REDUCTION MOD P OF STANDARD BASES

Matthias Aschenbrenner

Department of Mathematics, Statistics,
and Computer Science
University of Illinois at Chicago
851 S. Morgan St. (M/C 249)
Chicago, IL 60607, U.S.A.
maschenb@math.uic.edu.

To Volker Weispfenning, on his 60th birthday.

Abstract

We investigate the behavior of standard bases (in the sense of Hironaka and Grauert) for ideals in rings of formal power series over commutative rings with respect to specializations of the coefficients. For instance, we show that any ideal I of the ring of formal power series $A[[X]] = A[[X_1, \dots, X_N]]$ with coefficients in a Noetherian ring A admits a standard basis whose image under every specialization of A onto a field is a standard basis of the image of I. Applications include a modular criterion for ideal membership in $\mathbb{Z}[[X]]$ and a constructibility result for ideal membership in $K[[X]]$, where K is a field.

Partially supported by National Science Foundation grant DMS 03-03618.
Keywords: Standard bases, power series, ideal membership, constructibility
2000 Mathematics Subject Classification: Primary 13F25; Secondary 13P10

Let A be a commutative ring and let $N > 0$ be an integer. We denote by $A[[X]] = A[[X_1, \dots, X_N]]$ the ring of formal power series with coefficients from A, in the indeterminates $X = (X_1, \dots, X_N)$. Given a prime number p, we have a natural surjective ring homomorphism

$$f(X) \mapsto f(p; X) \colon \mathbb{Z}[[X]] \to \mathbb{F}_p[[X]],$$

where $f(p; X)$ (the reduction of $f(X)$ modulo p) is obtained by applying

$$a \mapsto a(p) := a + p\mathbb{Z} \colon \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

to the coefficients of f. If I is an ideal of $\mathbb{Z}[[X]]$, we write $I(p)$ for the ideal

$$I(p) := \big\{ f(p;X) : f(X) \in I \big\}$$

of $\mathbb{F}_p[[X]]$. It is a natural question, given a power series $f(X) \in \mathbb{Z}[[X]]$, whether membership of $f(p;X)$ in $I(p)$ for all primes p implies membership of $f(X)$ in I. A simple example shows that this is false in general: for every prime p, the element $2-T$ of $\mathbb{Z}[[T]]$ (where T is a single indeterminate) divides 2 modulo p, but the series $\frac{2}{2-T} = \sum_{n=0}^{\infty} \frac{1}{2^n} T^n$ is not an element of $\mathbb{Z}[[T]]$. However, recently Hans Schoutens made the following observation:

Theorem. *Given an ideal I of the ring $\mathbb{Z}[[X]]$, there exists a non-zero integer d with the following property: if $f(X)$ is an element of $\mathbb{Z}[[X]]$ such that $f(p;X) \in I(p)$ for all but finitely many primes p, then $f(X) \in I\mathbb{Z}[\frac{1}{d}][[X]]$.*

(Here $\mathbb{Z}[\frac{1}{d}] = \{a/d^e : a, e \in \mathbb{Z}\}$ denotes the localization of $\mathbb{Z}$ at its multiplicative subset $\{1, d, d^2, \dots\}$, and $I\mathbb{Z}[\frac{1}{d}][[X]]$ is the ideal generated by I in $\mathbb{Z}[\frac{1}{d}][[X]]$.)

The original proof of this fact by Schoutens (2001) used a uniform strong version of Artin Approximation with parameters for excellent Henselian local rings in mixed characteristic in combination with the Ax-Kochen-Ershov Principle. Later, Denef pointed out a simpler proof, also based on a version of Artin Approximation. Ideal membership being of a linear nature, the use of Artin Approximation in these arguments seems somewhat heavy-handed. In this note, we will give a rather elementary and in some sense more explicit proof of the theorem above.

Our argument will be based on the theory of *standard bases* for ideals in power series rings, introduced by Hironaka (1964) and Grauert (1972), and subsequently further extended by a number of authors: Becker (1990a,b, 1993), Briançon (1973), Galligo (1973, 1974). It is a (non-algorithmic) analog for power series of the theory of Gröbner bases (for polynomial ideals), initiated by Buchberger (1965, 1970). The theory of standard bases is usually developed for ideals in rings of (formal or convergent) power series with coefficients in a *field* K. (For convergent series ones takes $K = \mathbb{R}$ or $K = \mathbb{C}$.) Here we study a notion of standard basis for ideals in the ring $A[[X]]$ of formal power series with coefficients in a commutative ring A; see Section 2. (See Ribenboim (1993) for a generalization in a different direction.) Schoutens' theorem will be an immediate consequence of general statements about the behavior of standard bases under specialization. These general principles are also at the basis of some results proved in Bierstone and Milman (1987) and Parusiński and Szafraniec (1997); see Section 3.

Among other applications given in Section 3 is the following constructibility result. For this, let $C = (C_1, \dots, C_M)$ be a tuple of parametric variables, $M \geqslant 1$, and put $A = \mathbb{Z}[C]$. Given a power series $f(C,X) \in A[[X]]$ and an M-tuple c in a field K we denote by $f(c,X) \in K[[X]]$ the result of applying the homomorphism $\sigma_c \colon A \to K$ given by $C_i \mapsto c_i$ for $i = 1, \dots, M$ to the coefficients of $f(C,X)$. A constructible subset Σ of $\operatorname{Spec} A$ by definition is a (finite) Boolean combination of Zariski closed subsets of $\operatorname{Spec} A$. Given such Σ and an M-tuple c from a field K we write $\Sigma(K) := \{c \in K^M : \ker \sigma_c \in \Sigma\}$ (a Boolean combination of algebraic subsets of K^M).

Theorem. *Let $f_0(C,X),\dots,f_n(C,X) \in A[[X]] = A[[X_1,\dots,X_N]]$. There exists a constructible subset Σ of* Spec A *with the following property: for every field K and $c \in K^M$ we have $c \in \Sigma(K)$ if and only if*

$$f_0(c,X) \in \big(f_1(c,X),\dots,f_n(c,X)\big)K[[X]].$$

This fact can also be proved using the Weierstraß Division Theorem. In Aschenbrenner (2001), Chapter 5, we obtained an analog for p-adic restricted power series in this way. It is well-known that the theorem remains true if we replace $A[[X]]$ and $K[[X]]$ by $A[X]$ and $K[X]$, respectively. This can alternatively be seen as a consequence of classical results by Hermann (1926), or of the existence of uniform bounds for Gröbner bases in polynomial rings over fields constructed by Möller and Mora (1984) and Dubé (1990). The existence of such bounds may be established using elegant non-standard methods, see Robinson (1973), Dries and Schmidt (1984), Weispfenning (1988). (This approach, however, doesn't seem to adapt to formal power series, to yield another proof of the theorem above.)

1 Preliminaries

We collect terminology and preliminary remarks concerning orderings and formal power series, which will be useful later. Throughout this paper, we let N be a positive integer.

Orderings

An **ordered set** is a pair $(S,\leqslant)$, consisting of a set S and an **ordering** on S, that is, a binary relation $\leqslant$ on S which is reflexive, transitive and antisymmetric. (If $\leqslant$ is clear from the context, we also just say that S is an ordered set.) If x and y are elements of an ordered set $(S,\leqslant)$, we write as usual $x \leqslant y$ also as $y \geqslant x$, and we write $x < y$ if $x \leqslant y$ and $y \not\leqslant x$. If $x \in S$ has the property that $y \leqslant x \Rightarrow x = y$ for all $y \in S$, then x is called a **minimal** element of S. If $x \leqslant y$ for all $y \in S$, then x is called the **smallest** element of S. If $x \leqslant y$ or $y \leqslant x$ for all $x, y \in S$, then the ordering $\leqslant$ on S is called **total.** An ordering $\preceq$ on a set S is said to **extend** the ordering $\leqslant$ on S if $x \leqslant y \Rightarrow x \preceq y$ for all $x, y \in S$.

The cartesian product $S \times T$ of two ordered sets $(S,\leqslant_S)$ and $(T,\leqslant_T)$ can be made into an ordered set by means of the **product ordering**

$$(x,y) \sqsubseteq (x',y') \qquad :\Longleftrightarrow \qquad x \leqslant_S x' \text{ and } y \leqslant_T y',$$

or the **lexicographic ordering**

$$(x,y) \leqslant_{\text{lex}} (x',y') \qquad :\Longleftrightarrow \qquad x <_S x', \text{ or } x = x' \text{ and } y \leqslant_T y'.$$

Iterating this construction yields the product ordering $\sqsubseteq$ and the lexicographic ordering $\leqslant_{\text{lex}}$ on S^N.

Final segments and antichains

A **final segment** of an ordered set $(S, \leqslant)$ is a subset $F \subseteq S$ which is closed upwards: $x \leqslant y \wedge x \in F \Rightarrow y \in F$, for all $x, y \in S$. We construe the set $\mathcal{F}(S) = \mathcal{F}(S, \leqslant)$ of final segments of S as an ordered set, with the ordering given by *reverse* inclusion. Given a subset M of S, we denote by

$$\langle M \rangle := \big\{ y \in S : \exists x \in M \ (x \leqslant y) \big\}$$

the final segment **generated by** M**.** An **antichain** of S is a subset $A \subseteq S$ such that any two distinct elements x and y of A are incomparable: $x \not\leqslant y$ and $y \not\leqslant x$.

Well-founded orderings

An ordered set S is **well-founded** if there is no infinite strictly decreasing sequence $x_0 > x_1 > \cdots$ in S. (As usual, a totally ordered set S which is well-founded is called well-ordered.) If S is well-founded, then every final segment F of S has a smallest set of generators (the antichain of minimal elements of F). In a well-founded ordered set, we can argue by **Noetherian induction:** if $\mathcal{P}$ is a non-empty subset of S with the property that $y \in \mathcal{P}$ for all $y < x$ implies $x \in \mathcal{P}$, for every $x \in S$, then $\mathcal{P} = S$.

Noetherian orderings

We say that an ordered set S is **Noetherian** if it is well-founded and every antichain of S is finite. We have the following familiar characterization of Noetherian orderings (whose proof we leave to the reader).

Proposition 1.1. *The following are equivalent, for an ordered set* $(S, \leqslant)$*:*

(1) *S is Noetherian.*

(2) *Every infinite sequence $x_0, x_1, \ldots$ in S contains an increasing subsequence.*

(3) *Any final segment of S is finitely generated.*

(4) $\big(\mathcal{F}(S), \supseteq\big)$ *is well-founded (i.e., the ascending chain condition holds for final segments of S).*

(5) *Every total ordering on S which extends $\leqslant$ is a well-ordering.* □

The proposition immediately implies that if S and T are Noetherian ordered sets, then their cartesian product $S \times T$ is also Noetherian under the product ordering. We consider $\mathbb{N} = \{0, 1, 2, \ldots\}$ as an ordered set with its usual ordering, and we equip $\mathbb{N}^N$ with the product ordering $\sqsubseteq$.

Corollary 1.2. (Dickson's Lemma.) *The ordered set* $(\mathbb{N}^N, \sqsubseteq)$ *is Noetherian.* □

The following facts will be useful later.

Lemma 1.3. *Let $(S, \leqslant_S)$ be a Noetherian ordered set and $(T, \leqslant_T)$ be a well-founded ordered set, and let $\varphi\colon S \to T$ be* order-reversing, *i.e., $x \leqslant_S y \Rightarrow \varphi(x) \geqslant_T \varphi(y)$, for all $x, y \in S$. Then the set $M = \big\{\big(x, \varphi(x)\big) : x \in S\big\}$, ordered by*

$$\big(x, \varphi(x)\big) \leqslant \big(y, \varphi(y)\big) \quad \Longleftrightarrow \quad x \leqslant_S y \text{ and } \varphi(x) = \varphi(y)$$

is Noetherian.

