hexagon:2611.00508v1

An Algebraic Proof of Hilbert Nullstellensatz over Rationals

Liang Zhang* Xiaohua(Michael) Xuan†

Abstract

We, with the aid of AI, prove a finite approximate form of the weak Nullstellensatz over the Gaussian rationals: Let $f_1, \ldots, f_m$ be polynomials in n variables with rational complex coefficients. If there are no polynomials $g_1, \ldots, g_m$ in the same variables with rational complex coefficients such that $1 = g_1 f_1 + \cdots + g_m f_m$. (A finite Gröbner basis computation decides whether such polynomials exist.), then, for any positive rational number ε, there exists a pont z with n rational complex coordinates such that

$$\sum_{j=1}^{m} \mathrm{N}(f_j(z)) < \varepsilon^2,$$

where $\mathrm{N}(a + ib) = a^2 + b^2$. The proof is constructive and relis only on finite rational arithmetics without using real numbers or infinite sets concepts, and extends authors' earlier one-vaiable result on Fundemental Theorem of Algerba to several-varaibles case.

Contents

1 Introduction 2

2 Finite setting and statement 2

3 Elementary finite bounds 4

4 Polynomial reduction and Gröbner bases 5

5 From a proper ideal to a finite quotient algebra 14

6 Traces, nilpotents, and reduced quotients 18

7 A primitive element by finite search 19

8 Univariate approximation 20

9 Simultaneous approximation in one parameter 20

10 Proof of the main theorem 21

A The trace pairing and the nilradical 22

B Square-free reduction and the primitive element 24

*Corresponding author: liang.zhang@unidt.com
†Email: michael.xuan@unidt.com

1 Introduction

The existence of polynomial zeros is central to algebra. In one variable, the Fundamental Theorem of Algebra has a history that includes Gauss's dissertation of 1799 [5]. In 1893 Hilbert proved the Nullstellensatz in his work on invariants [7], linking polynomial ideals to their common zeros. Its early development through elimination and ideal theory is surveyed in [6].

Gröbner bases make ideal membership and elimination computational [1]. This raises a foundational question: how much of a polynomial existence theorem follows from finite algebraic data and explicitly justified finite operations?

Motivated by Wildberger's emphasis on finite objects and rational arithmetic [3, 4], the first paper in this series [2] gave a finite rational proof of an approximate version of the Fundamental Theorem of Algebra. Here we extend this approach to several variables: a proper polynomial ideal admits rational complex points where its given generators are simultaneously as small as prescribed. Algebraic types are interpreted through finite data, without completed infinite collections or limiting processes.

Section 2 introduces the finite setting and states the main theorem. Sections 3–4 develop the elementary estimates and polynomial reduction tools. Sections 5–7 reduce the problem to a finite-dimensional algebra and then to one polynomial in one variable. Sections 8–10 use the first paper's approximation result to obtain simultaneous approximation and complete the proof. The appendices supply the detailed arguments for the trace pairing, square-free reduction, and primitive-element construction.

2 Finite setting and statement

We write $x : T$ to mean that x is of type T. For an explicit finite list or set E, $x \in E$ denotes membership in E. For an explicit finite list or set E, the notation $E \subseteq T$ (also $E \subset T$) asserts that each listed entry is of type T.

A *rational complex number* (*Gaussian rational*) is a pair $a, b : \mathbb{Q}$, written $a + ib$, with $i^2 = -1$. We denote this type by K. For $u = a + ib : K$, write

$$|a| := \max\{a, -a\} \quad (a : \mathbb{Q}), \qquad \bar{u} := a - ib, \qquad \mathrm{N}(u) := u\bar{u} = a^2 + b^2, \qquad \mathrm{s}(u) := |a| + |b|.$$

The notation $j : \mathbb{N}$ means that j is a nonnegative integer. For a type T and a specified nonnegative integer ℓ, T^ℓ denotes the type of ℓ-tuples with entries of type T; T^0 has the single empty tuple. Subscripts > 0 and ≥ 0 impose the indicated rational or integer inequalities. The notation $u : K^\times$ means $(u : K) \wedge (u \neq 0)$. A polynomial of type $K[X] = K[X_1, \ldots, X_n]$ is specified by its finite list of nonzero terms with coefficients of type K.

For $\alpha = (\alpha_1, \ldots, \alpha_n) : \mathbb{N}^n$, define

$$X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}, \qquad |\alpha| := \alpha_1 + \cdots + \alpha_n.$$

For nonzero $f = \sum_\alpha c_\alpha X^\alpha : K[X]$, define

$$\deg f := \max\{|\alpha| : c_\alpha \neq 0\}.$$

A bound such as $\deg f < d$ or $\deg f \leq d$ includes the zero polynomial by convention; when $\deg f$ is used as an integer, f is nonzero. We set $0^0 = 1$ in finite polynomial evaluations.

A datum of rational-function type $K(X)$ is represented by f/g with $f, g : K[X]$ and $g \neq 0$, where $f/g = h/v$ means $fv = gh$. Addition and multiplication use the usual numerator–denominator formulas, and the inverse of a nonzero f/g is g/f.

Throughout, L denotes a rational-function field type

$$L = K(X_1, \ldots, X_e), \qquad e \geq 0,$$

with the convention $K(X_1, \dots, X_e) = K$ when $e = 0$. For further indeterminates $Y_1, \dots, Y_\ell$, a polynomial

$$f : L[Y_1, \dots, Y_\ell]$$

is specified by finitely many coefficients of type L. We also call such an f a *polynomial over* L; here "over L" refers to the coefficients being of type L. For polynomials f, g over L, write $f \mid g$ if $g = fh$ for some polynomial h in the same polynomial ring.

When X denotes a single indeterminate over L, we define the derivative of $f(X) = \sum_{j=0}^{d} c_j X^j : L[X]$ by $f'(X) := \sum_{j=1}^{d} j c_j X^{j-1}$. The symbol $\gcd(f, g)$ denotes the unique monic greatest common divisor when at least one input is nonzero. We set $\gcd(0, 0) := 0$.

Definition 2.1 (Proper ideal type and approximate zero)**.** Let

$$f_1, \dots, f_m : K[X_1, \dots, X_n],$$

and write

$$F = (f_1, \dots, f_m), \qquad I = \langle f_1, \dots, f_m \rangle.$$

Here I is an *ideal type* specified by the finite generator datum F. For $g : K[X]$, the assertion $g : I$ means that there are $h_1, \dots, h_m : K[X]$ such that

$$g = h_1 f_1 + \cdots + h_m f_m.$$

For another finitely generated ideal type $J = \langle g_1, \dots, g_t \rangle$ in the same polynomial type, the relation $I \subseteq J$ means that there is a finite polynomial matrix (c_{ij}) with

$$f_i = \sum_{j=1}^{t} c_{ij} g_j \qquad (1 \le i \le m).$$

Equality means such representations exist in both directions. The ideal type I is *proper* if $\neg(1 : I)$, that is, if no $h_1, \dots, h_m : K[X]$ satisfy

$$1 = h_1 f_1 + \cdots + h_m f_m. \tag{2.1}$$

For $z : K^n$, define

$$\mathcal{N}_F(z) := \sum_{j=1}^{m} \mathrm{N}(f_j(z)). \tag{2.2}$$

If $\mathcal{N}_F(z) < \varepsilon^2$, then z is called an ε-approximate common zero of F.

Remark 2.2 (Ideal membership and properness). Membership identities are checked coefficientwise. Section 4 will also give finite tests for nonmembership: Theorem 4.17 constructs a monic Gröbner basis G with generator representations, and Theorem 4.6 proves that the completely reduced remainder $\mathrm{NF}_G(g)$ satisfies

$$g : I \quad \Longleftrightarrow \quad \mathrm{NF}_G(g) = 0.$$

Thus properness is equivalent to $\mathrm{NF}_G(1) \neq 0$. Likewise, reducing the generators of I by a Gröbner basis of J decides $I \subseteq J$; zero remainders give the required generator representations. These tests also apply over L.

Theorem 2.3 (Finite approximate weak Nullstellensatz)**.** *Let $m, n : \mathbb{N}_{>0}$, $f_1, \dots, f_m : K[X_1, \dots, X_n]$, and $\varepsilon : \mathbb{Q}_{>0}$. Then at least one of the following holds:*

(i) *there exist polynomials $h_1, \dots, h_m : K[X_1, \dots, X_n]$ satisfying (2.1);*

(ii) *there exists a point $z : K^n$ satisfying $\mathcal{N}_F(z) < \varepsilon^2$.*

In particular, if $I = \langle F \rangle$ is proper, then (ii) *holds.*

3 Elementary finite bounds

Lemma 3.1 (Rational size inequalities)**.** *For $u, v : K$,*

$$\mathrm{N}(u) \le \mathrm{s}(u)^2, \qquad \mathrm{s}(u+v) \le \mathrm{s}(u) + \mathrm{s}(v), \qquad \mathrm{s}(uv) \le \mathrm{s}(u)\,\mathrm{s}(v). \tag{3.1}$$

For $b_{\mathrm{bd}} : \mathbb{Q}_{\ge 0}$ and a one variable polynomial $f(X) = \sum_{j=0}^{d} c_j X^j : K[X]$, define

$$\|f\|_{b_{\mathrm{bd}}} := \sum_{j=0}^{d} \mathrm{s}(c_j) b_{\mathrm{bd}}^j. \tag{3.2}$$

For $t : K$ with $\mathrm{s}(t) \le b_{\mathrm{bd}}$, one has

$$\mathrm{s}(f(t)) \le \|f\|_{b_{\mathrm{bd}}}, \qquad \mathrm{N}(f(t)) \le \|f\|_{b_{\mathrm{bd}}}^2. \tag{3.3}$$

For $z, w : K$ with $\mathrm{s}(z), \mathrm{s}(w) \le b_{\mathrm{bd}}$ and an integer $j \ge 1$,

$$\mathrm{s}(z^j - w^j) \le j b_{\mathrm{bd}}^{j-1}\, \mathrm{s}(z - w), \tag{3.4}$$

and

$$\mathrm{s}(f(z) - f(w)) \le \mathrm{s}(z - w) \sum_{j=1}^{d} j\, \mathrm{s}(c_j) b_{\mathrm{bd}}^{j-1}. \tag{3.5}$$

Proof. See [2, Lemmas 3.2–3.4]. □

Lemma 3.2 (Finite nonvanishing grid)**.** *Let $n, d : \mathbb{N}$. If*

$$f : K[X_1, \dots, X_n], \qquad f \ne 0, \qquad \deg f \le d,$$

then there is some

$$a \in \{0, 1, \dots, d\}^n \tag{3.6}$$

satisfying $f(a) \ne 0$.

