\widetilde{g}) < \deg(g)$;
— if g is irreducible by S, then $\widetilde{g} = g$ and $\alpha_i = 0$, $n_i = 0$ for all i.

Proof. We may assume that g is reducible by S; let $k = \deg(g)$. Write $S_k = \{h_1, \ldots, h_\ell\}$. The h_j's are of the form $X^{n_{i_j}} f_{i_j}$ where $i_j \in \{1, \ldots, s\}$. In particular, there are $\beta_1, \ldots, \beta_\ell \in R$ with $\mathrm{LC}(g) = \sum_j \beta_j \,\mathrm{LC}(h_j)$.

Set $\alpha_{i_j} = \beta_j$ for all j, and set the other α_i's to 0. Similarly, for any i which is not among the i_j's, set $n_i = 0$. Now set

$$\widetilde{g} = g - \sum_{j=1}^{\ell} \beta_j h_j = g - \sum_{i=1}^{s} \alpha_i X^{n_i} f_i,$$

for which $\deg(\widetilde{g}) < \deg(g)$ by (2) and (3). □

Note that $g - \widetilde{g} \in \langle S \rangle$. Applying recursively this lemma, we next obtain what we call a reduction of g by S.

Proposition 2.2. For each $g \in R[X]$ there is $g' \in R[X]$ with

$$g = \sum_{i=1}^{s} g_i f_i + g'$$

for suitable $g_1, \ldots, g_s \in R[X]$ satisfying

$$g_i \neq 0 \Rightarrow \mathrm{LC}(g_i)\,\mathrm{LC}(f_i) \neq 0 \;\&\; \deg(g_i) + \deg(f_i) \leqslant \deg(g) \tag{6}$$

such that

— g' is irreducible by S;
— if g is reducible by S, then $\deg g' < \deg g$;
— if g is irreducible by S, then $g' = g$ and $g_i = 0$ for all i.

Proof. We construct g' by recursion on $\deg(g)$. If g is irreducible by S, which includes the initial case $g = 0$, then $g' = g$ is as required, with $g_i = 0$ for all i. If g is reducible by S, then $\deg(\widetilde{g}) < \deg(g)$ where $\widetilde{g}$ is as in Proposition 2.1; whence there is $\widetilde{g}'$, irreducible by S, with

$$\widetilde{g} = \sum_{i=1}^{s} \widetilde{g}_i f_i + \widetilde{g}'$$

for suitable $\widetilde{g}_1, \ldots, \widetilde{g}_s \in R[X]$ satisfying the appropriate counterpart of (6): that is,

$$\widetilde{g}_i \neq 0 \Rightarrow \mathrm{LC}(\widetilde{g}_i)\,\mathrm{LC}(f_i) \neq 0 \;\&\; \deg(\widetilde{g}_i) + \deg(f_i) \leqslant \deg(\widetilde{g})\,. \tag{7}$$

Now $g' = \widetilde{g}'$ is as required, with $g_i = \widetilde{g}_i + \alpha_i X^{n_i}$ for every i where α_i and n_i are as in Proposition 2.1. To see this, note first that $\deg(\widetilde{g}') \leqslant \deg(\widetilde{g})$ no matter whether $\widetilde{g}$ is reducible; whence

$$\deg(g') = \deg(\widetilde{g}') \leqslant \deg(\widetilde{g}) < \deg(g)$$

in any case. To verify (6), assume that $g_i \neq 0$. Since then either $\widetilde{g}_i \neq 0$ or $\alpha_i \neq 0$, we need to distinguish three cases. First, if $\widetilde{g}_i \neq 0$ and $\alpha_i = 0$, then $g_i = \widetilde{g}_i$, and (6) follows from (7) together with $\deg(\widetilde{g}) < \deg(g)$. Next, if $\widetilde{g}_i = 0$ and $\alpha_i \neq 0$, then $g_i = \alpha_i X^{n_i}$, and (6) is a consequence of (3). Last, if both $\widetilde{g}_i \neq 0$ and $\alpha_i \neq 0$, then $\deg(\widetilde{g}_i) < n_i$ in view of (3), (7), and $\deg(\widetilde{g}) < \deg(g)$; whence $\mathrm{LC}(g_i) = \alpha_i$ and $\deg(g_i) = n_i$, in which case (3) applies again. □

Definition 2.2. Let $g \in R[X]$. We call any g' as in Proposition 2.2 a *reduction* of g by S.

Note that g' is not uniquely determined by g: for example, if $f_1 = X$, $f_2 = X + 1$, then $g = X + 1$ can be reduced to $g'_1 = 1$ with $g = f_1 + g'_1$ and to $g'_2 = 0$ with $g = f_2 + g'_2$.

Note further that $g - g' \in \langle S \rangle$: whence $g \in \langle S \rangle$ if and only if $g' \in \langle S \rangle$. In particular, if a reduction of g is 0, then $g \in \langle S \rangle$. Also, if $g' = 0$ and g is irreducible by S, then $g = 0$.

Lemma 2.2. Let $g \in R[X]$. If $g \in S$ and $g \neq 0$, then g is reducible by S. In particular, $g' = 0$ for every reduction g' of g by S which satisfies $g' \in S$.

Proof. If $g \in S$ and $g \neq 0$ with $\deg(g) = k$, then $g \in S_k$ and thus $\mathrm{LC}(g) \in \mathrm{LC}(S_k)$, which is to say (Lemma 2.1) that g is reducible by S. Recall that every reduction is irreducible. □

2.3. *Extensions of sets of polynomials*

Let $S = \{f_1, \ldots, f_s\}$ be a finite subset of $R[X]$; set $d = \max_{f \in S} \deg(f)$. For each $k \leqslant d$ fix a basis of syzygies B_k of $\mathrm{LC}(S_k)$, which is possible because R is assumed to be coherent. With $S_k = \{h_{k,1}, \ldots, h_{k,\ell}\}$ set

$$p_{k,\alpha} = \sum_{i=1}^{\ell} \alpha_i h_{k,i} \tag{8}$$

for every $\alpha \in B_k$ with $\alpha = (\alpha_1, \ldots, \alpha_\ell)$. Note that $\deg(p_{k,\alpha}) < k$ by Remark 2.1, and $p_{k,\alpha} \in \langle S \rangle$ since $S_k \subseteq \langle S \rangle$. By Proposition 2.2 each $p_{k,\alpha}$ has a—not necessarily uniquely determined—reduction $p'_{k,\alpha}$ by S, for which $p'_{k,\alpha} \in \langle S \rangle$ because $p'_{k,\alpha} - p_{k,\alpha} \in \langle S \rangle$.

Proposition 2.3. There is a finite subset S' of $R[X]$ such that

1 $S \subseteq S'$, and for every $k \leqslant d$ and $\alpha \in B_k$ there is a reduction $p'_{k,\alpha}$ of $p_{k,\alpha}$ with $p'_{k,\alpha} \in S'$;
2 for every $g \in S'$ either $g \in S$ or g is a reduction of $p_{k,\alpha}$ for some $k \leqslant d$ and $\alpha \in B_k$.

Definition 2.3. We call any S' as in Proposition 2.3 an *extension* of S.