Proof. We will show that (2) in Proposition 1.1 holds for M. Let

$$\big(x_0, \varphi(x_0)\big), \big(x_1, \varphi(x_1)\big), \ldots$$

be an infinite sequence in M. After passing to a subsequence if necessary, we may assume that $x_0 \leqslant_S x_1 \leqslant_S \cdots$ (since S is Noetherian). Therefore $\varphi(x_0) \geqslant_T \varphi(x_1) \geqslant_T \cdots$ and hence $\varphi(x_n) = \varphi(x_{n+1}) = \cdots$ for some n (since T is well-founded). So $\big(x_n, \varphi(x_n)\big) \leqslant \big(x_{n+1}, \varphi(x_{n+1})\big) \leqslant \cdots$ is an increasing subsequence as desired. □

Let $(S, \leqslant)$ be an ordered set. The set $\mathrm{O}(S, \leqslant)$ of all orderings on S which extend $\leqslant$ can be turned into a topological space by taking as a sub-basis of open sets all sets of the form

$$U(x, y) = \big\{\leqslant' : \leqslant' \text{ is an ordering on } S \text{ extending } \leqslant, \text{ and } x <' y\big\},$$

where (x, y) ranges over all ordered pairs of elements of S. It is an easy exercise to deduce from the Compactness Theorem of first-order logic that $\mathrm{O}(S, \leqslant)$ is compact. The set of total orderings $\mathrm{TO}(S, \leqslant)$ which extend $\leqslant$ form a closed subset of $\mathrm{O}(S, \leqslant)$. The following generalizes Becker (1990a), Lemma 2.1:

Lemma 1.4. *Let $(S, \leqslant)$ be a Noetherian ordered set, let $\leqslant'$ be a total ordering extending $\leqslant$, and let $S_1, \ldots, S_m$ be non-empty subsets of S. There exists a neighborhood U of $\leqslant'$ in $\mathrm{TO}(S, \leqslant)$ such that $\min_{\leqslant'}(S_i) = \min_{\leqslant''}(S_i)$ for all $\leqslant''$ in U and $i = 1, \ldots, m$.*

Proof. It suffices to consider the case $i = 1$. By Proposition 1.1, (3) there exist $s_1, \ldots, s_n \in S_1$ such that for every $s \in S_1$, we have $s_i \leqslant s$ for some i. In particular, we have $\min_{\leqslant'}(S_1) = s_k$ for some k. It is easy to see that the intersection U of the open set $\bigcap_{s_i <' s_j} U(s_i, s_j)$ with $\mathrm{TO}(S, \leqslant)$ does the job. □

Semigroup orderings

A **semigroup ordering** on $\mathbb{N}^N$ is a total ordering $\leqslant$ on $\mathbb{N}^N$ which satisfies

$$\nu \leqslant \mu \quad \Rightarrow \quad \nu + \lambda \leqslant \mu + \lambda \qquad \text{for all } \lambda, \mu, \nu \in \mathbb{N}^N.$$

An **admissible ordering** on $\mathbb{N}^N$ is a semigroup ordering such that $0 \in \mathbb{N}^N$ is the smallest element of $\mathbb{N}^N$. Any admissible ordering extends the product ordering $\sqsubseteq$ on $\mathbb{N}^N$, and hence is a well-ordering, by Corollary 1.2 and Proposition 1.1, (5). The set AO_N of admissible orderings on $\mathbb{N}^N$ is a closed subset of $\mathrm{TO}(\mathbb{N}^N, \sqsubseteq)$.

Example. An example for an admissible ordering is the lexicographic ordering on $\mathbb{N}^N$. Another example (isomorphic to $\mathbb{N}$) is the **degree lexicographic ordering**: For $\nu = (\nu_1, \ldots, \nu_N) \in \mathbb{N}^N$, put $|\nu| = \nu_1 + \cdots + \nu_N$ (the degree of ν), and define

$$\nu \leqslant \mu \quad :\Longleftrightarrow \quad \big(|\nu|, \nu_1, \ldots, \nu_N\big) \leqslant_{\text{lex}} \big(|\mu|, \mu_1, \ldots, \mu_N\big)$$

for $\nu, \mu \in \mathbb{N}^N$. This is an example of a **degree-compatible** ordering on $\mathbb{N}^N$, that is, an ordering $\leqslant$ on $\mathbb{N}^N$ such that $|\nu| < |\mu| \Rightarrow \nu < \mu$ for all $\nu, \mu \in \mathbb{N}^N$.

Every degree-compatible admissible ordering on $\mathbb{N}^N$ has order type ω. We refer to Becker (1990a), Section 3 for a proof of the following:

Lemma 1.5. *The admissible orderings of order type ω are dense in* AO_N. □

For the rest of this paper, unless noted otherwise, we fix an admissible ordering $\leqslant$ on $\mathbb{N}^N$. Let λ be the order type of the well-ordering $\leqslant$ (a limit ordinal), and $\{\nu_\alpha\}_{\alpha<\lambda}$ the enumeration of $\mathbb{N}^N$ in increasing order indexed by all ordinal numbers less than λ. We may relate the elements of $\mathbb{N}^N$ with *power products* of indeterminates $X = (X_1, \ldots, X_N)$: Let $X^* = \{X^\nu : \nu \in \mathbb{N}^N\}$ be the free commutative monoid generated by $X_1, \ldots, X_N$, where $X^\nu := X_1^{\nu_1} \cdots X_N^{\nu_N}$ for $\nu = (\nu_1, \ldots, \nu_N) \in \mathbb{N}^N$, ordered by divisibility:

$$X^\nu | X^\mu \quad :\Longleftrightarrow \quad X^\mu = X^\nu \cdot X^\lambda \text{ for some } \lambda \in \mathbb{N}^N.$$

Then $v\colon X^\nu \mapsto \nu, X^* \to \mathbb{N}^N$ is an isomorphism of monoids, and an isomorphism of ordered sets (i.e., bijective and order-preserving).

Formal power series

Let A be a ring. (Throughout this paper, "ring" stands for "commutative ring with unit $1 \neq 0$.") We let $A[[X]] = A[[X_1, \ldots, X_N]]$ denote the ring of formal power series in indeterminates $X = (X_1, \ldots, X_N)$ with coefficients in A. If A is an integral domain, then so is $A[[X]]$. We may write an element $f(X)$ of $A[[X]]$ alternatively as

$$f(X) = \sum_{\nu \in \mathbb{N}^N} f_\nu X^\nu, \tag{1.1}$$

where $f_\nu \in A$ for $\nu \in \mathbb{N}^N$, or in the form

$$f(X) = \sum_{\alpha<\lambda} f_\alpha X^{\nu_\alpha},$$

where $f_\alpha = f_{\nu_\alpha}$. We put

$$\mathrm{mono}(f) := \big\{f_\nu X^\nu : \nu \in \mathbb{N}^N\big\} \subseteq A \cdot X^*,$$

the set of **monomials** of f, and we let

$$\mathrm{supp}(f) := \big\{\nu \in \mathbb{N}^N : f_\nu \neq 0\big\} \subseteq \mathbb{N}^N$$

denote the **support** of f. If $f \neq 0$, then $\operatorname{supp} f$ has a smallest element $v(f)$ with respect to $\leqslant$, which we call the **leading exponent** of f. We have

$$v(f+g) \geqslant \min\{v(f), v(g)\}, \quad v(fg) \geqslant v(f) + v(g), \qquad \text{for all } f, g \in A[[X]],$$

where we put $v(0) := \infty > \mathbb{N}^N$. We have $v(f+g) = \min\{v(f), v(g)\}$ if $v(f) \neq v(g)$, and $v(fg) = v(f) + v(g)$ if A is an integral domain. For $f \in A[[X]]$, $f \neq 0$, we call

$$\operatorname{lc}(f) = f_{v(f)} \in A \setminus \{0\}, \quad \operatorname{lt}(f) = X^{v(f)} \in X^*, \quad \operatorname{lm}(f) = \operatorname{lc}(f) \operatorname{lt}(f)$$

the **leading coefficient**, **leading term,** and **leading monomial**, respectively, of the power series f.

The leading monomial ideal

Given a subset S of $A[[X]]$ we let $\operatorname{lm}(S)$ denote the ideal of the polynomial ring $A[X]$ generated by the leading monomials $\operatorname{lm}(f)$, where f ranges over the non-zero elements of S. By

$$v(S) = \{\nu \in \mathbb{N}^N : \nu \sqsupseteq v(f) \text{ for some } 0 \neq f \in S\},$$

we denote the final segment of $\mathbb{N}^N$ generated by the $v(f)$, $0 \neq f \in S$. (By Corollary 1.2 and Proposition 1.1, (3), there always exists a finite set G of non-zero elements of S such that $v(S) = v(G)$.) For $\nu \in \mathbb{N}^N$, $\operatorname{lc}(S, \nu)$ denotes the ideal of A generated by all $\operatorname{lc}(f)$, where f ranges over the non-zero elements of S with $v(f) \sqsubseteq \nu$. We call $\operatorname{lm}(S)$ the **leading monomial ideal** of S, $v(S)$ the **diagram of leading exponents** of S, and $\operatorname{lc}(S, \nu)$ the **leading coefficient ideal** of S of degree ν. Clearly $\operatorname{lc}(S, \nu) \neq \{0\}$ if and only if $\nu \in v(S)$. If $a \in \operatorname{lc}(S, \nu)$, $b \in \operatorname{lc}(S, \mu)$, then $ab \in \operatorname{lc}(S, \nu + \mu)$, and if $\nu \sqsubseteq \mu$, then $\operatorname{lc}(S, \nu) \subseteq \operatorname{lc}(S, \mu)$. We have a direct sum decomposition

$$\operatorname{lm}(S) = \bigoplus_{\nu \in \mathbb{N}^N} \operatorname{lc}(S, \nu) X^\nu$$

as A-modules, making $\operatorname{lm}(S)$ into an $\mathbb{N}^N$-graded A-algebra. If I is an ideal of $A[[X]]$, we have

$$\begin{aligned} \operatorname{lm}(I) &= \{\operatorname{lm}(f) : 0 \neq f \in I\} \cup \{0\}, \\ v(I) &= \{v(f) : 0 \neq f \in I\}, \\ \operatorname{lc}(I, \nu) &= \{\operatorname{lc}(f) : 0 \neq f \in I, v(f) = \nu\} \cup \{0\}, \end{aligned}$$

for all $\nu \in \mathbb{N}^N$.

2 Hironaka Division and Standard Bases

In this section we first prove a version of the Hironaka Division Theorem, which allows the simultaneous division with remainder of a power series by several (finitely many) other

power series. We then define standard bases of ideals in power series rings and give some criteria for a finite collection of power series to form a standard basis. Here we work in a somewhat greater generality than is actually needed for the proof of the theorems stated in the introduction. We expect this extra generality to be useful in applications, as is the case with the notion of Gröbner basis for ideals of polynomial rings over arbitrary Noetherian *rings*, rather than just fields (see Gianni et al. (1988)). In the last part of the section we isolate the class of *monic* ideals. Here a more precise version of the Hironaka Division Theorem holds. Standard bases of monic ideals also have good specialization properties, as we show in Section 3. Our arguments are adaptations of Becker (1990a,b, 1993). We finish with some remarks on standard bases of ideals generated by polynomials.

Hironaka division

The notations and conventions introduced in Section 1 remain in force. Let $G = \{g_1, \ldots, g_m\}$ be a finite set of non-zero elements of the ring $A[[X]] = A[[X_1, \ldots, X_N]]$ of formal power series with coefficients in the ring A. We can divide any $f \in A[[X]]$ by $g_1, \ldots, g_m$ with remainder, in the following sense:

Theorem 2.1. *For every $f \in A[[X]]$ there exist elements $q_1, \ldots, q_m, r \in A[[X]]$ satisfying the following properties:*

(1) $f = q_1 g_1 + \cdots + q_m g_m + r$,

(2) $\mathrm{mono}(r) \cap \mathrm{lm}(G) = \{0\}$, *and*

(3) $v(f) \leqslant v(q_i g_i)$ *for each* $i = 1, \ldots, m$.

In the proof of the theorem, we use the following notation: if $\nu \in \mathbb{N}^N$ and $g \in A[[X]]$ are such that $\mathrm{supp}(g) \subseteq \langle \nu \rangle$ (that is, if $X^\nu | X^\mu$ for every $\mu \in \mathrm{supp}(g)$), then there exists a unique $h \in A[[X]]$ with $g = h \cdot X^\nu$, and we write $h = g/X^\nu$.