Proof. For $n = 0$, evaluation at the empty tuple leaves the nonzero constant unchanged. For $n = 1$, if $f(0) = \cdots = f(d) = 0$, repeated Euclidean division gives

$$X(X-1)\cdots(X-d) \mid f,$$

contrary to $\deg f \le d$ and $f \ne 0$. For $n > 1$, write

$$f = \sum_{j=0}^{d} f_j(X_1, \dots, X_{n-1}) X_n^j$$

and choose j_0 such that $f_{j_0} \ne 0$. Since $\deg f_{j_0} \le d$, the induction hypothesis gives

$$a' = (a_1, \dots, a_{n-1}) \in \{0, 1, \dots, d\}^{n-1} \qquad \text{with} \qquad f_{j_0}(a') \ne 0.$$

Consequently

$$g(X_n) := f(a', X_n) = \sum_{j=0}^{d} f_j(a') X_n^j$$

is a nonzero polynomial of degree at most d. By the one-variable case, there exists $a_n \in \{0, 1, \dots, d\}$ such that

$$f(a', a_n) = g(a_n) \ne 0.$$

Thus $a = (a', a_n) \in \{0, 1, \dots, d\}^n$ has the required property. □

4 Polynomial reduction and Gröbner bases

4.1 Term orders and polynomial reduction

Definition 4.1 (Degree–lexicographic order)**.** Fix a variable order

$$X_1 \succ X_2 \succ \cdots \succ X_n.$$

For $\alpha, \beta : \mathbb{N}^n$, define

$$X^\alpha \prec_{\mathrm{dlex}} X^\beta$$

if

$$|\alpha| < |\beta|,$$

or if $|\alpha| = |\beta|$ and, at the first coordinate k for which $\alpha_k \neq \beta_k$, one has $\alpha_k < \beta_k$. We write $\prec$ for $\prec_{\mathrm{dlex}}$, and $M \preceq N$ means $M \prec N$ or $M = N$. Then

$$M \prec N \Longrightarrow UM \prec UN \tag{4.0}$$

for all monomials M, N, U. Moreover, for a monomial M with $\deg M = d$,

$$\{N : N \preceq M\} \subseteq \{X^\alpha : |\alpha| \leq d\}, \qquad \#\{X^\alpha : |\alpha| \leq d\} = \binom{d+n}{n}. \tag{4.0a}$$

The order $\prec$ is total, so every nonempty finite set of monomials has a unique maximum.

Definition 4.2 (Leading data)**.** For nonzero $p = \sum c_\alpha X^\alpha$, define its leading monomial by

$$\mathrm{LM}(p) := \max\{X^\alpha : c_\alpha \neq 0\}.$$

The leading coefficient $\mathrm{LC}(p)$ is the coefficient of $\mathrm{LM}(p)$ in p. Define its leading term by

$$\mathrm{LT}(p) := \mathrm{LC}(p)\,\mathrm{LM}(p).$$

The polynomial is monic if $\mathrm{LC}(p) = 1$.

Definition 4.3 (Reduction)**.** If $p, g \neq 0$ and $\mathrm{LM}(g) \mid \mathrm{LM}(p)$, one reduction step is

$$p \longmapsto p - \frac{\mathrm{LC}(p)}{\mathrm{LC}(g)} \frac{\mathrm{LM}(p)}{\mathrm{LM}(g)} g. \tag{4.1}$$

Given an ordered finite tuple $G = (g_1, \ldots, g_s)$ of nonzero polynomials (possibly the empty tuple), complete division starts with

$$f_{\mathrm{cur}} := p, \qquad r := 0, \qquad \mathfrak{q}_1 = \cdots = \mathfrak{q}_s := 0$$

and preserves

$$p = \sum_{j=1}^{s} \mathfrak{q}_j g_j + f_{\mathrm{cur}} + r. \tag{4.1a}$$

If $\mathrm{LT}(f_{\mathrm{cur}}) = cM$ and g_j is the first reducer with $\mathrm{LM}(g_j) \mid M$, define

$$U := \frac{M}{\mathrm{LM}(g_j)}, \qquad \lambda := \frac{c}{\mathrm{LC}(g_j)},$$

and update

$$f_{\mathrm{cur}} \leftarrow f_{\mathrm{cur}} - \lambda U g_j, \qquad \mathfrak{q}_j \leftarrow \mathfrak{q}_j + \lambda U. \tag{4.1b}$$

If no such reducer exists, update

$$f_{\mathrm{cur}} \leftarrow f_{\mathrm{cur}} - cM, \qquad r \leftarrow r + cM. \tag{4.1c}$$

Only a monomial satisfying

$$\mathrm{LM}(g_j) \nmid M \quad (1 \le j \le s) \tag{4.1d}$$

enters r. Thus, when $f_{\mathrm{cur}} = 0$, complete division records

$$p = \mathfrak{q}_1 g_1 + \cdots + \mathfrak{q}_s g_s + r, \tag{4.2}$$

where every monomial of r satisfies (4.1d).

Lemma 4.4 (Finite degree–lexicographic division)**.** *Let nonzero $p : L[X_1, \ldots, X_n]$ have total degree d, and let G be any finite reducer tuple. Complete division (4.1a)–(4.1c) performs at most*

$$\binom{d+n}{n} \tag{4.3}$$

steps. Every monomial occurring in f_{cur} or r during the division has total degree at most d. For $p = 0$, division returns the zero remainder without any steps.

Proof. Let $M = \mathrm{LM}(f_{\mathrm{cur}})$. In the reduction case (4.1b), write

$$g_j = \mathrm{LC}(g_j)\,\mathrm{LM}(g_j) + \sum_{N \prec \mathrm{LM}(g_j)} c_N N. \tag{4.4}$$

With $U = M/\,\mathrm{LM}(g_j)$, equation (4.0) gives

$$UN \prec U\,\mathrm{LM}(g_j) = M \qquad (N \prec \mathrm{LM}(g_j)). \tag{4.5}$$

Hence the term cM is cancelled and every newly created monomial is strictly smaller than M. Since the order first compares total degree,

$$UN \prec M \Longrightarrow \deg(UN) \le \deg M. \tag{4.6}$$

In the remainder case (4.1c), M is removed from f_{cur}, no new active monomial is created, and M is moved to r.

Consequently the successive active leading monomials form a strictly decreasing sequence, and every one has total degree at most $d = \deg p$. No leading monomial can occur twice. Equation (4.0a) gives the bound (4.3). The same argument gives the asserted degree bound for every active and remainder monomial. □

4.2 Critical pairs and the Gröbner property

Definition 4.5 (S-polynomials and their representations)**.** For monic g_i, g_j, define

$$\begin{aligned} \mathrm{lcm}(X^\alpha, X^\beta) &:= X_1^{\max(\alpha_1,\beta_1)} \cdots X_n^{\max(\alpha_n,\beta_n)}, \\ M_{ij} &:= \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j)), \\ S(g_i, g_j) &:= \frac{M_{ij}}{\mathrm{LM}(g_i)} g_i - \frac{M_{ij}}{\mathrm{LM}(g_j)} g_j. \end{aligned} \tag{4.7}$$

For $G = (g_1, \ldots, g_s)$, consider representations

$$S(g_i, g_j) = \sum_{k=1}^{s} \mathfrak{q}_{ijk} g_k \tag{4.8}$$

for $i < j$, satisfying

$$\mathrm{LM}(\mathfrak{q}_{ijk} g_k) \prec M_{ij} \qquad \text{whenever } \mathfrak{q}_{ijk} g_k \neq 0. \tag{4.8a}$$

Theorem 4.6 (Finite Buchberger criterion)**.** *Assume every S-polynomial of a monic finite tuple G admits a representation (4.8) with the leading monomial bound (4.8a). If a nonzero polynomial p has a representation*

$$p = \sum_{j=1}^{s} h_j g_j, \tag{4.9}$$

then some $\mathrm{LM}(g_j)$ divides $\mathrm{LM}(p)$. Complete division by G gives a unique completely reduced remainder, which is zero exactly when the dividend is of ideal type $\langle G\rangle$.

Proof. Let

$$M := \max_{j:h_j\neq 0} \mathrm{LM}(h_j g_j), \qquad \mathcal{A} := \{j : 1 \le j \le s,\ h_j \neq 0,\ \mathrm{LM}(h_j g_j) = M\}.$$

If $M = \mathrm{LM}(p)$, divisibility is immediate. Suppose $M \succ \mathrm{LM}(p)$. Note that the leading term of h_j is $c_j M/\mathrm{LM}(g_j)$ for $j \in \mathcal{A}$, where $c_j = \mathrm{LC}(h_j)$. Cancellation of the coefficient of M gives

$$\sum_{j\in\mathcal{A}} c_j = 0. \tag{4.10}$$

Fix $j_0 \in \mathcal{A}$. Direct expansion using (4.10) gives

$$\sum_{j\in\mathcal{A}} c_j \frac{M}{\mathrm{LM}(g_j)} g_j = \sum_{j\in\mathcal{A}\setminus\{j_0\}} c_j \frac{M}{M_{jj_0}} S(g_j, g_{j_0}). \tag{4.11}$$

Use $S(g_j, g_i) = -S(g_i, g_j)$ when the indices are reversed, and insert the representations (4.8). Every resulting product has leading monomial strictly smaller than M. Tails of the h_j also produce only smaller product monomials. Thus (4.9) is replaced by a finite identity with a strictly smaller maximum product monomial.