In other words, an extension S' of S consists of the elements of S together with finitely many reductions $p_{k,\alpha}$ such that for all $k \leqslant d$ and $\alpha \in B_k$ at least one—and possibly more than one—reduction of $p_{k,\alpha}$ belongs to S'. Note that $\langle S \rangle = \langle S' \rangle$ for every extension S' of S.

Definition 2.4. We call a finite subset S of $R[X]$ a *Gröbner basis* of an ideal I of $R[X]$ if $0 \in S$, $I = \langle S \rangle$, and $S = S'$ for *some* extension S' of S.

If every finitely generated left ideal of $R[X]$ has a Gröbner basis, we say that R is a *Gröbner ring*.

We often simply say "S is a Gröbner basis" in place of "S is a Gröbner basis of $\langle S \rangle$".

Lemma 2.3. The following items are equivalent for each finite subset S of $R[X]$ with $0 \in S$:

1 S is a Gröbner basis.
2 For all $k \leqslant d$ and $\alpha \in B_k$ *some* reduction of $p_{k,\alpha}$ equals 0.

In particular, if S is a Gröbner basis, then for all $k \leqslant d$ and $\alpha \in B_k$:

$$p_{k,\alpha} = \sum_{i=1}^{s} q_{k,\alpha,i} f_i \quad \text{with} \quad \deg(q_{k,\alpha,i}) + \deg(f_i) \leqslant \deg(p_{k,\alpha})\,. \tag{9}$$

Proof. Let first S' be an extension of S with $S = S'$. For all $k \leqslant d$ and $\alpha \in B_k$ there is a reduction $p'_{k,\alpha}$ of $p_{k,\alpha}$ by S such that $p'_{k,\alpha} \in S'$, for which $p'_{k,\alpha} \in S$ by $S = S'$ and thus $p'_{k,\alpha} = 0$ by Lemma 2.2. Conversely, if 0 is a reduction of $p_{k,\alpha}$ for all $k \leqslant d$ and $\alpha \in B_k$, then $S \cup \{0\}$ is an extension of S, which of course equals S whenever $0 \in S$. □

Note that $0 \in S$ is unnecessary for the implication from the first to the second equivalent.

We shall see (Lemma 2.7, Proposition 2.6) that if S is a Gröbner basis, then $S = S'$ for *every* extension S' of S, and that for all $k \leqslant d$ and $\alpha \in B_k$ *every* reduction of $p_{k,\alpha}$ equals 0.

2.4. *Properties of Gröbner bases*

Lemma 2.4. Let $S = \{f_1, \dots, f_s\}$ be a Gröbner basis, $k \in \mathbb{N}$, and $g \in R[X]$ with $\deg(g) < k$. If there are $\alpha_1, \dots, \alpha_s \in R$ and $n_1, \dots, n_s \in \mathbb{N}$ with

$$g = \sum_{i=1}^{s} \alpha_i X^{n_i} f_i \quad \text{and} \quad \alpha_i \neq 0 \Rightarrow n_i + \deg(f_i) = k\,,$$

then there are $g_1, \dots, g_s \in R[X]$ such that

$$g = \sum_{i=1}^{s} g_i f_i \quad \text{and} \quad \deg(g_i) + \deg(f_i) < k\,.$$

Proof. With $S_k = \{h_1, \dots, h_\ell\}$ there are $\beta_1, \dots, \beta_\ell \in R$ such that

$$g = \sum_{j=1}^{\ell} \beta_j h_j.$$

Since $\deg(g) < k$, $\beta = (\beta_1, \dots, \beta_\ell)$ is a syzygy of $\mathrm{LC}(S_k)$ (Remark 2.1).

Let $B_k = \{\beta^1, \dots, \beta^r\}$ be a basis of syzygies of $\mathrm{LC}(S_k)$. We thus can write

$$\beta = \sum_{u=1}^{r} \lambda_u \beta^u$$

where $\lambda_u \in R$ for every $u \leqslant r$; with $\beta^u = (\beta^u_1, \dots, \beta^u_\ell)$ this amounts to

$$\beta_j = \sum_{u=1}^{r} \lambda_u \beta^u_j$$

for every $j \leqslant \ell$. For each $u \leqslant r$ let

$$p_u = \sum_{j=1}^{\ell} \beta^u_j h_j\,,$$

for which $\deg(p_u) < k$ (Remark 2.1). Now we can rewrite g as

$$g = \sum_{u=1}^{r} \lambda_u p_u.$$

Let $d = \max_i \deg(f_i)$, and $u \leqslant \ell$. If $k \leqslant d$, then p_u is one of the $p_{k,\alpha}$ from (8); if $k > d$, then p_u is equal to some $X^{k-d} p_{d,\alpha}$. In any case 0 is a reduction of p_u (Lemma 2.3); whence

$$p_u = \sum_i q_{u,i} f_i \quad \text{with} \quad \deg(q_{u,i}) + \deg(f_i) \leqslant \deg(p_u)$$

as in (9), from which together with $\deg(p_u) < k$ the desired result follows immediately. □

Lemma 2.5. Let $S = \{f_1, \ldots, f_s\}$ be a Gröbner basis, $k \in \mathbb{N}$, and $g \in R[X]$ with $\deg(g) < k$. For any $h_1, \ldots, h_s \in R[X]$ with

$$g = \sum_{i=1}^{s} h_i f_i \quad \text{and} \quad \max_i(\deg(h_i) + \deg(f_i)) = k$$

there are $g_1, \ldots, g_s \in R[X]$ such that

$$g = \sum_{i=1}^{s} g_i f_i \quad \text{with} \quad \max_i(\deg(g_i) + \deg(f_i)) < k\,.$$

Proof. Let $g = \sum_i h_i f_i$ with $\deg(g) < k$ and $\max_i(\deg(h_i)+\deg(f_i)) = k$. We construct $\hat{g} = \sum_i \alpha_i X^{n_i} f_i$ as follows:
— if $\deg(h_i) + \deg(f_i) = k$, then set $\alpha_i = \mathrm{LC}(h_i)$ and $n_i = \deg(h_i)$;
— if $\deg(h_i) + \deg(f_i) < k$, then set $\alpha_i = 0$ and $n_i = 0$.
We now have

$$g - \hat{g} = \sum_i (h_i - \alpha_i X^{n_i}) f_i \quad \text{and} \quad \deg(h_i - \alpha_i X^{n_i}) + \deg(f_i) < k\,;$$

in particular, $\deg(\hat{g}) < k$ because $\deg(g) < k$; moreover, $n_i + \deg(f_i) = k$ whenever $\alpha_i \neq 0$. Hence by Lemma 2.4 there are $\hat{g}_1, \ldots, \hat{g}_s \in R[X]$ such that

$$\hat{g} = \sum_i \hat{g}_i f_i \quad \text{and} \quad \deg(\hat{g}_i) + \deg(f_i) < k.$$

If we set $g_i = (h_i - \alpha_i X^{n_i}) + \hat{g}_i$, then $g = \sum_i g_i f_i$ with $\deg(g_i) + \deg(f_i) < k$ as required. □

Iterated applications of Lemma 2.5 yield the following.