Proof. We define, by induction on $\alpha < \lambda$, sequences $\{b_{i,\alpha}\}_{\alpha<\lambda}$ (for $i = 1, \ldots, m$) of elements of A with the following properties:

(a) $v(g_i) \not\sqsubseteq \nu_\alpha \Rightarrow b_{i,\alpha} = 0$, and

(b) $v(f) > \nu_\alpha \Rightarrow b_{i,\alpha} = 0$,

for all $\alpha < \lambda$ and all i. Let $\alpha < \lambda$, and suppose that $b_{i,\beta}$ have already been defined, for $\beta < \alpha$ and $i = 1, \ldots, m$. Let $b_i^\alpha := \sum_{\beta<\alpha} b_{i,\beta} X^{\nu_\beta}$. By (a), we then have $q_i^\alpha := b_i^\alpha / \mathrm{lt}(g_i) \in A[[X]]$ for $i = 1, \ldots, m$, and we let

$$r^\alpha := f - (q_1^\alpha g_1 + \cdots + q_m^\alpha g_m).$$

Write $r^\alpha = \sum_{\gamma<\lambda} r_\gamma^\alpha X^{\nu_\gamma}$ with $r_\gamma^\alpha \in A$. We distinguish two cases: If $r_\alpha^\alpha X^{\nu_\alpha} \notin \mathrm{lm}(G)$, then we set $b_{i,\alpha} := 0$ for $i = 1, \ldots, m$. If $r_\alpha^\alpha X^{\nu_\alpha} \in \mathrm{lm}(G)$, we can write

$$r_\alpha^\alpha X^{\nu_\alpha} = a_1 X^{\nu_1} \mathrm{lm}(g_1) + \cdots + a_m X^{\nu_m} \mathrm{lm}(g_m)$$

for certain $a_1, \dots, a_m \in A$ and $\nu_1, \dots, \nu_m \in \mathbb{N}^N$, chosen such that $\nu_i + v(g_i) = \nu_\alpha$ if $a_i \neq 0$. We then set $b_{i,\alpha} := a_i$ for all i. Clearly property (a) continues to hold, for all i. For (b), suppose that $v(f) > \nu_\alpha$. Then by induction hypothesis $b_{i,\beta} = 0$ for all $\beta < \alpha$ and all i, hence $r^\alpha = f$ and so $r^\alpha_\alpha = f_\alpha = 0$. Therefore $b_{i,\alpha} = 0$, which shows that (b) holds as well, for all i. Now put

$$b_i := \sum_{\alpha<\lambda} b_{i,\alpha} X^{\nu_\alpha}, \quad q_i := b_i / \operatorname{lt}(g_i) \in A[[X]] \qquad \text{for } i = 1, \dots, m.$$

We claim that $q_1, \dots, q_m$ and $r := f - (q_1 g_1 + \cdots + q_m g_m)$ satisfy the requirements of the theorem. Part (1) is clear, and (3) holds by (b). Let $\alpha < \lambda$, and write

$$r = r^\alpha - \big(b_{1,\alpha} X^{\nu_\alpha} / \operatorname{lt}(g_1) \cdot g_1 + \cdots + b_{m,\alpha} X^{\nu_\alpha} / \operatorname{lt}(g_m) \cdot g_m\big) - h$$

where $h = \sum_{i=1}^m \sum_{\alpha<\beta<\lambda} b_{i,\beta} X^{\nu_\beta} / \operatorname{lt}(g_i) \cdot g_i$, so $\operatorname{supp}(h) > \nu_\alpha$. If $r^\alpha_\alpha X^{\nu_\alpha} \notin \operatorname{lm}(G)$, then $b_{i,\alpha} = 0$ for all i, so $r_\alpha X^{\nu_\alpha} = r^\alpha_\alpha X^{\nu_\alpha} \notin \operatorname{lm}(G)$. Otherwise, by definition of $b_{i,\alpha}$ we have

$$r^\alpha_\alpha X^{\nu_\alpha} - \big(b_{1,\alpha} X^{\nu_\alpha} / \operatorname{lt}(g_1) \cdot \operatorname{lm}(g_1) + \cdots + b_{m,\alpha} X^{\nu_\alpha} / \operatorname{lt}(g_m) \cdot \operatorname{lm}(g_m)\big) = 0.$$

It follows that $r_\alpha = 0$, hence $r_\alpha X^{\nu_\alpha} = 0$. This shows that $\operatorname{mono}(r) \cap \operatorname{lm}(G) = \{0\}$ as desired. □

Given $f \in A[[X]]$, we call any element $r \in A[[X]]$ for which there exist power series $q_1, \dots, q_m \in A[[X]]$ such that (1)–(3) in the theorem hold, a **remainder of f modulo G.** If $r = 0$ is a remainder of f modulo G, then we say that f **has a standard representation** in terms of G. In this case, we call any expression of f as linear combination $f = q_1 g_1 + \cdots + q_m g_m$ of $g_1, \dots, g_m$, with $q_1, \dots, q_m \in A[[X]]$ such that $v(f) \leqslant v(q_i g_i)$ for all i, a **standard representation of f** in terms of G.

Example. Let $A = \mathbb{Z}$ and $g = 2T + 2$, where T is a single indeterminate. The leading monomial ideal of $G = \{g\}$ is $2\mathbb{Z}[T]$, and every series of the form $(2k + 1)(T + 1)$, where $k \in \mathbb{Z}$, is a remainder of $f = T + 1$ modulo G.

Standard bases

Let now $g_1, \dots, g_m \in A[[X]]$ be non-zero power series and let I be an ideal of $A[[X]]$ containing $G = \{g_1, \dots, g_m\}$.

Theorem 2.2. *The following are equivalent:*

(1) $\operatorname{lm}(I) = \operatorname{lm}(G)$.

(2) $\operatorname{lc}(I, \nu) = \operatorname{lc}(G, \nu)$ *for all* ν.

(3) *Every* $f \in I$ *has* unique *remainder* 0 *modulo* G.

(4) *Every* $f \in I$ *has remainder* 0 *modulo* G (*i.e., f has a standard representation in terms of G*).

Proof. The equivalence of (1) and (2) is clear. Suppose that $\mathrm{lm}(I) = \mathrm{lm}(G)$. By Theorem 2.1, for every series $f \in A[[X]]$ there exist $q_1, \ldots, q_m \in A[[X]]$ such that $\mathrm{mono}(r) \cap \mathrm{lm}(I) = \{0\}$, where $r := f - (q_1 g_1 + \cdots + q_m g_m)$. Moreover, if $f \in I$, then $r \in I$, hence $r = 0$. This shows (3). The implication (3) $\Rightarrow$ (4) being trivial, we now show (4) $\Rightarrow$ (1): Let $0 \neq f = q_1 g_1 + \cdots + q_m g_m$ with $q_1, \ldots, q_m \in A[[X]]$ and $v(f) \leqslant v(q_i g_i)$ for all i. After rearranging the g_i (and the q_i accordingly) we may assume that

$$v(f) = v(q_1 g_1) = \cdots = v(q_l g_l) < v(q_{l+1} g_{l+1}), \ldots, v(q_m g_m)$$

for some $l \in \{1, \ldots, m\}$. Then

$$\mathrm{lm}(f) = \mathrm{lm}(q_1)\,\mathrm{lm}(g_1) + \cdots + \mathrm{lm}(q_l)\,\mathrm{lm}(g_l) \in \mathrm{lm}(G).$$

This shows that $\mathrm{lm}(I) = \mathrm{lm}(G)$ as required. □

We say that G is a **standard basis** for I if one of the equivalent conditions of the theorem is satisfied. Note that in this case, G generates I (by (4) in Theorem 2.2). We call G a **standard basis** if it is a standard basis for the ideal in $A[[X]]$ which it generates. We observe:

Lemma 2.3. *If A is Noetherian, then every ideal I of $A[[X]]$ has a standard basis.*

Proof. Apply Lemma 1.3 to $S = \mathbb{N}^N$, ordered by $\sqsubseteq$, and $T =$ the set of all ideals of A, ordered by reverse inclusion, and φ given by $\varphi(\nu) = \mathrm{lc}(I, \nu)$. By this lemma and Proposition 1.1, (3), there exist $\nu_1, \ldots, \nu_n \in v(I)$ such that for every $\nu \in v(I)$ we have $\nu_j \sqsubseteq \nu$ and $\mathrm{lc}(I, \nu_j) = \mathrm{lc}(I, \nu)$ for some j. Since A is Noetherian, we can choose $G = \{g_1, \ldots, g_m\} \subseteq I \setminus \{0\}$ such that $\mathrm{lc}(G, \nu_j) = \mathrm{lc}(I, \nu_j)$ for all j. Hence $\mathrm{lc}(G, \nu) = \mathrm{lc}(I, \nu)$ for all ν, so G is a standard basis for the ideal I. □

Remark. By Hilbert's Basis Theorem, if A is Noetherian, then so is $A[X]$. Hence the ideal $\mathrm{lm}(I)$ of $A[X]$ is finitely generated. Therefore there exists a finite subset $G = \{g_1, \ldots, g_m\}$ of non-zero elements of I such that $\mathrm{lm}(G) = \mathrm{lm}(I)$, i.e., G is a standard basis for I. This yields another proof of the previous lemma. (The proof given above avoids invoking Hilbert's Basis Theorem.)

Corollary 2.4. *Suppose that A is Noetherian. Let I be an ideal of $A[[X]]$ and $f = \sum_\nu f_\nu X^\nu \in A[[X]]$. If $f_\nu \in I \cap A$ for all ν, then $f \in I$.*

Proof. Let $G = \{g_1, \ldots, g_m\}$ be a standard basis for I. Dividing f by $g_1, \ldots, g_m$ as in Theorem 2.2, we can write

$$f = q_1 g_1 + \cdots + q_m g_m + r$$

with $q_1, \ldots, q_m, r \in A[[X]]$ such that $\mathrm{mono}(r) \cap \mathrm{lm}(I) = \{0\}$. Since $I \cap A \subseteq \mathrm{lc}(I, \nu)$ for all ν, it follows that $r_\nu \in \mathrm{lc}(I, \nu)$ for all ν. Hence $r = 0$, i.e., $f \in I$. □

S-series

We say that power series $S_1, \dots, S_k \in A[[X]]$ are **S-series** of $g_1, \dots, g_m$ if they have the form

$$S_i = \sum_{j=1}^{m} y_j^{(i)} \frac{X^\mu}{\operatorname{lt}(g_j)} g_j \qquad \text{for } i = 1, \dots, k,$$

where $X^\mu = \operatorname{lcm}\big(\operatorname{lt}(g_1), \dots, \operatorname{lt}(g_m)\big)$ and $y^{(i)} = \big(y_1^{(i)}, \dots, y_m^{(i)}\big)$, $i = 1, \dots, k$, form a finite set of generators for the module of solutions in A^m to the homogeneous linear equation

$$y_1 \operatorname{lc}(g_1) + \cdots + y_m \operatorname{lc}(g_m) = 0.$$

Note that $v(S_i) > \mu$ for every i. If A is Noetherian, then every submodule of A^m is finitely generated; hence for any $g_1, \dots, g_m \in A[[X]]$ there exist S-series of $g_1, \dots, g_m$.

Example 2.5. Suppose that some $\operatorname{lc}(g_i)$ is a unit of A. The series given by

$$S_{ij} = \operatorname{lc}(g_j) \frac{X^\mu}{\operatorname{lt}(g_i)} g_i - \operatorname{lc}(g_i) \frac{X^\mu}{\operatorname{lt}(g_j)} g_j,$$

for $1 \leqslant i < j \leqslant m$, are S-series of $g_1, \dots, g_m$.

We say that $G = \{g_1, \dots, g_m\}$ is **closed under S-series** if there exist S-series $S_1, \dots, S_k$ of $g_1, \dots, g_m$ each of which has a standard representation with respect to G. If G is closed under S-series, a representation of a series in $A[[X]]$ as a linear combination of $g_1, \dots, g_m$ which is *not* a standard representation can be improved in the following sense:

Lemma 2.6. *Suppose that $G = \{g_1, \dots, g_m\} \subseteq A[[X]]$ is closed under S-series, and let $q_1, \dots, q_m \in A[[X]]$ be such that, with $f = q_1 g_1 + \cdots + q_m g_m$,*

$$v(f) > \min_i v(q_i g_i).$$

Then there exist $q_1', \dots, q_m' \in A[[X]]$ such that $f = q_1' g_1 + \cdots + q_m' g_m$ and

$$\min_i v(q_i' g_i) > \min_i v(q_i g_i).$$

Proof. After rearranging the $g_1, \dots, g_m$ if necessary (and the $q_1, \dots, q_m$ accordingly), we may assume that

$$\nu_0 := v(q_1 g_1) = v(q_2 g_2) = \cdots = v(q_l g_l) < v(q_{l+1} g_{l+1}), \dots, v(q_m g_m)$$

for some $l \in \{1, \dots, m\}$. Since G is closed under S-series, we find $q_{ij} \in A[[X]]$ such that $S_i = \sum_j q_{ij} g_j$, for $i = 1, \dots, k$, are S-series of $g_1, \dots, g_m$, and $v(S_i) = \min_j v(q_{ij} g_j)$ for all i. For each i, write $S_i = \sum_{j=1}^m y_j^{(i)} \frac{X^\mu}{\operatorname{lt}(g_j)} g_j$ with $y^{(1)}, \dots, y^{(k)} \in A^m$ as above. Since

$$\operatorname{lm}(q_1 g_1) + \cdots + \operatorname{lm}(q_l g_l) = 0,$$

there exist $b_1, \dots, b_k \in A$ such that

$$\big(\operatorname{lc}(q_1), \dots, \operatorname{lc}(q_l), 0, \dots, 0\big) = b_1 y^{(1)} + \cdots + b_k y^{(k)}.$$

Let $\nu \in \mathbb{N}^N$ be such that $\nu + \mu = \nu_0$. Then

$$\big(b_1 S_1 + \cdots + b_k S_k\big) X^\nu = \operatorname{lm}(q_1) g_1 + \cdots + \operatorname{lm}(q_l) g_l.$$

It follows that $\left(\sum_i b_i S_i\right) X^\nu = \sum_j q_j'' g_j$, where $q_j'' = \sum_i b_i q_{ij} X^\nu \in A[[X]]$. Now define

$$q_j' = \begin{cases} q_j - \operatorname{lm}(q_j) + q_j'' & \text{if } 1 \leqslant j \leqslant l \\ q_j + q_j'' & \text{else.} \end{cases}$$

Then $f = \sum_j q_j' g_j$, and for $j = 1, \ldots, m$,

$$v(q_j'' g_j) \geqslant \min_i v(q_{ij} g_j) + \nu \geqslant \min_i v(S_i) + \nu > \nu_0$$

and hence $v(q_j' g_j) > \nu_0$ for all j, as desired. □

The following is a Buchberger-style criterion for a finite subset $G = \{g_1, \ldots, g_m\}$ of $A[[X]] \setminus \{0\}$ to be a standard basis, similar to Theorem 4.1 in Becker (1990a), and with an analogous proof.