Let M_0 be the maximum product monomial in the original identity (4.9). Each use of (4.11) strictly decreases that maximum. Therefore every later maximum belongs to

$$\{N : N \preceq M_0\}. \tag{4.11b}$$

This set is finite by (4.0a); more precisely, it has at most

$$\binom{\deg M_0 + n}{n}$$

elements. Hence after finitely many replacements one reaches $M = \mathrm{LM}(p)$, proving divisibility. If the dividend is of ideal type $\langle G\rangle$, its remainder in (4.2) is also of that type; a nonzero remainder would contradict divisibility. Conversely, a zero remainder gives the required generator representation. For uniqueness, the difference of two completely reduced remainders of the same dividend is of ideal type $\langle G\rangle$ and has only standard monomials. Divisibility therefore forces this difference to be zero. □

Definition 4.7 (Gröbner basis and leading-monomial ideal type)**.** A monic finite tuple G is a *Gröbner basis* of $\langle G\rangle$ if every nonzero element $p : \langle G\rangle$ has $\mathrm{LM}(g) \mid \mathrm{LM}(p)$ for some $g \in G$. The associated *leading-monomial ideal type* is specified by

$$\mathrm{in}(G) := \langle \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\rangle. \tag{4.11a}$$

Definition 4.8 (Standard monomial)**.** Let J be an ideal type in $L[Y_1, \ldots, Y_n]$ with a monic Gröbner basis $G = (g_1, \ldots, g_t)$. A monomial is *standard for G* if it is not divisible by any $\mathrm{LM}(g_\kappa)$.

Lemma 4.9 (Monomial membership and reduced remainders)**.** *For monomials $M, M_1, \dots, M_s$,*

$$M : \langle M_1, \dots, M_s \rangle \quad \Longleftrightarrow \quad M_j \mid M \text{ for some } j. \tag{4.11c}$$

If a nonzero polynomial r is completely reduced by a monic tuple $G = (g_1, \dots, g_s)$, then

$$\mathrm{LM}(g_j) \nmid \mathrm{LM}(r) \qquad (1 \le j \le s). \tag{4.11d}$$

Proof. If $M_j \mid M$, membership is immediate. Conversely, suppose

$$M = \sum_{j=1}^{s} h_j M_j.$$

The coefficient of M on the left is nonzero. Hence some product $h_j M_j$ contains the monomial M, and then $M_j \mid M$. This proves (4.11c). Complete reduction gives $\mathrm{LM}(g_j) \nmid \mathrm{LM}(r)$ for each of the finitely many indices j, which is (4.11d). By (4.11c), these divisibility tests also show that $\mathrm{LM}(r)$ has no representation in the monomial ideal type generated by $\mathrm{LM}(g_1), \dots, \mathrm{LM}(g_s)$. □

4.3 Finite bounds for the Gröbner construction

Definition 4.10 (Step-controlled divisibility-avoiding sequence)**.** Let

$$\delta : \mathbb{N} \longrightarrow \mathbb{N}$$

be a nondecreasing rule computing $\delta(q)$ from a supplied nonnegative integer q by finitely many operations. For $a = (a_1, \dots, a_n) : \mathbb{N}^n$, define

$$|a| := a_1 + \cdots + a_n, \qquad a \le b \Longleftrightarrow a_j \le b_j \quad (1 \le j \le n).$$

A finite sequence

$$a^{(0)}, a^{(1)}, \dots, a^{(\ell-1)} : \mathbb{N}^n$$

is δ-controlled if

$$|a^{(q)}| \le \delta(q) \quad (0 \le q < \ell), \tag{4.12}$$

and is divisibility-avoiding if

$$a^{(i)} \not\le a^{(q)} \quad (0 \le i < q < \ell). \tag{4.13}$$

Lemma 4.11 (Stepwise Buchberger degree control)**.** *Let the nonzero initial polynomials have total degree at most d, and let*

$$d_0 := \max(1, d). \tag{4.14}$$

Let $g^{(0)}, \dots, g^{(\ell-1)}$ be successively adjoined monic nonzero remainders of S-polynomials under complete division by the polynomials already present. For $0 \le q < \ell$, before adjoining $g^{(q)}$, every polynomial present has degree at most

$$2^q d_0. \tag{4.14a}$$

Writing $\mathrm{LM}(g^{(q)}) = X^{a^{(q)}}$, we have

$$|a^{(q)}| \le \delta(q), \qquad \delta(q) := 2^{q+1} d_0. \tag{4.14b}$$

Proof. The bound (4.14a) holds at $q = 0$. If it holds at q, then, for $M_{ij} = \mathrm{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$ and $S(g_i, g_j) \neq 0$,

$$\deg S(g_i, g_j) \le \deg M_{ij} \le \deg \mathrm{LM}(g_i) + \deg \mathrm{LM}(g_j) \le 2^{q+1} d_0. \tag{4.14c}$$

Here $\deg g = \deg \mathrm{LM}(g)$ because the order is degree–lexicographic. By Lemma 4.4, division does not increase degree. Hence $\deg g^{(q)} \le 2^{q+1} d_0$, proving both (4.14b) and the induction step for (4.14a). □

Definition 4.12 (Counter sequences)**.** Fix a nondecreasing rule $\delta : \mathbb{N} \to \mathbb{N}$ of the kind just specified. For $k : \mathbb{N}$, a *k-counter state* is a tuple

$$\mathcal{C} = (c_k, \dots, c_0; q), \qquad c_k, \dots, c_0, q : \mathbb{N}. \tag{4.15a}$$

Write $\mathbf{c} = (c_k, \dots, c_0)$, and let $\mathbf{e}_i : \mathbb{N}^{k+1}$ be defined by

$$(\mathbf{e}_i)_j := \begin{cases} 1, & j = i, \\ 0, & j \neq i, \end{cases} \qquad 0 \le i, j \le k.$$

Define the relation $\longrightarrow_{\delta,k}$ by

$$(\mathbf{c}; q) \longrightarrow_{\delta,k} (\mathbf{c} - \mathbf{e}_0; q + 1) \qquad (c_0 > 0), \tag{4.15b}$$

and, for $1 \le i \le k$, $c_i > 0$, and $h_{\mathrm{ctr}} \in \{0, \dots, \delta(q)\}$, by

$$(\mathbf{c}; q) \longrightarrow_{\delta,k} (\mathbf{c} - \mathbf{e}_i + h_{\mathrm{ctr}}\mathbf{e}_{i-1}; q + 1). \tag{4.15c}$$

A *k-counter sequence* is a finite sequence

$$\sigma = (\mathcal{C}^{(0)}, \dots, \mathcal{C}^{(t)}), \qquad \mathcal{C}^{(u)} \longrightarrow_{\delta,k} \mathcal{C}^{(u+1)} \quad (0 \le u < t).$$

Its length and terminal state are defined by

$$\ell(\sigma) := t, \qquad \mathrm{end}(\sigma) := \mathcal{C}^{(t)}.$$

Definition 4.13 (Recursive bounds)**.** We define a family of functions

$$\gamma_{\delta,k} : \mathbb{N}^{k+1} \times \mathbb{N} \longrightarrow \mathbb{N} \qquad (k \ge 0)$$

by induction on k. For $k = 0$, set

$$\gamma_{\delta,0}(c_0; q) := c_0. \tag{4.15d}$$

For $k \ge 1$, assume that $\gamma_{\delta,k-1}$ has been defined. Write $\mathbf{c} = (c_{k-1}, \dots, c_0)$ and $m = c_k$, and use the abbreviations

$$\gamma_{\delta,k-1}(\mathbf{c}; q) := \gamma_{\delta,k-1}(c_{k-1}, \dots, c_0; q),$$
$$\gamma_{\delta,k}(m, \mathbf{c}; q) := \gamma_{\delta,k}(m, c_{k-1}, \dots, c_0; q).$$

We define $\gamma_{\delta,k}(m, \mathbf{c}; q)$ by recursion on m, for all $\mathbf{c} : \mathbb{N}^k$ and $q : \mathbb{N}$. Let $\gamma_* := \gamma_{\delta,k-1}(\mathbf{c}; q)$, and let $\mathcal{P}_{\delta,k-1}(\mathbf{c}; q)$ denote the finite list of $(k-1)$-counter sequences with initial state $(\mathbf{c}; q)$ and length at most γ_*, generated by the finite transition choices. For $\sigma \in \mathcal{P}_{\delta,k-1}(\mathbf{c}; q)$, let

$$\ell_\sigma := \ell(\sigma), \qquad (\mathbf{b}_\sigma; s_\sigma) := \mathrm{end}(\sigma), \qquad s_\sigma = q + \ell_\sigma. \tag{4.15e}$$

Here $\mathbf{b}_\sigma = (b_{k-1,\sigma}, \dots, b_{0,\sigma}) : \mathbb{N}^k$. With $\mathbf{e}_{k-1} := (1, 0, \dots, 0) : \mathbb{N}^k$, define

$$\gamma_{\delta,k}(0, \mathbf{c}; q) := \gamma_*,$$

and, for $m \ge 1$,

$$\gamma_{\delta,k}(m, \mathbf{c}; q) := \max\Bigg\{ \gamma_*, \max_{\substack{\sigma \in \mathcal{P}_{\delta,k-1}(\mathbf{c};q) \\ 0 \le h_{\mathrm{ctr}} \le \delta(s_\sigma)}} \Big[\ell_\sigma + 1 + \gamma_{\delta,k}(m - 1, \mathbf{b}_\sigma + h_{\mathrm{ctr}}\mathbf{e}_{k-1}; s_\sigma + 1) \Big] \Bigg\}. \tag{4.15f}$$

Remark 4.14. The family $\mathcal{P}_{\delta,k-1}(\mathbf{c};q)$ contains the length-zero sequence $((\mathbf{c};q))$ and need not consist of maximal sequences. Its defining length bound gives

$$\#\mathcal{P}_{\delta,k-1}(\mathbf{c};q) \le \sum_{t=0}^{\gamma_*} \big[1+(k-1)(\delta(q+\gamma_*)+1)\big]^t :$$

at each stage there is at most one choice in (4.15b), and at most $\delta(q+\gamma_*)+1$ choices for each of the $k-1$ indices in (4.15c). Thus the recursion uses only bounded finite families.