Proposition 2.4. If an ideal I of $R[X]$ has a Gröbner basis $\{f_1, \ldots, f_s\}$, then for each $g \in I$ there are $g_1, \ldots, g_s \in R[X]$ such that

$$g = \sum_{i=1}^{s} g_i f_i \quad \text{and} \quad \deg(g) = \max_i(\deg(g_i) + \deg(f_i))\,.$$

Given an ideal I of $R[X]$ and $k \in \mathbb{N}$, the following subset is an ideal of R:

$$\ell_k(I) = \{a \in R : \exists a_0, \ldots, a_{k-1} \in R\,(aX^k + a_{k-1}X^{k-1} + \cdots + a_0 \in I)\}\,.$$

In other words, $\ell_k(I)$ is the set of the leading coefficients of the $g \in I$ with $\deg(g) \leqslant k$.

Proposition 2.5. If an ideal I of $R[X]$ has a Gröbner basis S, then $\ell_k(I) = \langle \mathrm{LC}(S_k)\rangle$ for every k; in particular, $\ell_k(I)$ is a finitely generated ideal of R for every k.

Proof. It suffices to prove that $\mathrm{LC}(g) \in \langle \mathrm{LC}(S_k)\rangle$ for every $g \in I$ with $g \neq 0$ and $\deg(g) = k$. Let $S = \{f_1, \ldots, f_s\}$. By Proposition 2.4 we can achieve that

$$g = \sum_i g_i f_i \quad \text{with} \quad \max_i(\deg(g_i) + \deg(f_i)) = k\,.$$

If we set $J = \{i \leqslant s : \deg(g_i) + \deg(f_i) = k\}$, then $\mathrm{LC}(g) = \sum_{i\in J} \mathrm{LC}(g_i)\,\mathrm{LC}(f_i)$ belongs to $\langle \mathrm{LC}(S_k)\rangle$: in fact, if $i \in J$, then $X^{n_i} f_i \in S_k$ with $n_i = \deg(g_i)$, and thus $\mathrm{LC}(f_i) \in \mathrm{LC}(S_k)$. □

Corollary 2.2. If an ideal I of $R[X]$ has a Gröbner basis, then the set $\mathrm{LC}(I)$ consisting of the leading coefficients of all the elements of I is a finitely generated ideal of R.

Proof. Let S be a Gröbner basis for I, and $d = \max_{f\in S\setminus\{0\}} \deg(f)$. Then

$$\mathrm{LC}(I) = \bigcup_{k\geqslant 0} \ell_k(I) = \bigcup_{k\geqslant 0} \langle \mathrm{LC}(S_k)\rangle = \langle \mathrm{LC}(S_d)\rangle = \ell_d(I)$$

by Proposition 2.5 and (1) on page 6. □

Lemma 2.2 is a forerunner of the following.

Lemma 2.6. Let S be a Gröbner basis of the left ideal I of $R[X]$, and $g \in R[X]$.

1 If $g \in I$ and $g \neq 0$, then g is reducible by S.
2 The following items are equivalent:
   (a) $g \in I$.
   (b) *Every* reduction of g by S is 0.
   (c) *Some* reduction of g by S is 0.

Proof. 1. If $g \in I$ and $g \neq 0$, then $\mathrm{LC}(g) \in \ell_k(I)$ where $k = \deg(g)$; by Proposition 2.5 we thus have $\mathrm{LC}(g) \in \langle \mathrm{LC}(S_k)\rangle$, which is to say (Lemma 2.1) that g is reducible by S.

2. If $g \in I$, and g' is a reduction of g by S, then $g' \in I$ (because $g - g' \in I$), and g' is irreducible; whence $g' = 0$ according to the first item of this lemma. □

Corollary 2.3. If R is a Gröbner ring, then $R[X]$ is strongly discrete.

Proof. Let S be a Gröbner basis of the finitely generated ideal I of $R[X]$. Given any $g \in R[X]$, pick a reduction g' of g by S. Since R is (strongly) discrete, we can check whether $g' = 0$, and thus decide whether $g \in I$. □

Recall that the $p_{k,\alpha}$ from (8) all belong to $\langle S\rangle$. By Lemma 2.3 and Lemma 2.6 we have:

Lemma 2.7. For a finite subset S of $R[X]$ with $0 \in S$, the following are equivalent:

1 S is a Gröbner basis.
2 For each $k \leqslant d$ and $\alpha \in B_k$ *every* reduction of $p_{k,\alpha}$ equals 0.
3 For each $k \leqslant d$ and $\alpha \in B_k$ *some* reduction of $p_{k,\alpha}$ equals 0.

Proposition 2.6. It is decidable whether a finite subset S of $R[X]$ is a Gröbner basis; and if S is a Gröbner basis, then $S = S'$ for *every* extension S' of S.

Proof. Since R is (strongly) discrete, it is decidable whether $0 \in S$. Assume now that $0 \in S$. For every $k \leqslant d$ and $\alpha \in B_k$ pick any reduction $p'_{k,\alpha}$ of $p_{k,\alpha}$. By Lemma 2.7, S is a Gröbner basis if and only if $p'_{k,\alpha} = 0$ for all $k \leqslant d$ and $\alpha \in B_k$, which is decidable.

Assume now that S is a Gröbner basis, and let S' be any extension of S. Apart from the elements of S, the elements of S' are reductions $p'_{k,\alpha}$ of the $p_{k,\alpha}$ with $k \leqslant d$ and

$\alpha \in B_k$. But all those $p'_{k,\alpha}$ are 0 in view of Lemma 2.7, and thus belong to S because $0 \in S$. □

2.5. *Existence of Gröbner bases*

We are going to show that if R is $\mathcal{RS}$-Noetherian, then for each finite subset S^0 of $R[X]$ by successive extensions $S^{i+1} = (S^i)'$ we arrive in a finite number of steps at a Gröbner basis of $\langle S^0\rangle$. Since $\langle \mathrm{LC}(S_k)\rangle = \langle \mathrm{LC}(S_{k+1})\rangle$ for all $k \geqslant \max_{f\in S} \deg(f)$, the sequence

$$\Phi(S) = \big(\langle \mathrm{LC}(S_i)\rangle\big)_{i\in\mathbb{N}}$$

belongs to $\mathfrak{I}^\star_R$. Clearly, $\Phi(S) \geqslant \Phi(T)$ in $\mathfrak{I}^\star_R$ whenever $S \geqslant T$ in $\mathfrak{I}_{R[X]}$: that is, when $S \subseteq T$.

Lemma 2.8. For every extension S' of a finite subset S of $R[X]$ with $0 \in S$, we have $\Phi(S) \geqslant \Phi(S')$ in $\mathfrak{I}^\star_R$, and moreover $\Phi(S) = \Phi(S')$ if and only if $S = S'$.

Proof. The first assertion is clear from $S \subseteq S'$. As for the second, assume that $\Phi(S) = \Phi(S')$, and remember that every element of S' which does not belong to S is a reduction h' of some $h \in R[X]$. To verify $S \supseteq S'$ it therefore suffices to show that if $h' \in S'$, then $h' = 0$; the latter indeed implies $h' \in S$ because $0 \in S$. Since R is (strongly) discrete, either $h' = 0$ or else $h' \neq 0$. In the latter case $\mathrm{LC}(h') \in \langle \mathrm{LC}(S'_k)\rangle$ with $k = \deg(h')$; since $\Phi(S) = \Phi(S')$, we thus have $\mathrm{LC}(h') \in \langle \mathrm{LC}(S_k)\rangle$, which (Lemma 2.1) contradicts the irreducibility of h'. □

The proof of the following in general requires an invocation of dependent choice.