Proposition 2.7. *If G is closed under S-series, then G is a standard basis.*

Proof. Suppose first that the order type λ of $\leqslant$ is ω; we will show that in this case, statement (2) of Theorem 2.2 holds. Assume for a contradiction that $q_1, \ldots, q_m \in A[[X]]$ are such that $f := q_1 g_1 + \cdots + q_m g_m \neq 0$ does not have a standard representation with respect to G. So $v(f) > \min_i v(q_i g_i)$, and by Lemma 2.6, there exist $q_1', \ldots, q_m' \in A[[X]]$ such that $f = q_1' g_1 + \cdots + q_m' g_m$ and $\nu_1 := \min_i v(q_i g_i) < \nu_2 := \min_i v(q_i' g_i)$. Then $v(f) > \min_i v(q_i' g_i)$, and we may repeat the argument with $q_1', \ldots, q_m'$ replacing $q_1, \ldots, q_m$, respectively. We obtain an infinite sequence $\nu_1 < \nu_2 < \cdots$ with $\nu_k < v(f)$ for all k, which is impossible, since $\lambda = \omega$. Now suppose that $\lambda > \omega$; in this case, we will show that (1) in the theorem holds. For this, let $f \in I$. By Lemma 1.4 and Proposition 1.5 we find an admissible ordering $\leqslant'$ of order type ω such that $v_\leqslant(f) = v_{\leqslant'}(f)$, $v_\leqslant(g_i) = v_{\leqslant'}(g_i)$ for all i, and such that G is closed under S-series, with respect to $\leqslant'$. By the first case, we have $\operatorname{lm}_\leqslant(G) = \operatorname{lm}_{\leqslant'}(G) = \operatorname{lm}_{\leqslant'}(I)$, and it follows that $\operatorname{lm}_\leqslant(f) \in \operatorname{lm}_\leqslant(G)$ as required. □

Before we introduce monic ideals, we record a consequence of this proposition.

Lemma 2.8. *Suppose that A is Noetherian. Let $G = \{g_1, \ldots, g_m\}$ be a standard basis for I with respect to the admissible ordering $\leqslant$. There exists a neighborhood U of $\leqslant$ in AO_N such that G is a standard basis for I with respect to every $\leqslant'$ in U.*

Proof. Let $S_1, \ldots, S_k$ be S-series of $g_1, \ldots, g_m$. Since G is a standard basis for I with respect to $\leqslant$, we find $q_{ij} \in A[[X]]$ such that $S_i = \sum_j q_{ij} g_j$ and $v_\leqslant(S_i) = \min_j v_\leqslant(q_{ij} g_j)$ for all i. By Lemma 1.4, there exists a neighborhood U of $\leqslant$ in AO_N such that $v_\leqslant(S_i) = v_{\leqslant'}(S_i)$ and $v_\leqslant(q_{ij} g_j) = v_{\leqslant'}(q_{ij} g_j)$ for all i, j. Hence every S_i has a standard representation in terms of G, with respect to $\leqslant'$, and so G is a standard basis for I with respect to $\leqslant'$, by Proposition 2.7. □

A set of non-zero generators $G = \{g_1, \ldots, g_m\}$ for the ideal I of $A[[X]]$ is called a **universal standard basis** for I if it is a standard basis for I with respect to *every* admissible ordering on $\mathbb{N}^N$. The previous lemma together with the compactness of AO_N (see Section 1) implies the following generalization of a result of Becker (1990a):

Corollary 2.9. *If A is Noetherian, then every ideal of $A[[X]]$ has a universal standard basis.* □

Monic ideals

The example following the proof of Theorem 2.1 shows that even if G is a standard basis, the remainder of $f \in A[[X]]$ modulo G is not uniquely determined in general. However, if the leading coefficients of $g_1, \ldots, g_m$ are units in A, this is true:

Lemma 2.10. *Suppose that the leading coefficients of $g_1, \ldots, g_m$ are units in A. The following are equivalent:*

(1) *G is a standard basis for I.*

(2) $v(G) = v(I)$.

(3) *For each $f \in A[[X]]$ there exists a* unique *$r \in A[[X]]$ such that*

   (a) *$f = q_1 g_1 + \cdots + q_m g_m + r$ for some $q_1, \ldots, q_m \in A[[X]]$, and*

   (b) $\mathrm{supp}(r) \cap v(I) = \emptyset$.

Proof. The implication (1) ⇒ (2) is clear, and the converse follows since the leading coefficients of $g_1, \ldots, g_m$ are units in A. Suppose $v(G) = v(I)$. For any $f \in A[[X]]$ there exist $r, q_1, \ldots, q_m \in A[[X]]$ such that $f = q_1 g_1 + \cdots + q_m g_m + r$ and $\mathrm{mono}(r) \cap \mathrm{lm}(G) = \{0\}$, by Theorem 2.1. Since the $\mathrm{lc}(g_i)$ are units and $v(G) = v(I)$, this implies $\mathrm{supp}(r) \cap v(I) = \emptyset$. If $r', q_1', \ldots, q_m' \in A[[X]]$ satisfy $f = q_1' g_1 + \cdots + q_m' g_m + r$ and $\mathrm{supp}(r') \cap v(G) = \emptyset$, then $r - r' = (q_1' - q_1)g_1 + \cdots + (q_m' - q_m)g_m \in I$ and $\mathrm{supp}(r - r') \cap v(I) = \emptyset$, hence $r = r'$. This shows (2) ⇒ (3). Now suppose (3) holds, i.e., for each $f \in A[[X]]$ there exists a unique $r \in A[[X]]$ such that $f - r \in (g_1, \ldots, g_m)A[[X]]$ and $\mathrm{supp}(r) \cap v(I) = \emptyset$. If $f \in I$, then $r = 0$, so by Theorem 2.1, we find $q_1, \ldots, q_m \in A[[X]]$ such that $f = q_1 g_1 + \cdots + q_m g_m$ and $v(f) = \min_i v(q_i g_i) \in v(G)$. Hence $v(I) = v(G)$, so G is a standard basis for I. □

We say that I is **monic** if $\mathrm{lc}(I, \nu) = A$ for all $\nu \in v(I)$. This is inspired by Definition 3.3 in Pauer (1992).

Examples. If A is a field, then every non-zero ideal in $A[[X]]$ is monic. If I is a principal ideal, then I is monic exactly if I is generated by a **monic** power series, i.e., a non-zero $f \in A[[X]]$ with $\mathrm{lc}(f) = 1$. More generally, if I has a standard basis $G = \{g_1, \ldots, g_m\}$ which is **monic**, i.e., $\mathrm{lc}(g_i) = 1$ for all i, then I is monic.

We say that $r \in A[[X]]$ is a **standard remainder of** $f \in A[[X]]$ **modulo** I if $f - r \in I$ and $\mathrm{supp}(r) \cap v(I) = \emptyset$. If I is monic, then every $f \in A[[X]]$ has a unique standard remainder modulo I; in fact:

Theorem 2.11. *The following are equivalent:*

(1) *I is monic.*

(2) *There exists a monic standard basis for I.*

(3) *Every $f \in A[[X]]$ has a unique standard remainder modulo I.*

(4) *Every $f \in A[[X]]$ has a standard remainder modulo I.*

Proof. Suppose that I is monic. By Dickson's Lemma and Proposition 1.1, (3) there exists a finite set $G = \{g_1, \dots, g_m\}$ of monic elements of I such that $v(G) = v(I)$. By the lemma, G is a standard basis for I. This shows (1) $\Rightarrow$ (2). The implication (2) $\Rightarrow$ (3) follows by the lemma, and (3) $\Rightarrow$ (4) is trivial. For (4) $\Rightarrow$ (1), let $\nu \in v(I)$ and $r \in A[[X]]$ a standard remainder of X^ν, so $X^\nu - r \in I$ and $\operatorname{supp}(r) \cap v(I) = \emptyset$. Hence $v(X^\nu - r) = \nu$, showing that $1 \in \operatorname{lc}(I, \nu)$. Thus I is monic. □

Note in particular that by the last theorem, any monic ideal of $A[[X]]$ is finitely generated (with no further assumptions on the ring A).

Remark. Let I be any ideal of $A[[X]]$ with standard basis $G = \{g_1, \dots, g_m\}$. Let d be the product of the leading coefficients of $g_1, \dots, g_m$. Suppose that d is not a zero divisor of A and let $A' = A[\frac{1}{d}]$ be the localization of A at the multiplicative subset $\{1, d, d^2, \dots\}$. Then G is a standard basis for $I' = IA'[[X]]$ (by Proposition 3.9), and each $c_i = \operatorname{lc}(g_i)$ is a unit in A'. Hence $G' = \{g_1/c_1, \dots, g_m/c_m\}$ is a monic standard basis for I'.

We say that $G = \{g_1, \dots, g_m\}$ is **reduced** if

(1) $\operatorname{lc}(g_i) = 1$ for all i (i.e., G is monic),

(2) the $v(g_1), \dots, v(g_m)$ form an antichain, and

(3) $\operatorname{supp}\big(g_i - \operatorname{lm}(g_i)\big) \cap v(G) = \emptyset$ for all i.

The following was first proved by Hironaka (1964) in the case where A is a field, for certain admissible orderings, and by Becker (1993) for any admissible ordering. An analog for ideals in *polynomial rings* over fields is due to Buchberger (1965).

Lemma 2.12. *Every monic ideal I has a unique reduced standard basis.*

Proof. Let $\nu_1, \dots, \nu_m \in v(I)$ be pairwise distinct, forming the smallest set of generators of the final segment $v(I)$. such that $\{\nu_1, \dots, \nu_m\}$ is . For $i = 1, \dots, m$, let r_i be the standard remainder of X^{ν_i} modulo I. Setting $g_i := X^{\nu_i} - r_i$ yields a reduced standard basis $G = \{g_1, \dots, g_m\}$ for I. If $H = \{h_1, \dots, h_n\}$ is another reduced standard basis for I, then $v(G) = v(H)$, hence by (2) in the definition above, we have $m = n$ and, after rearranging $h_1, \dots, h_m$ if necessary, we may assume that $v(h_1) = v(g_1), \dots, v(h_m) = v(g_m)$. We then have $\operatorname{supp}(g_i - h_i) \cap v(G) = \emptyset$ by (3), and since $g_i - h_i \in I$ we get $g_i - h_i = 0$ by uniqueness of the standard remainder. Thus $G = H$. □

Remark. The proof of the lemma shows that the reduced standard basis $G = \{g_1, \dots, g_m\}$ for I satisfies the condition $\operatorname{supp}(g_i) \cap v\big(G \setminus \{g_i\}\big) = \emptyset$ for every i.