Lemma 4.15 (Recursive finite stopping bound)**.** *The integer $\gamma_{\delta,k}(c_k,\dots,c_0;q)$ is computable by a finite procedure. Every k-counter sequence τ with initial state $(c_k,\dots,c_0;q)$ satisfies*

$$\ell(\tau) \le \gamma_{\delta,k}(c_k,\dots,c_0;q).$$

Proof. Induct on k, and then on $m := c_k$. For $k=0$, each relation (4.15b) decreases c_0 by one, so $\ell(\tau) \le c_0$. For $k \ge 1$, write the initial state as $(m,\mathbf{c};q)$ and let $\gamma_* := \gamma_{\delta,k-1}(\mathbf{c};q)$. By the induction hypothesis on k, every $(k-1)$-counter sequence with the indicated initial state has length at most γ_*, so it occurs in the explicitly bounded list $\mathcal{P}_{\delta,k-1}(\mathbf{c};q)$. The counting bound above makes this list finite. Each recursive call either decreases k, or leaves k unchanged and decreases m. Hence the recursion terminates.

If the first coordinate remains constant throughout τ, deleting that coordinate gives a $(k-1)$-counter sequence, so $\ell(\tau) \le \gamma_*$. Otherwise, let t be the index of the first relation that decreases this coordinate. The preceding t relations, with the constant first coordinate deleted, form a sequence $\sigma \in \mathcal{P}_{\delta,k-1}(\mathbf{c};q)$. The next state is

$$(m-1,\mathbf{b}_\sigma + h_{\mathrm{ctr}}\mathbf{e}_{k-1}; s_\sigma+1), \qquad 0 \le h_{\mathrm{ctr}} \le \delta(s_\sigma).$$

The induction hypothesis on m gives

$$\ell(\tau) \le \ell_\sigma + 1 + \gamma_{\delta,k}(m-1,\mathbf{b}_\sigma + h_{\mathrm{ctr}}\mathbf{e}_{k-1}; s_\sigma+1) \le \gamma_{\delta,k}(m,\mathbf{c};q).$$

□

Lemma 4.16 (Finite Dickson bound)**.** *Every δ-controlled divisibility-avoiding sequence in $\mathbb{N}^n$ has length at most the computable integer*

$$R_{\delta,n} := \gamma_{\delta,n}(1,0,\dots,0;0). \tag{4.16}$$

Proof. Let $a^{(0)},\dots,a^{(\ell-1)}$ satisfy (4.12)–(4.13), and write $[n] := \{1,\dots,n\}$. For $\mathcal{J} \subseteq [n]$ and $b : \mathbb{N}^n$, define the coordinate slice $\mathcal{S}(\mathcal{J},b)$ by

$$a : \mathcal{S}(\mathcal{J},b) \iff (a:\mathbb{N}^n) \wedge \bigwedge_{j\in[n]\setminus\mathcal{J}} (a_j = b_j), \qquad \dim \mathcal{S}(\mathcal{J},b) := |\mathcal{J}|.$$

If $a^{(q)} : \mathcal{S}(\mathcal{J},b)$, then, for every $a : \mathbb{N}^n$,

$$\big(a:\mathcal{S}(\mathcal{J},b) \wedge \neg(a^{(q)} \le a)\big) \iff \bigvee_{j\in\mathcal{J}} \bigvee_{0\le t<a_j^{(q)}} \big(a:\mathcal{S}(\mathcal{J},b) \wedge a_j = t\big).$$

An empty conjunction is true and an empty disjunction is false.

Construct indexed lists of coordinate slices

$$\mathcal{F}_q = (\mathcal{S}_\lambda^{(q)})_{\lambda=1}^{m_q} \qquad (0 \le q \le \ell)$$

with the covering property

$$\bigvee_{\lambda=1}^{m_q} (a^{(k)} : \mathcal{S}_\lambda^{(q)}) \qquad (q \le k < \ell).$$

Let $\mathcal{F}_0 = (\mathcal{S}([n], 0))$, where $\mathcal{S}([n], 0) = \mathbb{N}^n$. For $q < \ell$, let λ_q be the least index such that $a^{(q)} : \mathcal{S}_{\lambda_q}^{(q)}$, and write $\mathcal{S}_{\lambda_q}^{(q)} = \mathcal{S}(\mathcal{J}_q, b_q)$. List the finitely many pairs

$$\mathcal{A}_q := \{(j, t) : j \in \mathcal{J}_q,\ 0 \le t < a_j^{(q)}\}.$$

For such a pair, let $b_q^{j,t}$ be b_q with its j-th entry replaced by t, and define the slice

$$\mathcal{S}_{q;j,t} := \mathcal{S}(\mathcal{J}_q \setminus \{j\}, b_q^{j,t}).$$

Define

$$\mathcal{F}_{q+1} := (\mathcal{S}_\lambda^{(q)})_{\substack{1 \le \lambda \le m_q \\ \lambda \ne \lambda_q}} \sqcup (\mathcal{S}_{q;j,t})_{(j,t) \in \mathcal{A}_q},$$

where $\sqcup$ denotes concatenation of finite lists, with the second list ordered lexicographically by (j, t). We verify the covering property for $\mathcal{F}_{q+1}$. Fix k with $q < k < \ell$. By the covering property of $\mathcal{F}_q$, the point $a^{(k)}$ belongs to at least one slice of that list. If it belongs to a slice with index different from λ_q, that slice is retained in $\mathcal{F}_{q+1}$. It therefore suffices to consider the case $a^{(k)} : \mathcal{S}(\mathcal{J}_q, b_q)$. Since $a^{(q)}$ also belongs to this slice, its fixed coordinates give

$$a_j^{(k)} = (b_q)_j = a_j^{(q)} \qquad (j \in [n] \setminus \mathcal{J}_q).$$

On the other hand, (4.13) gives $a^{(q)} \not\le a^{(k)}$, so some coordinate satisfies $a_j^{(k)} < a_j^{(q)}$. This strict inequality cannot hold at a fixed coordinate, so $j \in \mathcal{J}_q$. Set $t := a_j^{(k)}$; then

$$(j, t) \in \mathcal{A}_q, \qquad a^{(k)} : \mathcal{S}(\mathcal{J}_q \setminus \{j\}, b_q^{j,t}) = \mathcal{S}_{q;j,t}.$$

Indeed, the old fixed coordinates still agree with b_q, and the newly fixed coordinate is $a_j^{(k)} = t$. Thus every point with $q < k < \ell$ is covered by $\mathcal{F}_{q+1}$. If $\mathcal{J}_q = \varnothing$, the removed slice is the singleton $\{a^{(q)}\}$; it contains no later point, by (4.13), so no replacement slice is needed.

Define

$$c_k(q) := \#\{\lambda : 1 \le \lambda \le m_q, \quad \dim \mathcal{S}_\lambda^{(q)} = k\} \quad (0 \le k \le n), \qquad \mathbf{c}(q) := (c_n(q), \dots, c_0(q)).$$

Then $\mathbf{c}(0) = (1, 0, \dots, 0)$. At the q-th replacement, let $k := |\mathcal{J}_q|$ and

$$h_q := \#\mathcal{A}_q = \sum_{j \in \mathcal{J}_q} a_j^{(q)} \le |a^{(q)}| \le \delta(q). \tag{4.16a}$$

One k-dimensional slice is removed; if $k > 0$, exactly h_q slices of dimension $k - 1$ are added. If $k = 0$, the family $\mathcal{A}_q$ is empty. Thus

$$\mathbf{c}(q+1) = \begin{cases} \mathbf{c}(q) - \mathbf{e}_0, & k = 0, \\ \mathbf{c}(q) - \mathbf{e}_k + h_q \mathbf{e}_{k-1}, & k > 0. \end{cases}$$

Since $c_k(q) > 0$ and $0 \le h_q \le \delta(q)$,

$$(\mathbf{c}(q); q) \longrightarrow_{\delta,n} (\mathbf{c}(q+1); q+1).$$

Thus

$$((\mathbf{c}(0); 0), \dots, (\mathbf{c}(\ell); \ell))$$

is an n-counter sequence of length ℓ with initial state $(1, 0, \dots, 0; 0)$. By Lemma 4.15,

$$\ell \le \gamma_{\delta,n}(1, 0, \dots, 0; 0) = R_{\delta,n}.$$

□

Theorem 4.17 (Finite Gröbner basis construction)**.** *Let*

$$F = (f_1, \dots, f_m)^{\mathsf{t}}, \qquad f_j : L[X_1, \dots, X_n].$$

A finite procedure produces a monic Gröbner basis G of $\langle F\rangle$, representations (4.8) with the leading monomial bound (4.8a), and polynomial matrices A, B satisfying

$$G = \mathsf{A}F, \qquad F = \mathsf{B}G. \tag{4.17}$$

It decides whether $1 : \langle F\rangle$ and, in that case, produces an identity $1 = \sum_j h_j f_j$.

Proof. Start with the monic normalizations of the nonzero entries of F. Successively reduce each unexamined S-polynomial by the current tuple, adjoining the monic normalization of every nonzero remainder and retaining the expressions in terms of F. Let s_0 be the number of nonzero entries of F, and let d be their maximum degree, with $d = 0$ if $s_0 = 0$. Let

$$d_0 := \max(1, d), \qquad \delta(q) := 2^{q+1} d_0, \qquad R := R_{\delta,n},$$

and

$$n_{\mathrm{row}} := s_0 + R, \qquad n_{\mathrm{pair}} := \binom{n_{\mathrm{row}}}{2}. \tag{4.18}$$

These bounds depend only on the initial data.

For the successively adjoined polynomials $g^{(q)}$, write $\mathrm{LM}(g^{(q)}) = X^{a^{(q)}}$. Lemma 4.11 and complete reduction give

$$|a^{(q)}| \le \delta(q), \qquad a^{(i)} \not\le a^{(q)} \quad (i < q).$$

Lemma 4.16 therefore bounds the number of additions by R. There are at most n_{row} polynomials and n_{pair} distinct pairs. Each pair is examined once, and every division is finite by Lemma 4.4; hence this construction terminates. Moreover, Lemma 4.9 gives at every addition

$$\mathrm{LM}(g) \nmid \mathrm{LM}(g^{(q)}) \qquad (g \text{ an entry of } G_{\mathrm{old}}). \tag{4.19}$$

If a nonzero remainder r is obtained from a pair, its division identity is $S(g_i, g_j) = \sum_\kappa \mathfrak{q}_\kappa g_\kappa + r$. Every nonzero product on the right, including r, has leading monomial strictly smaller than M_{ij}. Replacing r by its scalar multiple of the newly adjoined monic polynomial gives (4.8). Thus every examined pair admits such a representation, which remains valid after further additions. Theorem 4.6 shows that the final G is a Gröbner basis.