Theorem 2.1. If R is $\mathcal{RS}$-Noetherian, then R is a Gröbner ring.

Proof. Let S^0 be a finite subset of $R[X]$, and $I = \langle S^0\rangle$. We may assume that $0 \in S^0$. Construct a sequence of iterated extensions $(S^i)_{i\in\mathbb{N}}$ by setting $S^{i+1} = (S^i)'$ where $(S^i)'$ is any extension of S^i, which exists by Proposition 2.3. Note that $0 \in S^i$ and $\langle S^i\rangle = I$ for every i.

Now R is $\mathcal{RS}$-Noetherian: that is, $\mathfrak{I}_R \in \mathcal{RS}$. By Theorem 1.1, also $\mathfrak{I}^\star_R \in \mathcal{RS}$. Since $\Phi(S^0) \geqslant \Phi(S^1) \geqslant \cdots$ in $\mathfrak{I}^\star_R$, there is $n \geqslant 0$ with $\Phi(S^n) = \Phi(S^{n+1})$, for which $S^n = S^{n+1}$ by Lemma 2.8. Hence S^n is a Gröbner basis of the finitely generated left ideal I. □

2.6. *Bases of syzygies in $R[X]$*

To allow for some convenient notations from linear algebra, we consider a finite family $(f_1, \ldots, f_n)$ of elements of R as a column vector $f \in R^{n\times 1}$. A syzygy of f is then nothing but a row vector $a \in R^{1\times n}$ such that $af = 0$.

Independence of generators The following lemma is a classic: see (Mines *et al.* 1988, Theorem III.2.2), (Glaz 1989, Lemma 2.1.1), and (Lombardi and Quitté 2011, IV.1). Here we give a particularly elementary proof.

Lemma 2.9. Let $f = (f_1, \ldots, f_n) \in R^{n\times 1}$ and $g = (g_1, \ldots, g_m) \in R^{m\times 1}$ such that $\langle f\rangle = \langle g\rangle$. If g has a basis of syzygies, then f has a basis of syzygies.

Proof. There are $A \in R^{m\times n}$ and $B \in R^{n\times m}$ such that $Af = g$ and $Bg = f$. Let $M = BA - I_n$. Clearly, $Mf = 0$, so if $s_1, \ldots s_n \in R^{1\times n}$ are the rows of M, then each s_i is a syzygy of f. If a is a syzygy of f, then aB is a syzygy of g, and if b is a syzygy of g, then bA is a syzygy of f.

Let $\beta_1, \ldots, \beta_\ell \in R^{1\times m}$ be a basis of syzygies of g. Every $\alpha_i = \beta_i A$ is a syzygy of f. Moroever, $(\alpha_1, \ldots, \alpha_\ell, s_1, \ldots, s_n)$ is basis of syzygies of f. To see this let $a \in R^{1\times n}$ be a syzygy of f. Then aB is a syzygy of g, and $aB = \sum_{i=1}^{\ell} b_i\beta_i$ for suitable $b_1, \ldots, b_\ell \in R$. Hence

$$a = aBA - aM = \sum_{i=1}^{\ell} b_i\beta_i A - aM = \sum_{i=1}^{\ell} b_i\alpha_i - \sum_{i=1}^{n} a_i s_i$$

by virtue of $BA = I_n + M$. □

In particular, whether a finitely generated ideal has a basis of syzygies is independent of any particular choice of a finite set of generators.

Coherence with Gröbner bases We fix $f = (f_1, \ldots, f_n) \in R[X]^{n\times 1} \setminus \{0\}$ for the rest of this section, and set

$$d = \max_{j=1,\ldots,n} \deg(f_j)\,.$$

Just as $S \setminus \{0\} = \{f_1, \ldots, f_n\}$ we view S_k and $\mathrm{LC}(S_k)$ as finite families, for every $k \in \mathbb{N}$. As already noted, for $k \geqslant d$ we have $S_k = X^{k-d}S_d$, and thus $\mathrm{LC}(S_k) = \mathrm{LC}(S_d)$.

Given $k \in \mathbb{N}$ we write $S_k = (h_1, \ldots, h_{m_k})$ where $m_k \leqslant n$ and $h_i = X^{d_i} f_{\varphi_k(i)}$ with

$$1 \leqslant \varphi_k(1) < \ldots < \varphi_k(m_k) \leqslant n$$

such that $j = \varphi_k(i)$ for some i precisely when $\deg(f_j) \leqslant k$. Note that $d_i = k - \deg f_{\varphi_k(i)}$ for every i. We next consider the linear map

$$\Phi_k : R^{1\times n} \to R^{1\times m_k}\,, \quad (\alpha_1, \ldots, \alpha_n) \mapsto (\alpha_{\varphi_k(1)}, \ldots, \alpha_{\varphi_k(m_k)})\,.$$

Note that if $k \geqslant d$, then $m_k = n$ and thus $\Phi_k = \mathrm{id}$. We further define the linear map

$$\Psi_k : R^{1\times m_k} \to R^{1\times n}\,, \quad (\beta_1, \ldots, \beta_{m_k}) \mapsto (\alpha_1, \ldots, \alpha_n)$$
$$\text{where} \quad \alpha_j = \begin{cases} \beta_i & \text{if } j = \varphi_k(i) \text{ for some } i\,, \\ 0 & \text{if } j \neq \varphi_k(i) \text{ for every } i\,. \end{cases}$$

Clearly, $\Phi_k \circ \Psi_k = \mathrm{id}$; and $\Psi_k(\beta)$ is a syzygy of $\mathrm{LC}(S)$ whenever β is a syzygy of $\mathrm{LC}(S_k)$.

Now let $g \in R[X]^{1\times n}$. We set

$$k(g) = \max_{j=1,\ldots,n} (\deg(g_j) + \deg(f_j))$$

with the convention that $\deg(0) = -\infty$ (in particular $k(g) = -\infty$ when $g_j = 0$ for all j).

Now let $k \in \mathbb{N}$. We set

$$C_k(g_j) = \begin{cases} \text{the coefficient of } X^{k-\deg(f_j)} \text{ in } g_j & \text{if } 0 \leqslant k - \deg(f_j) \leqslant \deg(g_j)\,, \\ 0 & \text{otherwise} \end{cases}$$

for every $j \in \{1, \dots, n\}$, and define accordingly the linear map

$$C_k : R[X]^{1\times n} \to R^{1\times n}\,, \quad (g_1, \dots, g_n) \mapsto (C_k(g_1), \dots, C_k(g_n))\,.$$

Note that if $k \geqslant k(g)$, then

$$C_k(g_j) = \begin{cases} \mathrm{LC}(g_j) & \text{if } \deg(g_j) + \deg(f_j) = k\,, \\ 0 & \text{otherwise} \end{cases}$$

for every j. Hence, still for $k \geqslant k(g)$,

$$k > k(g) \iff C_k(g) = 0\,. \tag{10}$$

In particular, $C_{k(g)}(g) \neq 0$ whenever $g \neq 0$.