For division of a series $f \in A[[X]]$ by a sequence of monic series $g_1, \dots, g_m$, we have a more precise variant of Theorem 2.1. We call the power series $q_1, \dots, q_m \in A[[X]]$ and $r \in A[[X]]$ the **distinguished quotients** and **distinguished remainder** of f modulo $g_1, \dots, g_m$, respectively, if they satisfy the following properties:

(1) $f = q_1 g_1 + \cdots + q_m g_m + r$,

(2) $\operatorname{supp}(r) \cap v(G) = \emptyset$, and

(3) $\big(v(g_i) + \operatorname{supp}(q_i)\big) \cap \big\langle v(g_1), \dots, v(g_{i-1})\big\rangle = \emptyset$ for all $i = 1, \dots, m$.

The distinguished quotients and distinguished remainder of a given $f \in A[[X]]$ modulo $g_1, \dots, g_m$ are uniquely determined (if they exist): To see this, note that $v(G) = \Delta_1 \cup \cdots \cup \Delta_m$ is a partition of $v(G)$ into subsets

$$\Delta_i = \big\langle v(g_i)\big\rangle \setminus \big\langle v(g_1), \dots, v(g_{i-1})\big\rangle,$$

some possibly empty. So if $r, q_1, \dots, q_m$ satisfy (1)–(3), then by (3), we get $v(q_i g_i) \in \Delta_i$ for all i with $q_i \neq 0$, hence

$$v(f) = \min\big\{v(q_1 g_1), \dots, v(q_m g_m), v(r)\big\}$$

by (1) and (2). In particular, r is a remainder of f modulo G. Moreover, if $f = 0$, then we necessarily have $q_1 = \cdots = q_m = r = 0$, showing uniqueness. As to existence, we have:

Proposition 2.13. *If $g_1, \dots, g_m$ are monic, then for any $f \in A[[X]]$, there exist distinguished quotients $q_1, \dots, q_m$ and remainder r modulo $g_1, \dots, g_m$.*

Proof. Similarly to the proof of Theorem 2.1, we define, by induction on $\alpha < \lambda$, sequences $\{b_{i,\alpha}\}_{\alpha<\lambda}$ (for $i = 1, \dots, m$) of elements of A with the following properties:

(a) $v(g_i) \not\sqsubseteq \nu_\alpha \Rightarrow b_{i,\alpha} = 0$, and

(b) $\nu_\alpha \in \big\langle v(g_1), \dots, v(g_{i-1})\big\rangle \Rightarrow b_{i,\alpha} = 0$,

for all $\alpha < \lambda$ and all i. Let $\alpha < \lambda$, and suppose that $b_{i,\beta}$ have already been defined, for $\beta < \alpha$ and $i = 1, \dots, m$. Let $b_i^\alpha := \sum_{\beta<\alpha} b_{i,\beta} X^{\nu_\beta}$ and $q_i^\alpha := b_i^\alpha / \operatorname{lt}(g_i) \in A[[X]]$ for $i = 1, \dots, m$, and put $r^\alpha := f - (q_1^\alpha g_1 + \cdots + q_m^\alpha g_m)$. We distinguish two cases: If $\nu_\alpha \notin v(G)$, then we set $b_{i,\alpha} = 0$ for $i = 1, \dots, m$. If $\nu_\alpha \in v(G)$, then there exists a unique $k \in \{1, \dots, m\}$ such that $v(g_k) \sqsubseteq \nu_\alpha$ and $v(g_i) \not\sqsubseteq \nu_\alpha$ for $i = 1, \dots, k-1$, and we set $b_{k,\alpha} = r_\alpha^\alpha / \operatorname{lc}(g_k)$ and $b_{i,\alpha} = 0$ for $i \neq k$. Clearly properties (a) and (b) continue to hold, for α and all i. Put $b_i := \sum_{\alpha<\lambda} b_{i,\alpha} X^{\nu_\alpha}$ and $q_i := b_i / \operatorname{lt}(g_i) \in A[[X]]$ for $i = 1, \dots, m$. We claim that $q_1, \dots, q_m$ and $r := f - (q_1 g_1 + \cdots + q_m g_m)$ satisfy the requirements of the proposition. Here, (1) is clear, and (3) holds by (b). Let $\alpha < \lambda$ with $\nu_\alpha \in v(G)$. Write

$$r = r^\alpha - \big(b_{1,\alpha} X^{\nu_\alpha} / \operatorname{lt}(g_1) \cdot g_1 + \cdots + b_{m,\alpha} X^{\nu_\alpha} / \operatorname{lt}(g_m) \cdot g_m\big) - h$$

where $h = \sum_{i=1}^{m} \sum_{\alpha<\beta<\lambda} b_{i,\beta} X^{\nu_\beta} / \operatorname{lt}(g_i) \cdot g_i$. By definition of $b_{i,\alpha}$ there exists $k \in \{1, \ldots, m\}$ such that $v(g_k) \sqsubseteq \nu_\alpha$, $b_{k,\alpha} = r_\alpha^\alpha / \operatorname{lc}(g_k)$, and $b_{i,\alpha} = 0$ if $i \neq k$. So we have $r = r^\alpha - r_\alpha^\alpha X^{\nu_\alpha} - h$ where $\operatorname{supp}(h) > \nu_\alpha$. Hence $\nu_\alpha \notin \operatorname{supp}(r)$ as desired. □

Standard bases for ideals generated by polynomials

From now on until the rest of this section, we assume that A is an integral domain. Suppose $0 \neq g_1, \ldots, g_m \in A[X]$. Let $d = \operatorname{lc}(g_1) \cdots \operatorname{lc}(g_m)$ and $A' = A[\frac{1}{d}]$ (a subring of the fraction field of A). The next theorem is due to Mora (1982).

Theorem 2.14. *For every $f \in A[X]$ there exist $u, q_1, \ldots, q_m, r \in A[X]$ such that*

(1) $uf = q_1 g_1 + \cdots + q_m g_m + r$,

(2) *u is a unit in $A'[[X]]$,*

(3) $v(r) \notin v(G)$, *and*

(4) $v(f) \leqslant v(q_i g_i)$ *for all $i = 1, \ldots, m$.*

We call any element $r \in A[X]$ with the property that there exist $u, q_1, \ldots, q_m \in A[X]$ such that (1)–(4) in the theorem hold a **weak remainder of f modulo G.** Note that if f has weak remainder 0, then f, as an element of $A'[[X]]$, has a standard representation with respect to G.

The proof of this theorem given in Greuel and Pfister (1996) or Mora (1982) provides in fact an *algorithm* (relative to computations in A) which, given f and $g_1, \ldots, g_m$, computes a weak remainder of f modulo $G = \{g_1, \ldots, g_m\}$. (This is Mora's famous "tangent cone algorithm".) This yields an algorithmic procedure for computing, from given non-zero polynomials $f_1, \ldots, f_n \in A[X]$, elements $g_1, \ldots, g_m \in A[X]$ such that $G = \{g_1, \ldots, g_m\}$ is a standard basis of the ideal of $A'[[X]]$ generated by $f_1, \ldots, f_n$, where $A' = A[\frac{1}{d}]$, $d = \operatorname{lc}(g_1) \cdots \operatorname{lc}(g_m)$ is as above. Starting with $G_0 = \{f_1, \ldots, f_n\}$, we construct a sequence

$$G_0 = \{f_1, \ldots, f_n\} \subseteq G_1 \subseteq \cdots \subseteq G_k = \{g_{k,1}, \ldots, g_{k,m_k}\} \subseteq \cdots$$

of finite subsets of non-zero elements of the ideal of $A[X]$ generated by $f_1, \ldots, f_n$ as follows: Suppose that G_k has been constructed already. For all $1 \leqslant i < j \leqslant m_k$ compute weak remainders r_{ij} of

$$S_{ij} = \operatorname{lc}(g_{k,j}) \frac{X^\mu}{\operatorname{lt}(g_{k,j})} g_{k,i} - \operatorname{lc}(g_{k,i}) \frac{X^\mu}{\operatorname{lt}(g_{k,j})} g_{k,j}$$

modulo G_k. If all of these weak remainders are zero, then $G := G_k$ has the required properties, by Example 2.5 and Proposition 2.7. Otherwise, let

$$G_{k+1} := G_k \cup \{r_{ij} : 1 \leqslant i < j \leqslant m, r_{ij} \neq 0\}.$$

Since then $v(G_0) \subset v(G_1) \subset \cdots$ is a strictly increasing sequence of final segments of $\mathbb{N}^N$ (by (3) of Theorem 2.14), this procedure has to terminate after a finite number of steps.

3 Standard Bases and Specializations

As in the last section, we let A be a ring. A **specialization of A to B** is a ring homomorphism $\sigma\colon A \to B$. If σ is surjective, we say that σ is a **specialization of A onto B.** Any specialization $\sigma\colon A \to B$ has a natural extension to a ring homomorphism $A[[X]] \to B[[X]]$, which we also denote by σ: if $f(X) = \sum_\nu f_\nu X^\nu \in A[[X]]$ is as in (1.1), then

$$\sigma(f) := \sum_\nu \sigma(f_\nu) X^\nu \in B[[X]].$$

We extend this notation to subsets M of $A[[X]]$ as well:

$$\sigma(M) := \big\{\sigma(f) : f \in M\big\}.$$

If I is an ideal of $A[[X]]$ and σ is surjective, then $\sigma(I)$ is an ideal of $B[[X]]$.

Example. In the case where $A = R[C]$, with R a ring and $C = (C_1, \dots, C_M)$ a tuple of pairwise distinct indeterminates, a specialization $\sigma\colon A \to B$ is uniquely determined by its restriction to R and the images $\sigma(C_1), \dots, \sigma(C_M)$ of the indeterminates. Conversely, given any ring homomorphism $\sigma\colon R \to B$ and a tuple $c = (c_1, \dots, c_M) \in B^M$, there exists a unique extension of σ to a specialization $A \to B$, also denoted by σ, such that $\sigma(C) = c$ (i.e., $\sigma(C_i) = c_i$ for all i). If $\sigma|R$ and B are understood, we write $f(c, X)$ for the image of $f(C, X) \in A[[X]]$ under the unique specialization $\sigma\colon A \to B$ with $\sigma(C) = c$, and we put $M(c) := \big\{f(c, X) : f(C, X) \in M\big\}$ for a subset M of $A[[X]]$. (We use similar notation if, say, A is a ring of analytic functions; e.g., see Example 3.7 below.)

Example. For a prime ideal $\mathfrak{p}$ of A we write $a(\mathfrak{p})$ for the image of $a \in A$ under the specialization $\sigma_\mathfrak{p}\colon A \to A/\mathfrak{p}$ given by $a \mapsto a + \mathfrak{p}$. We put $f(\mathfrak{p}; X) := \sigma_\mathfrak{p}(f)$ for $f(X) \in A[[X]]$, and $M(\mathfrak{p}) := \sigma_\mathfrak{p}(M)$ for $M \subseteq A[[X]]$.

Specializations of monic ideals

The following observation is immediate from the definitions, and the fact that $\operatorname{supp}\big(\sigma(g)\big) \subseteq \operatorname{supp}(g)$ for all $g \in A[[X]]$ and specializations σ:

Lemma 3.1. *Let $g_1, \dots, g_m \in A[[X]]$ be monic. If $f \in A[[X]]$ has distinguished quotients $q_1, \dots, q_m$ and distinguished remainder $r \in A[[X]]$ modulo $g_1, \dots, g_m$, then $\sigma(f) \in B[[X]]$ has distinguished quotients $\sigma(q_1), \dots, \sigma(q_m)$ and distinguished remainder $\sigma(r)$ modulo $\sigma(g_1), \dots, \sigma(g_m)$, for each specialization $\sigma\colon A \to B$.*

This readily implies that monic standard bases behave well under specializations:

Proposition 3.2. *Let $G = \{g_1, \dots, g_m\}$ be a monic standard basis for an ideal I of $A[[X]]$ and let $\sigma\colon A \to B$ be a specialization of A to B. Then $\sigma(G)$ is a standard basis for the ideal $\sigma(I)B[[X]]$ of $B[[X]]$ generated by $\sigma(I)$, with $v(I) = v\big(\sigma(I)B[[X]]\big)$. If moreover G is reduced, then so is $\sigma(G)$.*

Proof. Let $S = S_{ij}$ (where $1 \leqslant i < j \leqslant m$) be as in Example 2.5. Then $\sigma(S)$ is an S-series of $\sigma(g_1), \dots, \sigma(g_m)$. Moreover, $S \in I$ has distinguished remainder 0 modulo $g_1, \dots, g_m$; so by Lemma 3.1, $\sigma(S)$ has distinguished remainder 0 modulo $\sigma(g_1), \dots, \sigma(g_m)$. Using Proposition 2.7 it follows that $\sigma(G)$ is a standard basis of $\sigma(I)B[[X]]$. Hence $v(I) = v\big(\sigma(I)B[[X]]\big)$, since $v(g_i) = v\big(\sigma(g_i)\big)$ for all i. This also implies that $\sigma(G)$ is reduced if G is reduced. □