Every adjoined polynomial is a combination of earlier polynomials; retaining these identities gives $G = \mathsf{A}F$. The normalized nonzero entries of F remain in G, giving $F = \mathsf{B}G$. Finally, $1 : \langle F\rangle = \langle G\rangle$ if and only if some $\mathrm{LM}(g)$ divides 1, by Theorem 4.6. This is equivalent to the occurrence of a constant polynomial in G; its monic normalization and its expression in F give the required identity. □

4.4 Homogenization and elimination

Definition 4.18 (Homogenization)**.** Let nonzero $p(X) = \sum_\alpha c_\alpha X^\alpha$ have total degree d. With a new variable X_0, define

$$p^{\mathrm{h}}(X_0, X) := X_0^d p(X_1/X_0, \dots, X_n/X_0) = \sum_\alpha c_\alpha X_0^{d-|\alpha|} X^\alpha. \tag{4.20}$$

Every monomial of p^{h} has total degree d, and

$$p^{\mathrm{h}}(1, X) = p(X). \tag{4.20a}$$

Define $0^{\mathrm{h}} := 0$.

Lemma 4.19 (Homogeneous degree–lexicographic elimination)**.** *Let* $F = (f_1, \dots, f_m) \subset K[S, Y]$, *let*

$$\widetilde{F} := (f_1^{\mathrm{h}}, \dots, f_m^{\mathrm{h}}) \subset K[X_0, S, Y], \tag{4.21}$$

and order the variables

$$Y_1 \succ \cdots \succ Y_v \succ X_0 \succ S_1 \succ \cdots \succ S_e \tag{4.22}$$

in degree–lexicographic order. If G *is the Gröbner basis of* $\langle \widetilde{F} \rangle$ *supplied by Theorem 4.17, then every* $g \in G$ *is homogeneous and*

$$\big[\forall p : K[S],\ ((p : \langle F \rangle) \Rightarrow p = 0)\big] \quad \Longleftrightarrow \quad \bigwedge_{g \in G} \neg\big(g : K[X_0, S]\big). \tag{4.23}$$

If an entry g *of* G *is of type* $K[X_0, S]$, *then*

$$g(1, S) : K[S], \quad g(1, S) \neq 0, \qquad g(1, S) : \langle F \rangle. \tag{4.24}$$

Proof. The generators f_j^{h} are homogeneous. If g_i, g_j are homogeneous, both summands of $S(g_i, g_j)$ have total degree

$$\deg \operatorname{lcm}(\mathrm{LM}(g_i), \mathrm{LM}(g_j)).$$

In division of a homogeneous polynomial, (4.4)–(4.6) show that each subtraction and every remainder term has that same total degree. Induction over the pair queue therefore proves that every element of G is homogeneous.

Suppose first that an entry g of G is of type $K[X_0, S]$. Write its homogeneous expansion as

$$g = \sum_{\alpha, i} c_{\alpha i} X_0^i S^\alpha, \qquad |\alpha| + i = d. \tag{4.25}$$

For each α, homogeneity fixes $i = d - |\alpha|$; hence setting $X_0 = 1$ cannot cancel distinct terms, and $g(1, S) \neq 0$. From the identity

$$g = \sum_{j=1}^{m} a_j(X_0, S, Y) f_j^{\mathrm{h}}$$

one obtains

$$g(1, S) = \sum_{j=1}^{m} a_j(1, S, Y) f_j(S, Y), \tag{4.26}$$

proving one implication of (4.23) and (4.24).

Conversely, let a supplied nonzero $p : K[S]$ have a representation

$$p(S) = \sum_{j=1}^{m} h_j(S, Y) f_j(S, Y). \tag{4.27}$$

Define

$$d := \max\Big(\deg p,\ \max_{j : h_j f_j \neq 0} (\deg h_j + \deg f_j)\Big). \tag{4.28}$$

Homogenizing every summand to the common degree d gives the finite identity

$$X_0^{d - \deg p} p^{\mathrm{h}}(X_0, S) = \sum_{j : h_j f_j \neq 0} X_0^{d - \deg h_j - \deg f_j} h_j^{\mathrm{h}}(X_0, S, Y) f_j^{\mathrm{h}}(X_0, S, Y). \tag{4.29}$$

The left side is a nonzero polynomial of type $K[X_0, S]$ with a representation in terms of $\widetilde{F}$. Theorem 4.6 supplies $g \in G$ such that

$$\mathrm{LM}(g) \mid \mathrm{LM}\Big(X_0^{d - \deg p} p^{\mathrm{h}}\Big). \tag{4.30}$$

Thus $\mathrm{LM}(g)$ contains no Y-variable. If another monomial of g contained a Y-variable, then it would have the same total degree as $\mathrm{LM}(g)$, and the variable order (4.22) would make it larger than $\mathrm{LM}(g)$. This is impossible. Hence $g : K[X_0, S]$, proving the other implication of (4.23). □

5 From a proper ideal to a finite quotient algebra

We construct finite coordinate algebras and their quotients, then obtain the required quotient data from a proper polynomial ideal type.

Definition 5.1 (Finite algebra type)**.** A *finite L-algebra type* A is specified by a finite coordinate basis $(e_1, \dots, e_s)$, the coordinates of a unit 1, and a multiplication table

$$e_i e_j = \sum_{k=1}^{s} c_{ij}^k e_k.$$

An object $x : A$ is a tuple $(x_1, \dots, x_s) : L^s$, written $x = \sum_i x_i e_i$. Addition is coordinatewise; multiplication uses the table. The data must satisfy the unit, commutativity, and associativity identities, checked on the basis. Here *finite* means finite-dimensional with these data supplied.

Remark 5.2 (Kernels and images in coordinates). For a finite matrix C over L, $\ker \mathsf{C}$ denotes the solution type of $\mathsf{C}v = 0$. Row reduction gives an independent list $(n_1, \dots, n_{\ell_{\ker}})$ expressing each solution as $v = \sum_j t_j n_j$ with unique coefficients. The image is represented by a column basis of C; row reduction tests membership and computes coordinates.

Proposition 5.3 (Quotients of finite coordinate algebras)**.** *Let A be a finite K-algebra type with basis $(e_1, \dots, e_s)$. Suppose independent vectors $(n_1, \dots, n_{\ell_{\mathrm{id}}})$ are supplied, together with expressions of each $e_i n_j$ as a K-linear combination of the n_k. These data specify an ideal type $\mathfrak{n} = \langle n_1, \dots, n_{\ell_{\mathrm{id}}} \rangle_A$ and a finite quotient-algebra type $A/\mathfrak{n}$ of dimension $s - \ell_{\mathrm{id}}$.*

Proof. For a supplied $x : A$, membership in $\mathfrak{n}$ means an identity $x = \sum_j a_j n_j$ with $a_j : A$. The supplied multiplication identities show that these are exactly the K-linear combinations of the n_j; thus membership is decided by finite row reduction. Extend $(n_1, \dots, n_{\ell_{\mathrm{id}}})$ to a basis $(n_1, \dots, n_{\ell_{\mathrm{id}}}, b_1, \dots, b_{d_{\mathrm{quot}}})$ of A, where $d_{\mathrm{quot}} = s - \ell_{\mathrm{id}}$. For $x : A$, let $[x]_{\mathfrak{n}}$ be its last d_{quot} coordinates in this basis. Define $A/\mathfrak{n}$ to be the type of these coordinate tuples, with

$$[x]_{\mathfrak{n}} + [y]_{\mathfrak{n}} = [x + y]_{\mathfrak{n}}, \qquad [x]_{\mathfrak{n}}[y]_{\mathfrak{n}} = [xy]_{\mathfrak{n}}.$$

Representatives have the same coordinates exactly when their difference is of ideal type $\mathfrak{n}$. Hence the operations are independent of representatives and inherit the algebra identities of A. The quotient basis is $([b_1]_{\mathfrak{n}}, \dots, [b_{d_{\mathrm{quot}}}]_{\mathfrak{n}})$, its unit is $[1]_{\mathfrak{n}}$, and its multiplication table consists of the last d_{quot} coordinates of the products $b_i b_j$. Another complement gives an isomorphic algebra by a finite change of basis. □

Definition 5.4 (Zero-dimensional ideal data)**.** Let $J = \langle F \rangle$ be an ideal type in $L[Y_1, \dots, Y_\ell]$. The finite data specifying that J is *zero-dimensional* are, for each k, a monic polynomial

$$h_k(Y_k) = Y_k^{d_k} + \sum_{i=0}^{d_k - 1} a_{ki} Y_k^i, \qquad d_k \geq 0,$$

together with a representation of h_k in terms of F. If J is proper, necessarily $d_k \geq 1$. For $\ell = 0$, the relation list is empty.

The next lemma constructs the quotient type from these data.

Lemma 5.5 (Standard-monomial quotient construction)**.** *Let J be an ideal type in $L[Y_1, \dots, Y_\ell]$ with the data of Definition 5.4. Finite Gröbner division constructs a finite L-algebra type, denoted by $L[Y]/J$, whose coordinate basis is represented by the standard monomials. It is nonzero if J is proper.*

Proof. Compute a monic Gröbner basis G by Theorem 4.17. Since each supplied h_k is of ideal type J with $\mathrm{LM}(h_k) = Y_k^{d_k}$, some $\mathrm{LM}(g)$ divides this pure power. Consequently every standard monomial Y^α satisfies $0 \le \alpha_k < d_k$. Inspect this finite box and retain the monomials not divisible by any $\mathrm{LM}(g)$, obtaining $(M_1, \dots, M_s)$. When $\ell = 0$, the sole candidate is 1, subject to the same test.