We finally set $\beta_k = \Phi_k \circ C_k : R[X]^{1\times n} \to R^{1\times m_k}$, which is a linear map. Note that for $k \geqslant k(g)$, $C_k(g_j) \neq 0$ implies that $\deg(f_k) \leqslant k$,, hence $j = \varphi_k(i)$ for some i; thus clearly $\beta_k(g) = 0$ precisely when $C_k(g) = 0$, and it follows that if $k \geqslant k(g)$,

$$k > k(g) \iff \beta_k(g) = 0\,. \tag{11}$$

Now we define

$$\beta : R[X]^{1\times n} \setminus \{0\} \to R^{1\times m_{k(g)}} \setminus \{0\}\,, \quad g \mapsto \beta_{k(g)}(g)\,.$$

Clearly, $\beta(g)$ is a syzygy of $\mathrm{LC}(S_{k(g)})$ if and only if $\deg(gf) < k(g)$, which is the case if, for instance, g is a syzygy of S: that is, $gf = 0$.

Although β is no longer a linear mapping, we have $\beta(-g) = -\beta(g)$, and the following.

Lemma 2.10. Let $k \in \mathbb{N}$, and $g, g' \in R[X]^{1\times n}$. If $k(g) = k(g') = k$, then $k(g+g') \leqslant k$ and

1. $k(g+g') < k \iff \beta(g) + \beta(g') = 0\,;$
2. $k(g+g') = k \implies \beta(g) + \beta(g') = \beta(g+g')\,.$

Proof. Note first that $g \neq 0$ and $g' \neq 0$, whereas $g + g'$ may be $= 0$. In any case

$$\beta(g) + \beta(g') = \beta_k(g) + \beta_k(g') = \beta_k(g+g')\,. \tag{12}$$

If $k(g+g') = k$, then also $\beta_k(g+g') = \beta(g+g')$; whence part 2 is proved.

If $k(g+g') < k$ then $\beta_k(g+g') = 0$, thus $\beta(g)+\beta(g') = 0$. Conversely, if $\beta(g)+\beta(g') = 0$ then $\beta_k(g+g') = 0$ and, by (11), $k(g+g') < k$; whence part 1 is proved. □

Lemma 2.11. If S is a Gröbner basis, and $k \leqslant d = \max_j \deg(f_j)$, then for every syzygy β of $\mathrm{LC}(S_k)$ with $\beta \neq 0$ there is a syzygy g_β of S such that $k(g_\beta) = k$ and $\beta(g_\beta) = \beta$.

Proof. With the notations developed before Lemma 2.10 we set $\alpha = \Psi_k(\beta)$ and

$$\ell_j = \begin{cases} d_i & \text{if } j = \varphi_k(i) \text{ for some } i\,, \\ 0 & \text{if } j \neq \varphi_k(i) \text{ for every } i\,. \end{cases}$$

If $\alpha_j \neq 0$, then $j = \varphi_k(i)$ for some i, for which

$$\ell_j + \deg(f_j) = d_i + \deg(f_{\varphi_k(i)}) = k\,.$$

Since α is a syzygy of $\mathrm{LC}(S)$, we further have $\deg(\sum_{j=1}^n \alpha_j X^{\ell_j} f_j) < k$.

Hence by Lemma 2.4 there are $e_1, \dots, e_n \in R[X]$ such that

$$\sum_{j=1}^{n} \alpha_j X^{\ell_j} f_j = \sum_{j=1}^{n} e_j f_j \quad \text{with} \quad \deg(e_j) + \deg(f_j) < k\,.$$

We now define $g_\beta = (g_1, \dots, g_n) \in R[X]^{1\times n}$ by $g_j = \alpha_j X^{\ell_j} - e_j$ for $j = 1, \dots, n$.

We have $\deg(g_j) + \deg(f_j) \leqslant k$ for every j, where equality holds precisely when $\alpha_j \neq 0$. By hypothesis there is i such that $\alpha_{\varphi_k(i)} = \beta_i \neq 0$; whence $k(g_\beta) = k$. Finally, $C_k(g_\beta) = \alpha = \Psi_k(\beta)$, thus $\beta(g_\beta) = \Phi_k(C_k(g_\beta)) = \Phi_k \circ \Psi_k(\beta) = \beta$. □

Proposition 2.7. Assume that f is a Gröbner basis. If $(\beta_1^k, \dots, \beta_{m_k}^k)$ is a basis of syzygies of $\mathrm{LC}(S_k)$ for every $k \leqslant d$, then $(g_{\beta_j^k} : j \leqslant m_k, k \leqslant d)$ is a basis of syzygies of f.

Proof. Let $g = (g_1, \dots, g_n)$ be a syzygy of f; set $k = \min\{k(g), d\}$. Clearly, $\beta(g)$ is a syzygy of $\mathrm{LC}(S_k) = \mathrm{LC}(S_{k(g)})$; whence there are $b_1, \dots, b_{m_k} \in R$ with $\beta(g) = b_1\beta_1^k + \cdots + b_{m_k}\beta_{m_k}^k$.

Let

$$g' = \sum_{i=1}^{m_k} b_i X^{k(g)-k} g_{\beta_i^k},$$

and $\widehat{g} = g - g'$. For every i we have $k(g_{\beta_i^k}) = k$, thus $k(b_i X^{k(g)-k} g_{\beta_i^k}) = k(g)$, and since $\beta(g_{\beta_i^k}) = \beta_i^k$ we have $\beta(b_i X^{k(g)-k} g_{\beta_i^k}) = b_i\beta_i^k$. Since $\sum_{i=1}^{m_k} b_i\beta_i^k = \beta(g) \neq 0$, from iterated applications of Lemma 2.10 we get $k(g') = k(g)$ and $\beta(g') = \sum_{i=1}^{m_k} b_i\beta_i^k = \beta(g)$. Now $\hat{g}$ is a syzygy of f and using Lemma 2.10 again we get $k(\widehat{g}) < k(g)$: we are done by induction on $k(g)$. □

Corollary 2.4. If R is a Gröbner ring, then $R[X]$ is coherent.

3. A Unified Hilbert Basis Theorem

Let R be a not necessarily commutative ring. Recall that "R is $\mathcal{C}$-Noetherian" means (Definition 1.1) that R is coherent and strongly discrete, and that $\mathfrak{I}_R$ belongs to the given Noether class $\mathcal{C}$. In particular, if R is $\mathcal{C}$-Noetherian, then the results from Section 2 apply to R, and R is $\mathcal{RS}$-Noetherian: any Noether class $\mathcal{C}$ is contained in the Richman-Seidenberg class $\mathcal{RS}$. From the definition of a Noether class $\mathcal{C}$ (Section 1.1) we will further use that if there is a strictly increasing mapping $E \to F$ between posets E and F, then $E \in \mathcal{C}$ whenever $F \in \mathcal{C}$.

Lemma 3.1. If R is $\mathcal{RS}$-Noetherian, then the mapping

$$\begin{array}{rccc} \Psi & : & \mathfrak{I}_{R[X]} & \to & \mathfrak{I}_R^\star \\ & & I = \langle f_1, \dots, f_m \rangle & \mapsto & (\ell_0(I), \dots, \ell_d(I)) \quad \text{where } d = \max \deg(f_i) \end{array}$$

is well-defined, and strictly increasing.