Consider now a set $\mathcal{S}$ of specializations $A \to B$ (for various B) which is **dense**, meaning that $\bigcap_{\sigma\in\mathcal{S}} \ker\sigma = (0)$. We have the following "modular" criterion for membership in a monic ideal of $A[[X]]$:

Proposition 3.3. *Let I be a monic ideal of $A[[X]]$. If $f \in A[[X]]$ satisfies $\sigma(f) \in \sigma(I)B[[X]]$ for all $\sigma\colon A \to B$ in $\mathcal{S}$, then $f \in I$.*

Proof. By Theorem 2.11, f has a unique standard remainder $r \in A[[X]]$ modulo I. By Proposition 3.2 we have $v(I) = v\big(\sigma(I)B[[X]]\big)$, so $\sigma(f)$ has standard remainder $\sigma(r)$ modulo $\sigma(I)B[[X]]$, for all $\sigma \in \mathcal{S}$. But $\sigma(f) \in \sigma(I)B[[X]]$, so $\sigma(r) = 0$ for all σ. Hence $r = 0$, that is, $f \in I$. □

Specializations of arbitrary ideals

Let $G = \{g_1, \dots, g_m\}$ be a standard basis (not necessarily monic) for an ideal I of $A[[X]]$, and suppose that the element $d := \operatorname{lc}(g_1)\cdots\operatorname{lc}(g_m)$ is not a zero divisor of A. After passing to the localization $A' = A[\frac{1}{d}]$ of A, the results above about specializations of monic ideals become applicable to the extension of I to $A'[[X]]$: by the remark following Theorem 2.11,

$$G' = \big\{g_1/\operatorname{lc}(g_1), \dots, g_m/\operatorname{lc}(g_m)\big\}$$

is a monic standard basis for $I' = IA'[[X]]$. Let $\sigma\colon A \to B$ be a specialization of A to B such that $\sigma(d)$ is a non-zero divisor of B. Then σ extends in a unique way to a specialization $A' \to B'$ of A' to $B' = B[\frac{1}{\sigma(d)}]$, which we also denote by σ, and $\sigma(G')$ is a monic standard basis for $\sigma(I')B'[[X]]$ (by Proposition 3.2). If $\sigma(d)$ is a unit in B, then $B = B'$ and $\sigma(I) = \sigma(I')B'[[X]]$. We get:

Corollary 3.4. *If $\sigma\colon A \to B$ is a specialization of A to B such that $\sigma(d)$ is a unit in B, then $\sigma(G)$ is a standard basis for the monic ideal $\sigma(I)B[[X]]$ of $B[[X]]$, and $v(I) = v\big(\sigma(I)B[[X]]\big)$. Moreover, for any $f \in A'[[X]]$ there exist $q_1, \dots, q_m$ and r in $A'[[X]]$ such that $\sigma(q_1), \dots, \sigma(q_m)$ are the distinguished quotients and $\sigma(r)$ is the distinguished remainder of $\sigma(f)$ modulo $\sigma(g_1), \dots, \sigma(g_m)$, for all such specializations σ.* □

Example. If $\sigma\colon A \to K$ is a specialization of A to a field K such that $\sigma(d) \neq 0$, then $\sigma(G)$ is a standard basis for the ideal $\sigma(I)K[[X]]$ of $K[[X]]$, and $v(I) = v\big(\sigma(I)K[[X]]\big)$.

Let now as above $\mathcal{S}$ be a dense set of specializations of A such that $\sigma(d)$ is a unit in B for every $\sigma\colon A \to B$ in $\mathcal{S}$. Then the set $\mathcal{S}' := \big\{\sigma' : \sigma \in \mathcal{S}\big\}$ of specializations of A' is dense. Proposition 3.3 applied to $\mathcal{S}'$ in place of $\mathcal{S}$ yields:

Corollary 3.5. *If $f \in A[[X]]$ satisfies $\sigma(f) \in \sigma(I)B[[X]]$ for all $\sigma\colon A \to B$ in $\mathcal{S}$, then $f \in I'$.* □

Here are a few applications of the preceding corollaries:

Example 3.6. Parusiński and Szafraniec (1997). Let K be a field, $V \subseteq K^m$ an irreducible algebraic set, and suppose that A is the ring of polynomial functions $V \to K$. For each $c \in V$, evaluation at c defines a specialization $h \mapsto h(c)$ of A onto K. Put $\Sigma := \big\{c \in V : d(c) = 0\big\}$, a proper algebraic subset of V. For every $c \in V \setminus \Sigma$, we have $v\big(I(c)\big) = v(I)$, and $G(c)$ is a standard basis for $I(c)$. If $f(X) \in A[[X]]$ with $f(c, X) \in I(c)$ for all $c \in V \setminus \Sigma$, then $f(X) \in I$.

Example 3.7. Bierstone and Milman (1987). Let $K = \mathbb{R}$ or $K = \mathbb{C}$. Let U be an open subset of K^m, let V be an irreducible analytic subset of U, and W a proper analytic subset of V. Suppose that A is the ring of meromorphic functions on V with poles in W. (If $W = \emptyset$ then A is the ring $\mathcal{O}(V)$ of analytic functions on V.) For each $c \in V \setminus W$, evaluation at c defines a specialization $h \mapsto h(c)$ of A onto K. Put $\Sigma := W \cup \big\{c \in V \setminus W : d(c) = 0\big\}$, a proper analytic subset of V. For every $c \in V \setminus \Sigma$, $G(c) = \big\{g_1(c, X), \ldots, g_m(c, X)\big\}$ is a standard basis for $I(c) = \big\{f(c, X) : f \in I\big\}$, and we have $v\big(I(c)\big) = v(I)$.

Example 3.8. Schoutens (2001). Suppose that $A = \mathbb{Z}$. If $f \in \mathbb{Z}[[X]]$ satisfies $f(p; X) \in I(p)$ for infinitely many primes p, then $f(X)$ is an element of the ideal of $\mathbb{Z}[\frac{1}{d}][[X]]$ generated by I. (This is a stronger form of the first theorem stated in the introduction.)

Flat specializations

Let $\sigma\colon A \to B$ be a specialization. For every ideal I of $A[[X]]$ we have

$$\operatorname{lm}\big(\sigma(I)B[[X]]\big) \supseteq \sigma\big(\operatorname{lm}(I)\big)B[X].$$

We are interested under which conditions on σ the reverse inclusion also holds. If σ is flat with $v\big(\sigma(g_j)\big) = v(g_j)$ for all j (for example, if σ is flat and injective), then the images of S-series of $g_1, \ldots, g_m$ under σ are S-series of $\sigma(g_1), \ldots, \sigma(g_m)$. Hence if in addition A is Noetherian and $G = \{g_1, \ldots, g_m\}$ is a standard basis for I, then $\sigma(G) = \big\{\sigma(g_1), \ldots, \sigma(g_m)\big\}$ is a standard basis for $\sigma(I)B[[X]]$, with $\operatorname{lm}\big(\sigma(I)B[[X]]\big) = \sigma\big(\operatorname{lm}(I)\big)B[X]$. More generally, we have:

Proposition 3.9. *If A is Noetherian and σ is flat, then*

$$\operatorname{lm}\big(\sigma(I)B[[X]]\big) = \sigma\big(\operatorname{lm}(I)\big)B[X]$$

for every ideal I of $A[[X]]$. In particular, if G is a standard basis for I, then $\sigma(G)$ is a standard basis for the ideal $\sigma(I)B[[X]]$ of $B[[X]]$ generated by the image of I.

Proof. Let $cX^\nu \in \operatorname{lm}\big(\sigma(I)B[[X]]\big)$ with $c \in B$, $c \neq 0$ and $\nu \in \mathbb{N}^N$. We claim that $cX^\nu \in \sigma\big(\operatorname{lm}(I)\big)B[X]$. For this, we may assume (by Lemmas 1.4 and 2.8) that the admissible ordering $\leqslant$ has order type ω. We can write

$$cX^\nu = \operatorname{lm}\big(b_1\sigma(f_1) + \cdots + b_r\sigma(f_r)\big)$$

for some r and some $b_i \in B$ and $f_i \in I$. Note that $\mu := \min_i v\big(\sigma(f_i)\big) \leqslant \nu$. We may assume that the b_i and f_i are chosen such that μ is maximal, and it is enough to see that $\mu = \nu$. Suppose otherwise, i.e., $\mu < \nu$. Then $b_1\sigma(f_{1,\mu}) + \cdots + b_r\sigma(f_{r,\mu}) = 0$, hence $b = (b_1, \ldots, b_r)$ is a B-linear combination $b = c_1y^{(1)} + \cdots + c_ky^{(k)}$ of solutions $y^{(1)}, \ldots, y^{(k)} \in A^r$ of the linear equation $y_1f_{1,\mu} + \cdots + y_rf_{r,\mu} = 0$, by flatness of σ. Put $h_i := \sum_j y_j^{(i)} f_j \in I$ for $i = 1, \ldots, k$. Then

$$c_1\sigma(h_1) + \cdots + c_k\sigma(h_k) = b_1\sigma(f_1) + \cdots + b_r\sigma(f_r)$$

with $v\big(\sigma(h_i)\big) > \mu$ for every i, a contradiction. □

Remarks. The last proposition applies in particular to the case where $B = S^{-1}A$ is the localization of A at a multiplicative subset S. An analog of Proposition 3.9 for Gröbner bases has been shown in Bayer et al. (1993).

Using Theorem 2.2 we obtain:

Corollary 3.10. *If $A \subseteq B$ is a faithfully flat extension of Noetherian rings, then $IB[[X]] \cap A[[X]] = I$ for every ideal I of $A[[X]]$.* □

Comprehensive standard bases

Let $\mathcal{S}$ be a class of specializations of A and I an ideal of $A[[X]]$. We say that a standard basis G of I is **comprehensive** with respect to $\mathcal{S}$ if $\sigma(G)$ is a standard basis for the ideal $\sigma(I)B[[X]]$ of $B[[X]]$, for all specializations $\sigma\colon A \to B$ from $\mathcal{S}$. A standard basis in $A[[X]]$ is called **comprehensive** with respect to $\mathcal{S}$ if it is a comprehensive standard basis of the ideal of $A[[X]]$ which it generates. This is modeled after the definition of comprehensive Gröbner basis in Weispfenning (1992).

Examples.

(1) Every monic standard basis is comprehensive for the class of all specializations of A, by Proposition 3.2.

(2) Every standard basis is comprehensive for the class of all flat specializations of A, by Proposition 3.9.

In general, the existence of comprehensive standard bases appears to be a rather subtle matter. We will show here:

Theorem 3.11. *If A is Noetherian, then every ideal of $A[[X]]$ has a standard basis which is comprehensive for all specializations of A to fields.*

For the proof of this theorem we first note that Proposition 3.9 implies the following fact, which allows us to focus on specializations of A to fields of the form $\mathrm{Frac}(A/\mathfrak{p})$ for a prime ideal $\mathfrak{p}$ of A. Here and below, we use $\mathrm{Frac}(R)$ to denote the field of fractions of a domain R.

Lemma 3.12. *Let G be a subset of $A[[X]]$. The following are equivalent:*

(1) *G is a comprehensive standard basis for all specializations of A to a field.*

(2) *G is a comprehensive standard basis for all specializations $\sigma\colon A \to K$ of A to a field K with $K = \operatorname{Frac}\big(\sigma(A)\big)$.*

(3) *G is a comprehensive standard basis for all specializations $A \to \kappa(\mathfrak{p}) := \operatorname{Frac}(A/\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal of A.*

We consider the set $\operatorname{Spec} A$ of prime ideals of A as a topological space equipped with the Zariski topology. Its closed sets are the subsets of $\operatorname{Spec} A$ of the form

$$V(M) := \big\{\mathfrak{p} \in \operatorname{Spec} A : M \subseteq \mathfrak{p}\big\}$$

for a subset M of A. We write $V(a) = V(\{a\})$ for $a \in A$. For any multiplicative subset S of A, we identify $\operatorname{Spec} S^{-1}A$ with the subspace $\operatorname{Spec} A \setminus \bigcup_{s\in S} V(s)$ of $\operatorname{Spec} A$, and for any $\mathfrak{p} \in \operatorname{Spec} A$, we identify $\operatorname{Spec} A/\mathfrak{p}$ with the (closed) subspace $V(\mathfrak{p})$, in the usual way. From now on, the ring A is always assumed to be Noetherian, so that $\operatorname{Spec} A$, ordered by reverse inclusion, is well-founded. A constructible subset of $\operatorname{Spec} A$ by definition is a finite Boolean combination of closed subsets.