An object of the proposed quotient type is an s-tuple over L. For a supplied $f : L[Y]$, define $[f]_J$ as the coefficient tuple of its completely reduced remainder in $(M_1, \dots, M_s)$. Theorem 4.6 gives

$$[f]_J = [g]_J \quad \Longleftrightarrow \quad f - g : J.$$

Every tuple $(c_1, \dots, c_s)$ is represented by $\sum_i c_i M_i$, whose remainder is itself. Thus the coordinate basis is

$$([M_1]_J, \dots, [M_s]_J).$$

Define addition and multiplication by

$$[f]_J + [g]_J = [f + g]_J, \qquad [f]_J[g]_J = [fg]_J. \tag{5.0}$$

Changing representatives changes the sums and products by elements of the ideal type J, so both operations are well-defined and inherit the algebra identities from finite polynomial arithmetic. The unit is $[1]_J$, and division of the s^2 products $M_i M_j$ gives the finite multiplication table required by Definition 5.1. Properness gives $[1]_J \neq 0$. We omit the subscript on $[f]_J$ when the ideal is fixed. □

Remark 5.6 (Finite-dimensional quotients). Definition 5.4 supplies finite-dimensionality data before the quotient is used. Conversely, a finite coordinate presentation yields the required relations by linear dependence among powers of each coordinate. For proper ideals, this is the usual zero-dimensional condition. Finiteness refers to coordinate length, not the number of values; the quotient need not be a field.

Definition 5.7 (Coordinate-independent set)**.** For a proper ideal type I in $K[X_1, \dots, X_n]$, a coordinate subset $S \subseteq \{X_1, \dots, X_n\}$ is independent modulo I if the following predicate holds:

$$\mathrm{Ind}_I(S) \quad :\Longleftrightarrow \quad \forall f : K[S],\ ((f : I) \Rightarrow f = 0). \tag{5.1}$$

Remark 5.8 (Elimination and coordinate selection). Lemma 4.19 decides $\mathrm{Ind}_I(S)$ by variable-occurrence tests on a homogeneous Gröbner basis. If it fails, the lemma gives a nonzero polynomial of type $K[S]$ and its generator representation in I. A maximal independent subset is chosen from the 2^n coordinate subsets, ordered by their indicator tuples.

Theorem 5.9 (Finite proper zero-dimensional specialization)**.** *Let $I = \langle F \rangle$ be a proper ideal type in $K[X]$. A finite procedure permutes the variables and writes them as*

$$X = (S, Y), \qquad S = (S_1, \dots, S_e), \quad Y = (Y_1, \dots, Y_\ell), \tag{5.2}$$

and produces a point $a : K^e$ such that

$$J_a := \langle f_1(a, Y), \dots, f_m(a, Y) \rangle \tag{5.3}$$

is proper and zero-dimensional. It also produces a monic Gröbner basis of J_a, the two matrices expressing this basis and the original generators in terms of each other, and the specializations of (5.16). If $\ell = 0$, then $I = 0$.

Proof. Enumerate the 2^n coordinate subsets. For every S, homogenize F and apply the degree–lexicographic elimination test of Lemma 4.19; this decides

$$\mathrm{Ind}_I(S). \tag{5.4}$$

The empty coordinate list satisfies (5.4): a supplied nonzero constant of type I could be inverted, giving $1 : I$. Choose the first inclusion-maximal S satisfying (5.4), and let Y be its complement.

If $\ell = 0$, then $S = X$ and (5.4) gives $I = 0$. Let $a = (0, \dots, 0)$. Then J_a is the zero ideal type in K, with the empty Gröbner basis and zero transformation matrices. Hence assume $\ell > 0$.

For $1 \le k \le \ell$, maximality of S gives

$$\neg \operatorname{Ind}_I(S \cup \{Y_k\}). \tag{5.5}$$

Apply Lemma 4.19 with retained variables (S, Y_k) and eliminated variables $Y \setminus \{Y_k\}$. It supplies a first homogeneous row

$$\widetilde{h}_k(X_0, S, Y_k) : K[X_0, S, Y_k], \qquad \widetilde{h}_k \neq 0, \qquad \widetilde{h}_k : \langle \widetilde{F} \rangle.$$

Dehomogenize its representation at $X_0 = 1$. Equation (4.24) gives

$$\begin{aligned} h_k(S, Y_k) := \widetilde{h}_k(1, S, Y_k) &= \sum_{i=0}^{d_k} c_{ki}(S) Y_k^i \\ &= \sum_{j=1}^{m} u_{kj}(S, Y) f_j(S, Y), \\ c_{k,d_k}(S) \neq 0, \qquad d_k \ge 1. & \end{aligned} \tag{5.6}$$

Indeed, $d_k = 0$ would give a nonzero $h_k : K[S]$ with $h_k : I$, contradicting (5.4).

Let

$$L := K(S), \qquad I_L := \langle f_1, \dots, f_m \rangle_{L[Y]}. \tag{5.7}$$

Division of (5.6) by $c_{k,d_k}(S)$ gives

$$\widehat{h}_k := c_{k,d_k}(S)^{-1} h_k = Y_k^{d_k} + \sum_{i=0}^{d_k - 1} a_{ki}(S) Y_k^i : I_L. \tag{5.8}$$

These are the finite dimensionality data required by Definition 5.4. In polynomial congruence notation,

$$Y_k^{d_k} \equiv - \sum_{i=0}^{d_k - 1} a_{ki}(S) Y_k^i \pmod{I_L}. \tag{5.9}$$

Induction on the exponent of Y_k, followed by induction on k, reduces every monomial, modulo I_L, to an L-linear combination of elements of the finite set

$$\mathcal{M} := \left\{ Y_1^{\alpha_1} \cdots Y_\ell^{\alpha_\ell} : 0 \le \alpha_k < d_k \ (1 \le k \le \ell) \right\}, \qquad |\mathcal{M}| = \prod_{k=1}^{\ell} d_k. \tag{5.10}$$

Thus, by Lemma 5.5,

$$A_{\mathrm{loc}} := L[Y]/I_L \tag{5.11}$$

is finite-dimensional over L.

We prove that the ideal type I_L is proper. Suppose that

$$1 = \sum_{j=1}^{m} h_j(S, Y) f_j(S, Y), \qquad h_j : L[Y]. \tag{5.12}$$

Write every coefficient occurring in the finite tuple $(h_1, \dots, h_m)$ as

$$\frac{u_{j\alpha}(S)}{v_{j\alpha}(S)}, \qquad v_{j\alpha}(S) \neq 0,$$

and define

$$b(S) := \prod_{j,\alpha} v_{j\alpha}(S) \neq 0, \qquad \widetilde{h}_j := bh_j : K[S,Y]. \tag{5.13}$$

Multiplication of (5.12) by b gives

$$0 \neq b(S) = \sum_{j=1}^{m} \widetilde{h}_j(S,Y) f_j(S,Y) : I, \tag{5.14}$$

contrary to (5.4). Hence I_L is proper and $A_{\mathrm{loc}} \neq 0$.

Apply Theorem 4.17 over L to obtain a monic Gröbner basis $G = (g_1, \ldots, g_t)$ with the identities

$$g_\kappa = \sum_{j=1}^{m} a_{\kappa j}(S,Y) f_j, \qquad f_j = \sum_{\kappa=1}^{t} b_{j\kappa}(S,Y) g_\kappa, \tag{5.15}$$

and, for every $\iota < \kappa$, a representation

$$S(g_\iota, g_\kappa) = \sum_{i=1}^{t} \mathfrak{q}_{\iota\kappa i}(S,Y) g_i, \qquad \mathfrak{q}_{\iota\kappa i} g_i \neq 0 \implies \mathrm{LM}(\mathfrak{q}_{\iota\kappa i} g_i) \prec \mathrm{lcm}(\mathrm{LM}(g_\iota), \mathrm{LM}(g_\kappa)). \tag{5.16}$$

Let $\mathcal{D}$ be the finite set of all nonzero denominators occurring in G, (5.15), and (5.16). Define

$$\rho(S) := \prod_{u \in \mathcal{D}} u(S), \qquad \prod_{u \in \varnothing} u := 1, \qquad d := \deg \rho. \tag{5.17}$$

The product of finitely many nonzero polynomials is nonzero, since their leading coefficients multiply; hence $\rho \neq 0$. By Lemma 3.2, lexicographic testing of

$$\{0, 1, \ldots, d\}^e \tag{5.18}$$

finds $a = (a_1, \ldots, a_e)$ with $\rho(a) \neq 0$.

For $M_\kappa := \mathrm{LM}(g_\kappa)$, monicity gives a finite expression

$$g_\kappa(S,Y) = M_\kappa + \sum_{Y^\alpha \prec M_\kappa} h_{\kappa\alpha}(S) Y^\alpha. \tag{5.19}$$

Since all denominators are nonzero at a,

$$g_\kappa(a,Y) = M_\kappa + \sum_{Y^\alpha \prec M_\kappa} h_{\kappa\alpha}(a) Y^\alpha, \qquad \mathrm{LM}(g_\kappa(a,Y)) = M_\kappa. \tag{5.20}$$

Since the denominators are nonzero at a, evaluation preserves sums and products, so the rational-function identities specialize. In particular, (5.15) gives

$$g_\kappa(a,Y) : J_a, \qquad f_j(a,Y) : \langle g_1(a,Y), \ldots, g_t(a,Y) \rangle,$$

and therefore

$$J_a = \langle g_1(a,Y), \ldots, g_t(a,Y) \rangle. \tag{5.21}$$

Specializing (5.16), together with (5.20), gives representations (4.8) with the leading monomial bound (4.8a). Hence $G(a,Y)$ is a Gröbner basis of J_a.

Because I_L is proper, $M_\kappa \neq 1$ for every κ. If $1 : J_a$, the Buchberger criterion applied to a $G(a,Y)$-combination of 1 would give

$$M_\kappa \mid \mathrm{LM}(1) = 1$$

for some κ, hence $M_\kappa = 1$, a contradiction. Thus J_a is proper.