Proof. By Theorem 2.1 and Proposition 2.5, the mapping Ψ is well-defined. In fact, $\Psi(I) = \Phi(S)$ where S is a Gröbner basis of I and Φ is the mapping defined in Section 2.5.

Given $I, J \in \mathfrak{I}_{R[X]}$ with $I \subseteq J$ we have $\ell_n(I) \subseteq \ell_n(J)$ for every n: that is, Ψ is increasing. To prove that Ψ is strictly increasing, let $I, J \in \mathfrak{I}_R[X]$ with $I \subseteq J$, and assume that $\ell_n(I) = \ell_n(J)$ for every $n \in \mathbb{N}$. We deduce that $I \supseteq J$ as well, by showing $f \in I$ for each $f \in J$.

To this end we proceed by induction on n where $f = aX^n + g$ for suitable $a \in R$ and $g \in R[X]$ with $\deg g < n$. If $n = 0$, then $f = a$ belongs to $\ell_0(J) = \ell_0(I)$; whence $f \in I$ as required. Assume next that $n > 0$. Since a is an element of $\ell_n(J) = \ell_n(I)$, we also have $aX^n + h \in I$ for some $h \in R[X]$ with $\deg h < n$. Now

$$g - h = f - (aX^n + h) \in J$$

and thus, by induction, $g - h \in I$; whence

$$f = aX^n + h + (g - h) \in I$$

as required, simply because $aX^n + h \in I$ and $J \subseteq I$. □

The existence of a Gröbner basis was only needed for proving that Ψ is well-defined.

Theorem 3.1. If R is $\mathcal{C}$-Noetherian, then $R[X]$ is $\mathcal{C}$-Noetherian.

Proof. Let R be $\mathcal{C}$-Noetherian. First, $R[X]$ is coherent and strongly discrete by Corollary 2.4 and Corollary 2.3, respectively. By Theorem 1.1, moreover, we have $\mathfrak{I}_R^\star \in \mathcal{C}$, and thus $\mathfrak{I}_{R[X]} \in \mathcal{C}$ by Lemma 3.1. □

Corollary 3.1. If R is $\mathcal{C}$-Noetherian, then $R[X_1, \ldots, X_n]$ is $\mathcal{C}$-Noetherian.

4. Discussion

With Theorem 3.1 we have also reproved Theorem VIII.1.5 of (Mines *et al.* 1988): if R is $\mathcal{RS}$-Noetherian, then so is $R[X]$. The road we have followed is on the one hand somewhat more specific: we needed to suppose from the outset that R be strongly discrete, whereas in (Mines *et al.* 1988) the issue of strong discreteness could be treated separately. (Coherence needed to be included in (Mines *et al.* 1988), too.) On the other hand our approach is more general inasmuch as it works for all Noether classes of posets rather than being limited to the Richman-Seidenberg chain condition. In particular we also have reproved the Hilbert basis theorem for strongly Noetherian rings (Perdry 2004).

While in the classical proof of the Hilbert basis theorem referred to in the introduction one needs to invoke the ascending chain condition on $\mathfrak{I}_R^\star$ only once, in the constructive proof provided in the present paper we have used twice that $\mathfrak{I}_R^\star \in \mathcal{C}$. The additional invocation is required to prove that the mapping Ψ from Lemma 3.1 is well-defined, which is to say that

(*) for each $I \in \mathfrak{I}_{R[X]}$ all the $\ell_n(I)$ belong to $\mathfrak{I}_R$.

In view of Proposition 2.5 the ring R has property (*) provided that R is a Gröbner ring which by Theorem 2.1 can be ensured whenever R is $\mathcal{RS}$-Noetherian; more precisely—see the proof of Theorem 2.1—one needs that $\mathfrak{I}_R^\star \in \mathcal{RS}$.

Yet it is possible to prove (*) without any talk of Gröbner bases, following (Mines *et*

al. 1988) and using $\mathfrak{I}_R \in \mathcal{RS}$ rather than $\mathfrak{I}_R^\star \in \mathcal{RS}$—that is, by applying the Richman-Seidenberg condition to chains of ideals rather than to chains of chains of ideals; see Appendix 5.1 below. However, the avenue we have followed above is not only closer to the classical proof quoted in the introduction but might also be considered somewhat more natural. In a similar way, Gröbner bases have been used for constructive proofs in the context of polynomials over a field (Lombardi and Perdry 1998).

5. Appendix

5.1. *Doing without Gröbner bases*

We sketch how, following (Mines *et al.* 1988) and without Gröbner bases, one can see that if R is coherent and $\mathcal{RS}$-Noetherian, and I is a finitely generated ideal of $R[X]$, then for every n the ideal $\ell_n(I)$ of R is finitely generated.

Let first R be an arbitrary ring, and $n \geqslant 0$. As in (Mines *et al.* 1988) we denote by $R[X]_{n+1}$ the set of polynomials of degree $\leqslant n$. This is a free R-module of rank $n+1$. The mapping

$$\mathrm{LC} : R[X]_{n+1} \to R\,,\ f \mapsto \mathrm{LC}(f)$$

is R-linear, and for every left ideal I of $R[X]$ we have

$$\mathrm{LC}(I \cap R[X]_{n+1}) = \ell_n(I)\,.$$

Now let R be coherent and $\mathcal{RS}$-Noetherian. Theorem VIII.1.2 of (Mines *et al.* 1988) says that if I is a finitely generated left ideal of $R[X]$, then $I \cap R[X]_{n+1}$ is a finitely generated R-module. In all,

$$I \in \mathfrak{I}_{R[X]} \implies \ell_n(I) \in \mathfrak{I}_R\,.$$

5.2. *Corrections to the preparatory paper*

We list three substantial corrections to (Perdry and Schuster 2011).

1 In the proof of Proposition 3.1, $\varphi(a_n) \geqslant \varphi(a_{n+1})$ must be replaced by $\varphi(a_n) = \varphi(a_{n+1})$.

2 The proof of Proposition 4.1 needs to be concluded as follows. Let T be a decreasing tree with root labelled by y. To prove that T has finite depth, let $a_1, \dots, a_k$ with $k \geqslant 0$ be the childs of the root of T, labelled by $x_1, \dots, x_k$. For each i, if $x_i < y$, then $x_i \in H$ by hypothesis; whence the subtree of T with root a_i has depth $\leqslant N_i$ for some $N_i \in \mathbb{N}$. Set $N = \max\{N_i : x_i < y\}$. We show that T halts before $N+1$. To this end, let u be a branch of T. We either have $|u| \leqslant 0$, in which case u halts before $|u|+1 \leqslant 1$, or else $|u| \geqslant 1$. In the latter case, there is i such that u passes through a_i. If $x_i = y$, then u halts before 1; if otherwise $x_i < y$, then u halts before $N_i + 1 \leqslant N + 1$.