Let $G = \{g_1, \dots, g_m\}$ be a standard basis in $A[[X]]$. Suppose that no $\operatorname{lc}(g_i)$ is a zero-divisor of A, let $d = \operatorname{lc}(g_1) \cdots \operatorname{lc}(g_m)$, and put

$$\Sigma := V(d) = V\big(\operatorname{lc}(g_1)\big) \cup \cdots \cup V\big(\operatorname{lc}(g_m)\big),$$

a closed subset of $\operatorname{Spec} A$. For every $\mathfrak{p} \in \operatorname{Spec} A \setminus \Sigma$ we have $v\big(g_i(X)\big) = v\big(g_i(\mathfrak{p}; X)\big)$ for all i, and $G(\mathfrak{p})$ is a standard basis in $\kappa(\mathfrak{p})[[X]]$, by Corollary 3.4. For later use we also note another consequence of this corollary:

Lemma 3.13. *Let $A' = A[\frac{1}{d}]$. For every $f(X) \in A'[[X]]$ there exist $q_1, \dots, q_m \in A'[[X]]$ and $r(X) \in A'[[X]]$ such that $q_1(\mathfrak{p}; X), \dots, q_m(\mathfrak{p}; X)$ are the distinguished quotients and $r(\mathfrak{p}; X)$ is the distinguished remainder of $f(\mathfrak{p}; X)$ modulo $g_1(\mathfrak{p}; X), \dots, g_m(\mathfrak{p}; X)$, for each $\mathfrak{p} \in \operatorname{Spec} A \setminus \Sigma$.*

In the following, we fix an ideal I of $A[[X]]$.

Proposition 3.14. *For every $\mathfrak{q} \in \operatorname{Spec} A$ there exists a finite subset $G_\mathfrak{q}$ of I such that $G_\mathfrak{q}(\mathfrak{p})$ is a standard basis for the ideal generated by $I(\mathfrak{p})$ in $\kappa(\mathfrak{p})[[X]]$, for all $\mathfrak{p} \in V(\mathfrak{q})$.*

Proof. We proceed by Noetherian induction. The claim is certainly true if $\mathfrak{q}$ is a maximal ideal. Otherwise, let $\overline{A} := A/\mathfrak{q}$ and $\overline{I} := I(\mathfrak{q}) \subseteq \overline{A}[[X]]$. Choose a finite subset $G = \{g_1, \dots, g_m\}$ of I such that $\overline{G} := G(\mathfrak{q})$ is a standard basis for the ideal $\overline{I}$ of $\overline{A}[[X]]$. Let $\nu_i = v\big(g_i(\mathfrak{q}; X)\big)$ and $a_i = g_{i,\nu_i}$ for $i = 1, \dots, m$, so $\operatorname{lc}\big(g_i(\mathfrak{q}; X)\big) = a_i(\mathfrak{q})$. Let $d := a_1 \cdots a_m \in A \setminus \mathfrak{q}$ and $\Sigma := V(d)$.

By the remarks preceding Lemma 3.13 (applied to the domain $\overline{A}$ and the standard basis $\overline{G}$ of $\overline{I}$ in place of A and G, respectively), for every $\mathfrak{p} \in V(\mathfrak{q}) \setminus \Sigma$, $G(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$ with $v\big(g_i(\mathfrak{q}; X)\big) = v\big(g_i(\mathfrak{p}; X)\big)$ for all i. Let now

$$V(\mathfrak{q}) \cap \Sigma = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_s)$$

be a decomposition of the proper closed subset $V(\mathfrak{q}) \cap \Sigma$ of $V(\mathfrak{q})$ into irreducible closed subsets, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in \operatorname{Spec} A$. By induction hypothesis applied to $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ in place of $\mathfrak{q}$ there exist finite subsets $G_{\mathfrak{p}_i}$ of I such that $G_{\mathfrak{p}_i}(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$, for all $\mathfrak{p} \in V(\mathfrak{p}_i)$. Let

$$G_{\mathfrak{q}} := G \cup G_{\mathfrak{p}_1} \cup \cdots \cup G_{\mathfrak{p}_s}.$$

If $\mathfrak{p} \in V(\mathfrak{q}) \cap \Sigma$, then $\mathfrak{p} \in V(\mathfrak{p}_i)$ for some i, hence $G_{\mathfrak{q}}(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$, since it contains the standard basis $G_{\mathfrak{p}_i}(\mathfrak{p})$. This finishes the inductive step. □

Applying the proposition to the finitely many minimal primes of A gives rise to a finite subset G_0 of I, every specialization of which to a residue field $\kappa(\mathfrak{p})$ of A is a standard basis for $I(\mathfrak{p})$. Let G be a standard basis for I which extends G_0. Then G is a comprehensive standard basis for all specializations of A to fields, by Lemma 3.12. This completes the proof of Theorem 3.11. □

Remark. If we drop the condition that A be Noetherian, an argument similar to the one above still shows: every ideal of $A[[X]]$ contains a finite subset which is a standard basis under every specialization of A to a field.

Applications

We finish with some consequences of Theorem 3.11 and its proof. We first note that by the remarks following Theorem 2.14:

Corollary 3.15. *Every ideal of $A[[X]]$ generated by polynomials from $A[X]$ has a standard basis which consists entirely of elements of $A[X]$ and which is comprehensive for all specializations of A to fields.* □

Applying this to the case where $A = \mathbb{Z}[C]$ for a tuple $C = (C_1, \ldots, C_M)$ of indeterminates yields:

Corollary 3.16. *For every $d \in \mathbb{N}$ there exists a bound $\beta = \beta(N, d) \in \mathbb{N}$ with the following property: for every field K and all polynomials $f_1, \ldots, f_n \in K[X] = K[X_1, \ldots, X_N]$ of degree at most d, there exist $g_1, \ldots, g_m \in K[X]$ of degree at most β such that $G = \{g_1, \ldots, g_m\}$ is a standard basis for the ideal of $K[[X]]$ generated by $f_1, \ldots, f_n$.* □

The last corollary is similar to a result of Weispfenning (1988) about uniform degree bounds for Gröbner bases. It would be interesting to obtain an explicit (say doubly-exponential) bound β, as for Gröbner bases in Dubé (1990), Möller and Mora (1984).

The inductive argument used in the proof of Proposition 3.14 also shows:

Corollary 3.17. *There exists a partition*

$$\operatorname{Spec} A = \Sigma_1 \cup \cdots \cup \Sigma_t \qquad (t > 0)$$

of $\operatorname{Spec} A$ *into constructible subsets and for each $j = 1, \ldots, t$ a finite subset G_j of I such that $G_j(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})$ with $v\big(g(\mathfrak{p}; X)\big) = v\big(g(\mathfrak{q}; X)\big) \in \mathbb{N}^N$ for every $\mathfrak{p}, \mathfrak{q} \in \Sigma_j$ and $g \in G_j$.* □

In the context of the previous corollary, it follows that there exist final segments $F_1, \dots, F_t$ of $\mathbb{N}^N$ such that $v\big(I(\mathfrak{p})\big) = F_j$ for all j and $\mathfrak{p} \in \Sigma_j$. In particular, the set of $v\big(I(\mathfrak{p})\big)$, where $\mathfrak{p}$ ranges over all prime ideals of A, is finite. Here is an application of this observation.

For an ideal J of $R = K[[X]]$, where K is a field, we denote by $H_J \colon \mathbb{N} \to \mathbb{N}$ the Hilbert-Samuel function of J, given by $H_J(s) = \dim_K R/(J, \mathfrak{m}^{s+1})$ for every s, where $\mathfrak{m}$ is the maximal ideal of R. The following is a well-known consequence of the existence of standard remainders modulo J:

Lemma 3.18. *If the admissible ordering $\leqslant$ is degree-compatible, then the images of the monomials X^ν with $\nu \in \mathbb{N}^N \setminus v(J)$ and $|\nu| \leqslant s$ form a basis of the K-vector space $R/(J, \mathfrak{m}^{s+1})$.*

Hence by the remark following Corollary 3.17 we see that only finitely many Hilbert-Samuel functions H_J arise, where $J = \sigma(I)K[[X]]$ and $\sigma \colon A \to K$ ranges over all specializations of A to fields. An analogous fact holds for Hilbert functions of homogeneous ideals in polynomial rings over fields; for a non-standard proof of this see Schmidt-Göttsch (1987).

Corollary 3.19. *Suppose that A is a domain, and let $f(X) \in A[[X]]$. The set*

$$\Sigma = \big\{\mathfrak{p} \in \operatorname{Spec} A : f(\mathfrak{p}; X) \in I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]\big\}$$

is constructible. Moreover, given generators $f_1, \dots, f_n$ of I there exists a partition

$$\Sigma = \Delta_1 \cup \dots \cup \Delta_t$$

of Σ into constructible subsets (for some $t \in \mathbb{N}$, $t > 0$), as well as non-zero $d_1, \dots, d_t \in A$ and n-tuples $(q_{1j}, \dots, q_{nj})$ of elements of $A_j[[X]]$, where $A_j = A[\frac{1}{d_j}]$, $j = 1, \dots, t$, such that for every $j \in \{1, \dots, t\}$ we have $\Delta_j \cap V(d_j) = \emptyset$ and

$$f(\mathfrak{p}; X) = q_{1j}(\mathfrak{p}; X) f_1(\mathfrak{p}; X) + \dots + q_{nj}(\mathfrak{p}; X) f_n(\mathfrak{p}; X)$$

for $\mathfrak{p} \in \Delta_j$.

Proof. Let $\Sigma_1, \dots, \Sigma_t$ as in Corollary 3.17. By Lemma 3.13, for every $j = 1, \dots, t$ there exist $r_j(X) \in A_j[[X]]$ such that $r_j(\mathfrak{p}; X)$ is the standard remainder of $f(\mathfrak{p}; X)$ modulo $I(\mathfrak{p})$, for all $\mathfrak{p} \in \Sigma_j$. Here $A_j = A[\frac{1}{d_j}]$ is a localization of A at a non-zero element d_j. The set of prime ideals $\mathfrak{p} \in \Sigma_j$ which contain every coefficient of r_j is closed. Therefore each $\Delta_j := \big\{\mathfrak{p} \in \Sigma_j : r_j(\mathfrak{p}; X) = 0\big\}$ is constructible with $\Sigma = \Delta_1 \cup \dots \cup \Delta_t$. The second part also follows from Lemma 3.13. □

The previous corollary, applied to $A = \mathbb{Z}[C]$ where $C = (C_1, \dots, C_M)$ is a tuple of indeterminates, combined with Corollary 3.10, implies the second theorem stated in the introduction:

Corollary 3.20. *Let $f_0(C, X), \dots, f_n(C, X) \in A[[X]]$, where $A = \mathbb{Z}[C]$. There exists a constructible subset Σ of $\operatorname{Spec} A$ with the following property: for every field K and $c \in K^M$ we have $c \in \Sigma(K)$ if and only if*

$$f_0(c, X) \in \big(f_1(c, X), \dots, f_n(c, X)\big)K[[X]].$$

Moreover, there exists a partition

$$\Sigma = \Delta_1 \cup \cdots \cup \Delta_t \qquad (\textit{for some } t \in \mathbb{N},\ t > 0)$$

of Σ *into constructible subsets, polynomials* $d_1(C), \ldots, d_t(C) \in A$ *with* $\Delta_j \cap V(d_j) = \emptyset$ *for all* j*, and* n*-tuples*

$$\big(q_{1j}(C,X), \ldots, q_{nj}(C,X)\big), \qquad j = 1, \ldots, t,$$

of power series in $A_j[[X]]$*, with* $A_j = A[\frac{1}{d_j}]$*, such that for every field* K *and* $c \in \Delta_j(K)$ *we have*

$$f(c,X) = q_{1j}(c,X) f_1(c,X) + \cdots + q_{nj}(c,X) f_n(c,X)$$

in $K[[X]]$*.* □

Remark. It is possible to develop a theory of standard bases for submodules of finitely generated free modules over $A[[X]]$. (See Bierstone and Milman (1987).) Without proof, let us note that the appropriate generalization of Theorem 3.11 then also holds, and together with Schreyer's method (see, e.g., Eisenbud (1995), Chapter 15, in the polynomial case) this can be used to show the analog of the preceding corollary for homogeneous linear equations: Given $f_1(C,X), \ldots, f_n(C,X) \in A[[X]]$, where $A = \mathbb{Z}[C]$, there exists a partition

$$\operatorname{Spec} A = \Pi_1 \cup \cdots \cup \Pi_s \qquad (s \in \mathbb{N}, s > 0)$$

of $\operatorname{Spec} A$ into constructible subsets and for each $j \in \{1, \ldots, s\}$ a non-zero element b_j of A with $\Pi_j \cap V(b_j) = \emptyset$ and finitely many vectors

$$y^{(j,1)}(C,X), \ldots, y^{(j,r)}(C,X) \in A_j[[X]]^n \qquad (\text{for some } r \in \mathbb{N}),$$

where $A_j = A[\frac{1}{b_j}]$, such that for every M-tuple c with entries in a field K and $j \in \{1, \ldots, s\}$ such that $c \in \Delta_j(K)$ the vectors

$$y^{(j,1)}(c,X), \ldots, y^{(j,r)}(c,X) \in K[[X]]^n$$

generate the $K[[X]]$-module of solutions (in $K[[X]]^n$) to the equation

$$f_1(c,X) y_1 + \cdots + f_n(c,X) y_n = 0.$$

Here is a variant of Corollary 3.17 for parametrizing reduced standard bases:

Corollary 3.21. *Suppose that* A *is a domain. There exists a partition*

$$\operatorname{Spec} A = \Sigma_1 \cup \cdots \cup \Sigma_t \qquad (t > 0)$$

of $\operatorname{Spec} A$ *into constructible subsets and for each* $j = 1, \ldots, t$ *an element* $d_j \neq 0$ *of* A *with* $V(d_j) \cap \Sigma_j = \emptyset$ *and a finite subset* G'_j *of* $IA_j[[X]]$*, where* $A_j = A[\frac{1}{d_j}]$*, such that* $G'_j(\mathfrak{p})$ *is the reduced standard basis for* $I(\mathfrak{p})$*, for every* $\mathfrak{p} \in \Sigma_j$*.*

Proof. Choose constructible subsets $\Sigma_1, \ldots, \Sigma_t$ of $\operatorname{Spec} A$ as in Corollary 3.17 and final segments $F_1, \ldots, F_t$ of $\mathbb{N}^N$ as in the remark following it. Fix $j \in \{1, \ldots, t\}$, let $\Sigma := \Sigma_j$, $F := F_j$, and let $\nu_1, \ldots, \nu_m \in F$ be pairwise distinct such that $\{\nu_1, \ldots, \nu_m\}$ is the smallest set of generators for the final segment F. By Lemma 3.13, given $i \in \{1, \ldots, m\}$ there exists $r_i(X) \in A'[[X]]$ such that $r_i(\mathfrak{p}; X)$ is the standard remainder of X^{ν_i} modulo $I(\mathfrak{p})$, for all $\mathfrak{p} \in \Sigma$. Here $A' = A[\frac{1}{d}]$ is a localization of A at a non-zero element d with $d \notin \mathfrak{p}$ for all $\mathfrak{p} \in \Sigma$. Setting $g_i := X^{\nu_i} - r_i$ yields a finite subset $G' = \{g_1, \ldots, g_m\}$ of $IA'[[X]]$ such that $G'(\mathfrak{p})$ is the reduced standard basis for $I(\mathfrak{p})$, for each $\mathfrak{p} \in \Sigma$. (See proof of Lemma 2.12.) $\square$

We close this paper with a strengthening of Theorem 3.11. See Weispfenning (2003) for a proposal, in a different direction, to make the notion of comprehensive Gröbner basis more canonical.

Corollary 3.22. *Suppose that A is Noetherian. Every ideal I of $A[[X]]$ has a universal standard basis G with the property that $\sigma(G)$ is a universal standard basis for $\sigma(I)K[[X]]$, for every specialization $\sigma\colon A \to K$ of A to a field K.*

Proof. By Lemma 3.12 it is enough to show the existence of a universal standard basis G for I such that $G(\mathfrak{p})$ is a universal standard basis for $I(\mathfrak{p})$, for every prime ideal $\mathfrak{p}$ of A. We claim that the following strengthening of Proposition 3.14 holds: For every $\mathfrak{q} \in \operatorname{Spec} A$ and admissible ordering $\leqslant$ there exists a finite subset $G_{\mathfrak{q},\leqslant}$ of I and an open neighborhood $U_{\mathfrak{q},\leqslant}$ of $\leqslant$ in AO_N such that for all $\mathfrak{p} \in V(\mathfrak{q})$ and all $\leqslant'$ in $U_{\mathfrak{q},\leqslant}$, $G_{\mathfrak{q},\leqslant}(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$ with respect to $\leqslant'$. If this claim holds, then by compactness of AO_N there exists, for each $\mathfrak{q} \in \operatorname{Spec} A$, a finite subset $G_{\mathfrak{q}}$ of I with the property that $G_{\mathfrak{q}}(\mathfrak{p})$ is a universal standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$. Any universal standard basis G containing $G_{\mathfrak{q}}$ for each minimal prime $\mathfrak{q}$ of A then has the desired property.

The proof of the claim proceeds by Noetherian induction on $\mathfrak{q}$, as in Proposition 3.14. If $\mathfrak{q}$ is a maximal ideal we may choose $U_{\leqslant,\mathfrak{q}} = \mathrm{AO}_N$ for all $\leqslant$ in AO_N and $G_{\leqslant,\mathfrak{q}}$ to be a lifting of a universal standard basis for $I(\mathfrak{q})\kappa(\mathfrak{q})[[X]]$. Now suppose that $\mathfrak{q}$ is not maximal, and let $G = \{g_1, \ldots, g_m\}$ be a finite subset of I with the property that $\overline{G} = G(\mathfrak{q})$ is a standard basis with respect to $\leqslant$ for the ideal $\overline{I} = I(\mathfrak{q})$ of $\overline{A}[[X]]$, where $\overline{A} = A/\mathfrak{q}$. Let $\nu_i := v_{\leqslant}\big(g_i(\mathfrak{q}; X)\big)$ for $i = 1, \ldots, m$. By Lemmas 1.4 and 2.8 there exists an open neighborhood U of $\leqslant$ in AO_N such that for every $\leqslant'$ in U, $G(\mathfrak{q})$ is a standard basis with respect to $\leqslant'$ and $\nu_i = v_{\leqslant'}\big(g_i(\mathfrak{q}; X)\big)$ for each i. Let $a_i := g_{i,\nu_i}$ for each i and $\Sigma := V(a_1 \cdots a_m)$. Then, for every $\mathfrak{p} \in V(\mathfrak{q}) \setminus \Sigma$ and $\leqslant'$ in U, $G(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$ with respect to $\leqslant'$ and $v_{\leqslant'}\big(g_i(\mathfrak{q}; X)\big) = v_{\leqslant'}\big(g_i(\mathfrak{p}; X)\big)$ for all i. Let now $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in \operatorname{Spec} A$ such that

$$V(\mathfrak{q}) \cap \Sigma = V(\mathfrak{p}_1) \cup \cdots \cup V(\mathfrak{p}_s).$$

By induction hypothesis there exist finite subsets $G_{\mathfrak{p}_i,\leqslant}$ of I and open neighborhoods $U_{\mathfrak{p}_i,\leqslant}$ of $\leqslant$ such that $G_{\mathfrak{p}_i,\leqslant}(\mathfrak{p})$ is a standard basis for $I(\mathfrak{p})\kappa(\mathfrak{p})[[X]]$ with respect to $\leqslant'$, for all $\mathfrak{p} \in V(\mathfrak{p}_i)$ and $\leqslant'$ in $U_{\mathfrak{p}_i,\leqslant}$. Setting

$$G_{\mathfrak{q},\leqslant} := G \cup G_{\mathfrak{p}_1,\leqslant} \cup \cdots \cup G_{\mathfrak{p}_s,\leqslant}, \quad U_{\mathfrak{q},\leqslant} := U \cap U_{\mathfrak{p}_1,\leqslant} \cap \cdots \cap U_{\mathfrak{p}_s,\leqslant}$$

finishes the inductive step. $\square$

References

M. Aschenbrenner. *Ideal Membership in Polynomial Rings over the Integers*. PhD thesis, University of Illinois at Urbana-Champaign, 2001.

D. Bayer, A. Galligo, and M. Stillman. Gröbner bases and extension of scalars. In *Computational Algebraic Geometry and Commutative Algebra, Cortona, 1991*, Sympos. Math., XXXIV, pages 198–215. Cambridge Univ. Press, Cambridge, 1993.

T. Becker. Stability and Buchberger criterion for standard bases in power series rings. *J. Pure Applied Algebra*, 66:219–227, 1990a.

T. Becker. Standard bases and some computations in rings of power series. *J. Symbolic Comput.*, 10:165–179, 1990b.

T. Becker. Standard bases in power series rings: uniqueness and superfluous critical pairs. *J. Symbolic Comput.*, 15:251–265, 1993.

E. Bierstone and P. Milman. Relations among analytic functions, I. *Ann. Inst. Fourier*, 37: 187–239, 1987.

J. Briançon. Weierstrass préparé à la Hironaka. *Astérisque*, 7, 8:67–73, 1973.

B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*. PhD thesis, Universität Innsbruck, 1965.

B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequ. Math.*, 4:374–383, 1970.

L. van den Dries and K. Schmidt. Bounds in the theory of polynomial rings over fields. A nonstandard approach. *Invent. Math.*, 76(1):77–91, 1984.

T. W. Dubé. The structure of polynomial ideals and Gröbner bases. *SIAM J. Comput.*, 19 (4):750–775, 1990.

D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

A. Galligo. Sur le théorème de préparation de Weierstrass pour un idéal de $k\{x_1, \ldots, x_n\}$. *Astérisque*, 7–8:165–169, 1973.

A. Galligo. À propos du théorème de préparation de Weierstrass. In *Fonctions de plusieurs variables complexes* (*Sém. François Norguet, Octobre 1970–Decembre 1973; à la mémoire d'André Martineau*), volume 409 of *Lecture Notes in Math.*, pages 543–579. Springer-Verlag, Berlin, 1974.

P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6(2–3):149–167, 1988.

H. Grauert. Über die Deformation isolierter Singularitäten analytischer Mengen. *Invent. Math.*, 15:171–198, 1972.

G.-M. Greuel and G. Pfister. Advances and improvements in the theory of standard bases and syzygies. *Arch. Math. (Basel)*, 66(2):163–176, 1996.

G. Hermann. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.*, 95:736–788, 1926.

H. Hironaka. Resolution of singularities of an algebraic variety over a field of characteristic zero. *Ann. of Math.*, 79:109–326, 1964.

H. M. Möller and F. Mora. Upper and lower bounds for the degree of Gröbner bases. In *EUROSAM 84, Cambridge, 1984*, pages 172–183. Springer-Verlag, Berlin, 1984.

T. Mora. An algorithm to compute the equations of tangent cones. In J. Calmet, editor, *Computer Algebra, EUROCAM '82, European Computer Algebra Conference, Marseille, France, 5–7 April 1982*, volume 144 of *Lecture Notes in Computer Science*, pages 158–165. Springer-Verlag, Berlin-Heidelberg-New York, 1982.

A. Parusiński and Z. Szafraniec. Algebraically constructible functions and signs of polynomials. *Manuscripta Math.*, 93:443–456, 1997.

F. Pauer. On lucky ideals for Gröbner basis computations. *J. Symbolic Comput.*, 14:471–482, 1992.

P. Ribenboim. Extension of Hironaka's standard basis theorem for generalized power series. *Arch. Math. (Basel)*, 60(5):436–439, 1993.

A. Robinson. On bounds in the theory of polynomial ideals. In *Selected Questions of Algebra and Logic. A Collection Dedicated to the Memory of A. I. Mal′cev*, pages 245–252. Izdat. "Nauka" Sibirsk. Otdel., Novosibirsk, 1973.

K. Schmidt-Göttsch. Bounds and definability over fields. *J. Reine Angew. Math.*, 377:18–39, 1987.

H. Schoutens. Reduction modulo p of power series with integer coefficients. preprint, 2001.

V. Weispfenning. Some bounds for the construction of Gröbner bases. In *Applicable algebra, error-correcting codes, combinatorics and computer algebra, Karlsruhe, 1986*, pages 195–201. Springer-Verlag, Berlin, 1988.

V. Weispfenning. Comprehensive Gröbner bases. *J. Symbolic Comput.*, 14(1):1–29, 1992.

V. Weispfenning. Canonical comprehensive Gröbner bases. *J. Symbolic Comput.*, 36(3–4):669–683, 2003. International Symposium on Symbolic and Algebraic Computation, ISSAC'2002, Lille.