Finally, (5.8) and the Gröbner property over L give, for every k, an index $\kappa(k)$ such that

$$\mathrm{LM}(g_{\kappa(k)}) \mid \mathrm{LM}(\widehat{h}_k) = Y_k^{d_k}.$$

A monomial dividing a pure power of Y_k is a pure power of Y_k; hence

$$M_{\kappa(k)} = Y_k^{e_k}, \qquad 1 \le e_k \le d_k. \tag{5.22}$$

Equation (5.20) preserves (5.22). Therefore every standard monomial Y^α of $G(a, Y)$ satisfies

$$0 \le \alpha_k < e_k \quad (1 \le k \le \ell), \tag{5.23}$$

so there are at most $D := \prod_k e_k$ standard monomials. List these monomials and compute the remainder coordinate vectors of $1, Y_k, \ldots, Y_k^D$ for each k. Finite row reduction finds a nontrivial linear relation among these $D+1$ vectors. Normalize its highest nonzero coefficient. The result is a monic polynomial in Y_k with zero remainder; the recorded division identities express it in terms of the generators of J_a. Its degree is positive because J_a is proper. These are the finite dimensionality data of Definition 5.4, so J_a is zero-dimensional and Lemma 5.5, with $L = K$, constructs the quotient type $K[Y]/J_a$. □

6 Traces, nilpotents, and reduced quotients

Definition 6.1 (Trace and nilpotents)**.** Let A be a finite K-algebra type as in Definition 5.1. For $x = \sum_i x_i e_i : A$, let

$$M_x : A \longrightarrow A, \qquad y \longmapsto xy$$

denote multiplication by x. In the supplied basis its matrix, also denoted by M_x, has entries

$$(M_x)_{kj} = \sum_{i=1}^{s} x_i c_{ij}^k.$$

For a square matrix $\mathsf{C} = (\mathsf{C}_{ij})_{1 \le i,j \le s}$, define

$$\mathrm{Tr}(\mathsf{C}) := \sum_{i=1}^{s} \mathsf{C}_{ii}.$$

Define

$$\mathrm{Tr}_A(x) := \mathrm{Tr}(M_x). \tag{6.1}$$

An element x is nilpotent if $x^q = 0$ for some positive integer q. Write

$$x : \mathrm{Nil}(A) \quad \Longleftrightarrow \quad (x : A) \ \wedge \ (x \text{ is nilpotent}).$$

The algebra A is reduced if its only nilpotent element is zero, equivalently, if $\mathrm{Nil}(A) = 0$. A *minimal polynomial* of $x : A$ is the least-degree monic polynomial $m_x(X_0) : K[X_0]$ satisfying $m_x(x) = 0$; it is found by the first linear dependence among $1, x, \ldots, x^{\dim_K A}$.

Theorem 6.2 (Trace radical)**.** *Let $A \neq 0$ be a finite commutative algebra over the characteristic-zero field K. Define the bilinear form*

$$\langle x, y \rangle_A := \mathrm{Tr}_A(xy). \tag{6.2}$$

For a supplied $x : A$ and the coordinate basis $(e_1, \ldots, e_s)$,

$$\bigwedge_{j=1}^{s} \big(\langle x, e_j \rangle_A = 0\big) \quad \Longleftrightarrow \quad x : \mathrm{Nil}(A). \tag{6.3}$$

Thus one finite row reduction on the Gram matrix of (6.2) *computes a basis of* $\mathrm{Nil}(A)$*, also a finite generating list of this ideal type, and*

$$B := A/\operatorname{Nil}(A) \tag{6.4}$$

is a finite nonzero reduced K*-algebra.*

See Appendix A for the proof.

Remark 6.3 (Applying the coordinate quotient to the nilradical). By Theorem 6.2, row reduction of $\Gamma = (\mathrm{Tr}(M_{e_i e_j}))$ gives a basis $(n_1, \ldots, n_{\ell_{\mathrm{nil}}})$ of the ideal type $\mathrm{Nil}(A)$. Expressing each $e_i n_j$ in this basis supplies the data for Proposition 5.3, which constructs the quotient basis and multiplication table.

The existential exponent in nilpotence also has a finite test. If $s = \dim_K A > 0$, then x is nilpotent if and only if $x^s = 0$. Compute bases for $\ker M_x^j$ for $0 \le j \le s$. Each basis is expressible in the next, and any change of dimension increases it by at least one. Either the last kernel has dimension s, or two successive kernels already have the same solution type. In the latter case, $M_x^{j+2} v = 0$ implies $M_x v : \ker M_x^{j+1} = \ker M_x^j$, so the next kernel also agrees; finite induction repeats this conclusion up to any supplied exponent q. Thus $M_x^q = 0$ implies $M_x^s = 0$, and applying this to 1 gives $x^s = 0$. For the zero algebra the test is immediate.

7 A primitive element by finite search

Lemma 7.1 (Finite square-free reduction)**.** *Let* $u : L[X_0]$ *be nonzero of degree* d*. Finite Euclidean divisions compute a monic polynomial* u_{sf} *such that*

$$u_{\mathrm{sf}} \mid u, \qquad u \mid u_{\mathrm{sf}}^d, \qquad \gcd(u_{\mathrm{sf}}, u'_{\mathrm{sf}}) = 1.$$

If $\gcd(u, u') \neq 1$*, then* $\deg u_{\mathrm{sf}} < \deg u$*.*

See Appendix B.1 for the proof.

Theorem 7.2 (Finite primitive-element construction)**.** *Let* $B \neq 0$ *be a finite reduced commutative* K*-algebra of dimension* s*, generated by* $\beta_1, \ldots, \beta_\ell$*. Here the generating data include polynomials* $H_i : K[Y_1, \ldots, Y_\ell]$ *expressing the supplied basis vectors as* $e_i = H_i(\beta_1, \ldots, \beta_\ell)$*. Define*

$$E_s := \frac{s(s-1)}{2}. \tag{7.1}$$

A search through the finite grid $\{0, 1, \ldots, E_s\}^\ell$ *finds* $c = (c_1, \ldots, c_\ell)$ *such that*

$$\theta := \sum_{k=1}^{\ell} c_k \beta_k, \qquad B = K[\theta]. \tag{7.2}$$

Finite row reduction computes a monic polynomial $p : K[X_0]$ *and* $\varphi_k : K[X_0]$ *satisfying*

$$\deg p = s, \qquad \deg \varphi_k < s, \qquad B \cong K[X_0]/\langle p \rangle, \qquad \beta_k = \varphi_k(\theta). \tag{7.3}$$

See Appendix B.3 for the proof.

Remark 7.3 (Scalar extension and a univariate quotient). The type B_L in Appendix B.3 retains the basis and multiplication table of B, allowing rational-function coefficients of type L. Specialization requires the denominators used to remain nonzero. For monic p of degree s, the quotient $K[X_0]/\langle p \rangle$ has basis $[1]_{\langle p \rangle}, \ldots, [X_0^{s-1}]_{\langle p \rangle}$, with equality and multiplication computed by Euclidean remainders. Thus (7.3) is an isomorphism of finite coordinate algebras.

8 Univariate approximation

Theorem 8.1 (Finite approximate FTA over K)**.** *Let $p(X_0) : K[X_0]$ be nonzero and nonconstant. For every $\eta : \mathbb{Q}_{>0}$, a finite rational procedure returns $t : K$ such that*

$$\mathrm{N}(p(t)) < \eta^2. \tag{8.1}$$

Before receiving η, the argument determines from the coefficients of p a positive integer R_p such that every resulting point satisfies

$$\mathrm{s}(t) \le 2R_p. \tag{8.2}$$

Proof. This is the approximation theorem of the first paper [2]. Its construction chooses R_p by a strict rational leading-term inequality and a mesh by rational variation bounds, then searches a finite rational square grid. The proof uses integer crossing numbers of finite rational polygons and a finite triangulation. The radius depends only on p; only the mesh depends on η. □

9 Simultaneous approximation in one parameter

Theorem 9.1 (Exact one-parameter divisibility)**.** *Let $a : K^e$ and let J_a be the proper zero-dimensional ideal type in $K[Y_1, \dots, Y_\ell]$ produced by Theorem 5.9. Let*

$$A = K[Y]/J_a, \qquad B = A/\operatorname{Nil}(A),$$

and let $p, \varphi_1, \dots, \varphi_\ell$ be produced by Theorem 7.2. Then finite univariate division computes $s_j(X_0) : K[X_0]$ such that

$$f_j(a, \varphi_1(X_0), \dots, \varphi_\ell(X_0)) = p(X_0)s_j(X_0) \qquad (1 \le j \le m). \tag{9.1}$$

For every $\varepsilon : \mathbb{Q}_{>0}$, one call to Theorem 8.1 produces $t : K$ satisfying

$$\sum_{j=1}^{m} \mathrm{N}\big(f_j(a, \varphi_1(t), \dots, \varphi_\ell(t))\big) < \varepsilon^2. \tag{9.2}$$

Proof. Let

$$\alpha_k := [Y_k] : A, \qquad \beta_k := [\alpha_k]_{\mathrm{Nil}(A)} : B. \tag{9.2a}$$

The definitions of the two quotients give

$$f_j(a, \alpha_1, \dots, \alpha_\ell) = 0 \text{ in } A, \qquad f_j(a, \beta_1, \dots, \beta_\ell) = 0 \text{ in } B. \tag{9.2b}$$

Let θ be the element of Theorem 7.2. Then

$$\beta_k = \varphi_k(\theta), \qquad B \cong K[X_0]/\langle p \rangle, \quad [X_0]_{\langle p \rangle} \longmapsto \theta. \tag{9.2c}$$

Define

$$g_j(X_0) := f_j(a, \varphi_1(X_0), \dots, \varphi_\ell(X_0)) : K[X_0]. \tag{9.2d}$$

Equations (9.2b)–(9.2c) give $g_j(\theta) = 0$. Finite univariate division by the monic polynomial p gives

$$g_j(X_0) = p(X_0)s_j(X_0) + r_j(X_0), \qquad \deg r_j < \deg p = s. \tag{9.2e}$$

At $X_0 = \theta$, one has $r_j(\theta) = 0$. Write

$$r_j(X_0) = \sum_{i=0}^{s-1} r_{ji} X_0^i.$$

Since $(1, \theta, \dots, \theta^{s-1})$ is a basis of B,

$$\sum_{i=0}^{s-1} r_{ji}\theta^i = 0 \Longrightarrow r_{j0} = \cdots = r_{j,s-1} = 0. \tag{9.2f}$$

Thus $r_j = 0$, and (9.2e) is exactly (9.1).