3 In the proof of Lemma 4.1, four occurrences of $\mathcal{C}$ need to be read as $\mathcal{FD}$.

5.3. *Prime decomposition with trees of finite depth*

As in (Perdry 2004) we study a *minimal prime property* of a strongly discrete, commutative ring A:

MPP *For every* $\mathfrak{a} \in \mathfrak{I}_A$ *there are prime ideals* $\mathfrak{p}_1, \ldots, \mathfrak{p}_k \in \mathfrak{I}_A$ *with* $\mathfrak{p}_i \supseteq \mathfrak{a}$ *for every* i *such that if* $\mathfrak{p} \in \mathfrak{I}_A$ *is a prime ideal with* $\mathfrak{p} \supseteq \mathfrak{a}$*, then* $\mathfrak{p} \supseteq \mathfrak{p}_i$ *for some* i*.*

By removing the unnecessary ones among the $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ one indeed obtains the minimal primes over $\mathfrak{a}$. All the ideals that occur in MPP are supposed to be finitely generated.

In the following, as in (Perdry 2004), one needs to assume that A allows for a *strong primality test*:

SPT *For every* $\mathfrak{a} \in \mathfrak{I}_A$ *either* $\mathfrak{a}$ *is a prime ideal or else there is* $rs \in \mathfrak{a}$ *with* $r, s \notin \mathfrak{a}$*.*

With SPT a constructive proof of MPP has been given (Perdry 2004) in each of the following cases:

(i) A is $\mathcal{RS}$-Noetherian, and the fan theorem for binary trees is assumed;
(ii) A is a fully Lasker-Noether ring in the sense of (Perdry 2004).

Following the method of (Perdry 2004) we now sketch how to relax these hypotheses: we prove MPP still with SPT but in the case that A is $\mathcal{FD}$-Noetherian. Here $\mathcal{FD}$ is the Noether class of posets that have the finite-depth property (Perdry and Schuster 2011), which we recall first. Since every fully Lasker-Noether ring is strongly Noetherian in the sense of (Perdry 2004), and every strongly Noetherian ring is $\mathcal{FD}$-Noetherian (Perdry and Schuster 2011), our treatment includes case (ii). As we only need to consider binary trees, it includes case (i) too: $\mathcal{FD}$ equals $\mathcal{RS}$ in the presence of the fan theorem (Perdry and Schuster 2011).

5.3.1. *Trees of finite depth* We briefly sketch the required material from (Perdry and Schuster 2011). A *(finitely branching) tree* is a poset T such that T has a least element ε, the *root* of T; for every $a \in T$ the set $D_a = \{x \in T : a < x\}$ has a finite number of minimal elements, the *childs* of a; and for every $a \in T$ the set $\{x \in T : x < a\}$ is a finite chain. The elements of T are also called *nodes*. If $D_a = \varnothing$, then a is a *leaf* of T.

A *branch* of T is a (possibly finite) sequence $a_0 = \varepsilon, a_1, a_2, \ldots$ in T such that a_{i+1} is a child of a_i for all i. If $u = a_0, a_1, a_2, \ldots, a_n$ is a finite branch of T, then $|u| = n$ is the *length* of u. We say that the length of the empty sequence $()$ is < 0, and that an infinite branch of T has length $\geqslant n$ for all $n \in \mathbb{N}$.

A mapping $\varphi : F \to G$ between posets is *(strictly) decreasing* if $\varphi : F \to G^\circ$ is (strictly) increasing where G° stands for G with the reverse order. A mapping φ from a tree T to a set E is called a *labelling* of (the nodes of) T by (the elements of) E. Now let T be a tree labelled by a poset E with labelling $\varphi : T \to E$. We further assume that T is a *(strictly) decreasing* tree: that is, φ is a (strictly) decreasing mapping.

A (finite or infinite) branch $u = a_0, a_1, a_2, \ldots$ of T *halts before* $N \in \mathbb{N}$ if either $|u| < N$ or else $|u| \geqslant N$ and there is $n < N$ with $\varphi(a_n) = \varphi(a_{n+1})$. If a branch halts before N, then it halts before M for every $M \geqslant N$; a finite branch $u = a_0, a_1, a_2, \ldots, a_N$ halts before $|u| = N$ precisely when $\varphi(a_n) = \varphi(a_{n+1})$ for some $n < N$. Last but not least, only $()$ halts before 0.

We say that T has *depth* $\leqslant N$ if every branch of T halts before N. Finally, T has *finite depth* if it has depth $\leqslant N$ for some $N \in \mathbb{N}$. (This notion of depth is essentially the one given in (Mines *et al.* 1988, I.5).) A poset E has the *finite-depth property* if every decreasing tree T labelled by E has finite depth. The class $\mathcal{FD}$ consisting of the posets

with the finite-depth property is a Noether class; in particular, $\mathcal{FD}$ is a subclass of the Richman-Seidenberg class $\mathcal{RS}$.

If a branch in a strictly decreasing tree halts before n, then it has length $< n$. Hence if a poset E is in $\mathcal{FD}$, then every strictly decreasing tree T labelled by E is *finite*: that is, there is $N \in \mathbb{N}$ such that every branch of T is finite and has length $\leqslant N$. If a tree T is finite, then it is *well-founded*: that is, every branch of T is finite. The *generalized fan theorem (GFT)* says that, for every tree T, if T is well-founded, then T is finite. This GFT is equivalent to the assertion that $\mathcal{RS}$ actually equals $\mathcal{FD}$.

5.3.2. *Prime decomposition* Let A be a strongly discrete, commutative ring.

Proposition 5.1. If A is $\mathcal{FD}$-Noetherian, and we have SPT for A, then MPP holds for A.

Proof. We construct, for each $\mathfrak{a} \in \mathfrak{I}_A$, a strictly decreasing binary tree labelled by $\mathfrak{I}_A$. To start with, let the root be labelled by $\mathfrak{a}$. By SPT either $\mathfrak{a}$ is prime, in which case we stop the construction, or else there is $rs \in \mathfrak{a}$ with $r, s \notin \mathfrak{a}$. In the latter case we endow the root of the tree with two childs, label them by the ideals $\mathfrak{a} + \langle r \rangle$ and $\mathfrak{a} + \langle s \rangle$ strictly containing $\mathfrak{a}$, and continue the construction of the tree by applying SPT to each of them.

Since $\mathfrak{I}_A$ has the finite-depth property, the resulting tree is finite. Moreover, the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ labelling the leaves of the tree are as required. They indeed belong to $\mathfrak{I}_A$, contain $\mathfrak{a}$, and are prime ideals. It thus remains to see that if $\mathfrak{p} \in \mathfrak{I}_A$ is a prime ideal with $\mathfrak{p} \supseteq \mathfrak{a}$, then $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i. Starting with the case $\mathfrak{a} = \mathfrak{b}$, this follows from the following consideration.

Let $\mathfrak{b}$ be a label of a node, and $\mathfrak{p}$ a prime ideal with $\mathfrak{p} \supseteq \mathfrak{b}$. Again by SPT either $\mathfrak{b}$ is prime, in which case $\mathfrak{b}$ labels a leaf and thus $\mathfrak{p}_i = \mathfrak{b}$ for some i, or else the node labelled by $\mathfrak{b}$ has two childs labelled by $\mathfrak{b} + \langle r \rangle$ and $\mathfrak{b} + \langle s \rangle$ where $rs \in \mathfrak{b}$ but $r, s \notin \mathfrak{b}$. In the latter case $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$; whence $\mathfrak{p} \supseteq \mathfrak{b} + \langle r \rangle$ or $\mathfrak{p} \supseteq \mathfrak{b} + \langle s \rangle$. This allows us to climb the tree. □

A particular case of the finite-depth property was sufficient: that is, every strictly decreasing binary tree is finite. This has ensured the termination of the algorithm contained in the proof. As a by–product one gets a constructive proof of the following:

Corollary 5.1. If A is $\mathcal{FD}$-Noetherian, and we have SPT for A, then

$$\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$$

for every $\mathfrak{a} \in \mathfrak{I}_A$ where the $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are to $\mathfrak{a}$ as in MPP.

To see the crucial part $\supseteq$ of $\sqrt{\mathfrak{a}} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_k$ it suffices to observe that

$$\sqrt{\mathfrak{b} + \langle r \rangle} \cap \sqrt{\mathfrak{b} + \langle s \rangle} \subseteq \sqrt{\mathfrak{b}}$$

whenever $\mathfrak{b}$ is a label of a node with two childs labelled by $\mathfrak{b} + \langle r \rangle$ and $\mathfrak{b} + \langle s \rangle$.

With an appropriate strong primarity test in place of SPT, and an otherwise analogous termination proof, also the primary decomposition à la Lasker–Noether can be accomplished in any $\mathcal{FD}$-Noetherian ring. To verify this along the lines of (Perdry 2004) is left to the reader. Last but not least, proofs as the ones of Proposition 5.1 and Corollary 5.1

above have, among other things, inspired a technique of proof by induction for not necessarily Noetherian rings (Schuster 2012); see also (Hendtlass and Schuster 2012). This technique is based upon Open Induction (Raoult 1988), a specific form of which (Berger 2004; Coquand 1992) has been used in one of the other constructive proofs (Coquand and Persson 1999) of the Hilbert basis theorem mentioned before.

Acknowledgements Henri Lombardi and Alban Quadrat enabled the two authors of this paper to get together, in Besançon and at the *Mathematisches Forschungsinstitut Oberwolfach*, to finish the present work. The final version was produced within a project funded by the *Centre de Coopération Universitaire Franco-Bavarois* alias *Bayerisch-Französisches Hochschulzentrum* when the second author was working at the Mathematisches Institut der Universität München.

References

Adams, W. W. and Loustaunau, P. (1994). *An Introduction to Gröbner Bases*, vol. 3 of *Grad. Stud. Math.*. Providence, R.I.: American Mathematical Society.

Berger, U. (2004) A computational interpretation of open induction. In F. Titsworth (Ed.), *Proceedings of the Nineteenth Annual IEEE Symposium on Logic in Computer Science.* IEEE Computer Society Publications, 326–334.

Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. Dissertation, Universitt Innsbruck, 1965.

Coquand, T. (1992). Constructive topology and combinatorics. *Constructivity in Computer Science.* Proceedings, San Antonio, TX, 1991. Berlin and Heidelberg: Springer, vol. 613 of *Lecture Notes in Computer Science*, 159–164.

Coquand, T. and Persson, H. (1999). Gröbner bases in type theory. In T. Altenkirch et al. (Eds.), *Types for proofs and programs.* Proceedings, TYPES, Irsee, 1998. Berlin and Heidelberg: Springer, vol. 1657 of *Lecture Notes in Computer Science*, 33–46.

Coquand, T. and Lombardi, H. (2006). A logical approach to abstract algebra. *Math. Struct. in Comput. Science*, *16*, 885–900.

Edwards, H. M. (2005). *Essays in Constructive Mathematics*. New York: Springer.

Glaz, S. (1989). *Commutative Coherent Rings*. Berlin and New York: Springer.

Hadj Kacem, A. and Yengui, I. (2010). Dynamical Gröbner bases over Dedekind rings. *J. Alg.* , *324*, 12–24.

Hendtlass, M. and Schuster, P. (2012). A direct proof of Wiener's theorem. In S.B. Cooper et al. (Eds.), *How the World Computes.* Turing Centenary Conference and Eighth Conference on Computability in Europe. Proceedings, CiE 2012, Cambridge, UK, June 2012. Berlin and Heidelberg: Springer, vol. 7318 of *Lecture Notes in Computer Science*, 294–303.

Jacobsson, C. and Löfwall, C. (1991). Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem. *J. Symb. Comput.*, *12*(3), 337–372.

Kaplansky, I. (1974). *Commutative Rings.*. Chicago and London: The University of Chicago Press. Revised edition.

Lombardi, H. and Perdry, H. (1998). The Buchberger algorithm as a tool for ideal theory of polynomial rings in constructive mathematics. In B. Buchberger and F. Winkler (Eds.), *Gröbner Bases and Applications*. vol. 251 of *London Math. Soc. Lecture Notes Ser.*, 393–407.

Lombardi, H. and Quitté, C. (2011). *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini*. Paris: Calvage et Mounet. English version forthcoming at Springer. Preliminary version available at the home page of H. Lombardi.

Lombardi, H., Yengui, I., and Schuster, P. (2012). The Gröbner ring conjecture in one variable. *Math. Z.*, *270*, 1181–1185.

Mines, R., Richman, F., and Ruitenburg, W. (1988). *A Course in Constructive Algebra*. New York: Springer. Universitext.

Perdry, H. (2004). Strongly Noetherian rings and constructive ideal theory. *J. Symb. Comput.*, *37*(4), 511–535.

Perdry, H. (2008). Lazy bases: a minimalist constructive theory of Noetherian rings. *Math. Log. Quart.*, *54*(1), 70–82.

Perdry, H. and Schuster, P. (2011). Noetherian orders. *Math. Structures Comput. Sci.*, *21*, 111–124.

Raoult, J.-C. (1988) Proving open properties by induction. *Inform. Process. Lett.*, *29*, 19–23.

Richman, F. (1974). Constructive aspects of Noetherian rings. *Proc. Amer. Math. Soc.*, *44*, 436–441.

Richman, F. (2003). The ascending tree condition: constructive algebra without countable choice. *Comm. Algebra*, *31*, 1993–2002.

Schuster, P. (2012). Induction in algebra: a first case study. In *2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science.* Proceedings, LICS 2012, Dubrovnik, Croatia, June 2012. IEEE Computer Society Publications, 581–585

Schuster, P. and Zappe, J. (2006). Do Noetherian rings have Noetherian basis functions? In A. Beckmann et al. (Eds.), *Logical Approaches to Computational Barriers.* Second Conference on Computability in Europe. Proceedings, CiE 2006, Swansea, UK, July 2006. Berlin and Heidelberg: Springer, vol. 3988 of *Lecture Notes in Computer Science*, 481–489.

Seidenberg, A. (1974). What is Noetherian? *Rend. Sem. Mat. Fis. Milano*, *44*, 55–61.

Tennenbaum, J. (1973). *A Constructive Version of Hilbert's Basis Theorem*. Ph.D. thesis, University of California San Diego.

Yengui, I. (2006). Dynamical Gröbner bases. *J. Alg.* , *301*, 447–458.

Zariski, O. and Samuel, P. (1958). *Commutative Algebra.*. Van Nostrand, Princeton, N.J. Vol. I.