Compute R_p from Theorem 8.1, let $b_{\mathrm{bd,p}} := 2R_p$, and define

$$C_j := \|s_j\|_{b_{\mathrm{bd,p}}}, \qquad C := \sum_{j=1}^{m} C_j^2, \qquad \eta_{\mathrm{app}} := \frac{\varepsilon}{1+C}. \tag{9.3}$$

These are explicit nonnegative rationals and $\eta_{\mathrm{app}} > 0$. Apply Theorem 8.1 to (p, η_{app}); the polynomial p is nonconstant because $\deg p = \dim_K B \geq 1$. It returns t with $\mathrm{s}(t) \leq b_{\mathrm{bd,p}}$ and $\mathrm{N}(p(t)) < \eta_{\mathrm{app}}^2$. Write

$$s_j(X_0) = \sum_{i=0}^{v_j} u_{ji} X_0^i.$$

Then

$$\mathrm{s}(s_j(t)) \leq \sum_{i=0}^{v_j} \mathrm{s}(u_{ji})\,\mathrm{s}(t)^i \leq \sum_{i=0}^{v_j} \mathrm{s}(u_{ji}) b_{\mathrm{bd,p}}^i = C_j, \qquad \mathrm{N}(s_j(t)) \leq C_j^2. \tag{9.3a}$$

Let $\Phi(t) := (\varphi_1(t), \dots, \varphi_\ell(t))$. Multiplicativity of N and (9.1) give

$$\begin{aligned} \sum_{j=1}^{m} \mathrm{N}(f_j(a, \Phi(t))) &= \mathrm{N}(p(t)) \sum_{j=1}^{m} \mathrm{N}(s_j(t)) \\ &\leq \eta_{\mathrm{app}}^2 C = \varepsilon^2 \frac{C}{(1+C)^2} < \varepsilon^2, \end{aligned} \tag{9.4}$$

because $(1+C)^2 - C = 1 + C + C^2 > 0$. □

10 Proof of the main theorem

Proof of Theorem 2.3. Fix the variable order, use degree–lexicographic monomial order, and examine each finite list of critical pairs in lexicographic order. Theorem 4.17, with $L = K$, computes

$$G = \mathsf{A}F, \qquad F = \mathsf{B}G, \qquad \langle F \rangle = \langle G \rangle. \tag{10.1}$$

If $g_\kappa = c : K^\times$, then

$$1 = c^{-1} g_\kappa = \sum_{j=1}^{m} c^{-1} \mathsf{A}_{\kappa j} f_j, \tag{10.2}$$

which is alternative (i). If no such g_κ occurs, the last assertion of Theorem 4.17 gives

$$\neg(1 : I), \qquad I := \langle F \rangle. \tag{10.3}$$

Apply Theorem 5.9; if no Y-variables remain, then all the f_j vanish and $z = 0$ gives alternative (ii). Otherwise, Lemma 5.5 and Theorems 6.2, 7.2, and 9.1 give an approximate common zero in the reordered coordinates; restoring the original variable order yields $z : K^n$ with $\mathcal{N}_F(z) < \varepsilon^2$, proving alternative (ii). □

A The trace pairing and the nilradical

Lemma A.1 (Nilpotent endomorphisms have zero trace)**.** *If* $\mathsf{T}^q = 0$ *on a finite-dimensional* L*-vector space* $\mathcal{V}$*, then*

$$\operatorname{Tr}(\mathsf{T}) = 0. \tag{A.1}$$

Proof. The zero-dimensional case is immediate. Otherwise take $q \geq 1$ and let $\mathcal{K}_j$ denote the coordinate solution type of $\mathsf{T}^j v = 0$. Starting with the empty basis $\mathcal{B}_0$, row reduction successively constructs bases

$$\mathcal{B}_j = (\mathcal{B}_{j-1}, w_{j,1}, \ldots, w_{j,d_j}), \qquad 1 \leq j \leq q. \tag{A.2}$$

Indeed, each vector already in $\mathcal{B}_{j-1}$ satisfies $\mathsf{T}^j v = 0$; append independent columns from a computed basis of $\ker \mathsf{T}^j$ until a basis of that solution type is obtained. Since $\mathsf{T}^q = 0$, $\mathcal{B}_q$ is a basis of $\mathcal{V}$.

For each newly appended vector, the identity $\mathsf{T}^{j-1}(\mathsf{T} w_{j,a}) = \mathsf{T}^j w_{j,a} = 0$ gives, by row reduction, coefficients such that

$$\mathsf{T} w_{j,a} = \sum_{b \in \mathcal{B}_{j-1}} c_{b,j,a}\, b. \tag{A.3}$$

Thus the image of every vector in the ordered basis $\mathcal{B}_q$ is a linear combination of earlier basis vectors. Its matrix has zero diagonal. Since trace is the sum of diagonal entries and is invariant under change of basis, this gives (A.1). □

Proof of Theorem 6.2. For $u, v : A$, associativity gives

$$M_u M_v = M_{uv}, \qquad M_u^q = M_{u^q}. \tag{6.2a}$$

Suppose $x^q = 0$. For every $y : A$, commutativity and (6.2a) give

$$(xy)^q = x^q y^q = 0, \qquad M_{xy}^q = 0. \tag{6.2b}$$

Lemma A.1, applied to $\mathsf{T} = M_{xy}$, gives

$$\langle x, y \rangle_A = \operatorname{Tr}(M_{xy}) = 0 \quad (y : A). \tag{6.2e}$$

Thus nilpotent elements satisfy the kernel condition in (6.3).

Conversely, let x be nonnilpotent, and let $n_0 := \dim_K A$. The $n_0 + 1$ vectors

$$1, x, x^2, \ldots, x^{n_0}$$

are linearly dependent. Let $m_x(X_0)$ be their least-degree monic relation. For every $g : K[X_0]$, Euclidean division gives

$$g = \mathfrak{q}_g m_x + r_g, \qquad \deg r_g < \deg m_x,$$

and therefore

$$g(x) = 0 \quad \Longleftrightarrow \quad m_x \mid g. \tag{6.5}$$

Indeed, $g(x) = 0$ implies $r_g(x) = 0$, and minimality forces $r_g = 0$.

Extract the highest power of X_0 dividing m_x:

$$m_x(X_0) = X_0^q h(X_0), \qquad q \geq 0, \quad h(0) \neq 0, \quad \deg h > 0. \tag{6.6}$$

The last inequality follows because $h : K^\times$ would give $x^q = 0$. Since $\gcd(X_0^q, h) = 1$, the Euclidean algorithm computes

$$u_0(X_0) X_0^q + v_0(X_0) h(X_0) = 1. \tag{6.7}$$

Define

$$g(X_0) := u_0(X_0)X_0^q, \qquad \mathfrak{e} := g(x). \tag{6.8}$$

Equation (6.7) gives

$$X_0^q \mid g, \qquad h \mid (g-1).$$

Hence

$$X_0^q \mid (g^2-g), \qquad h \mid (g^2-g), \qquad m_x = X_0^q h \mid (g^2-g), \tag{6.9}$$

where the last divisibility follows from $\gcd(X_0^q, h) = 1$. Equation (6.5) yields

$$\mathfrak{e}^2 = \mathfrak{e}, \qquad h(x)\mathfrak{e} = u_0(x)m_x(x) = 0. \tag{6.10}$$

If $\mathfrak{e} = 0$, then (6.5) gives $m_x \mid u_0 X_0^q$. Coprimality gives $h \mid u_0$: if $a_0 X_0^q + b_0 h = 1$, then

$$u_0 = a_0 u_0 X_0^q + b_0 u_0 h,$$

and both terms on the right are divisible by h. Hence both terms on the left of (6.7) are divisible by h. This would give $h \mid 1$, contrary to $\deg h > 0$. Therefore

$$\mathfrak{e}^2 = \mathfrak{e}, \qquad \mathfrak{e} \neq 0, \qquad h(x)\mathfrak{e} = 0. \tag{6.11}$$

Since $h(0) \neq 0$, one has $\gcd(X_0, h) = 1$. Compute

$$w(X_0)X_0 + z(X_0)h(X_0) = 1 \tag{6.12}$$

and let $b := w(x)\mathfrak{e}$. Equations (6.11)–(6.12) give

$$xb = w(x)x\mathfrak{e} = (1 - z(x)h(x))\mathfrak{e} = \mathfrak{e}. \tag{6.13}$$

The idempotence of $\mathfrak{e}$ gives, for every $a : A$,

$$a = \mathfrak{e}a + (a - \mathfrak{e}a), \qquad \mathfrak{e}a : \operatorname{im} M_{\mathfrak{e}}, \quad a - \mathfrak{e}a : \ker M_{\mathfrak{e}}.$$

Moreover,

$$v = \mathfrak{e}u, \quad M_{\mathfrak{e}}v = 0 \quad \Longrightarrow \quad v = \mathfrak{e}u = \mathfrak{e}^2 u = \mathfrak{e}v = 0.$$

Thus

$$A = \operatorname{im} M_{\mathfrak{e}} \oplus \ker M_{\mathfrak{e}}. \tag{6.14}$$

In an adapted basis,

$$M_{\mathfrak{e}} = \operatorname{diag}(\mathsf{I}_m, 0), \qquad m := \dim_K \operatorname{im} M_{\mathfrak{e}} \geq 1. \tag{6.15}$$

Here $m \geq 1$ because $\mathfrak{e} = M_{\mathfrak{e}}(1) \neq 0$. Characteristic zero gives

$$\langle x, b\rangle_A = \operatorname{Tr}(M_{xb}) = \operatorname{Tr}(M_{\mathfrak{e}}) = m \neq 0. \tag{6.16}$$

Writing b in the supplied basis shows that at least one $\langle x, e_j\rangle_A$ is nonzero. Thus a nonnilpotent element does not satisfy the left-hand condition of (6.3). Together with (6.2e), this proves (6.3).

For a basis $(e_1, \ldots, e_{n_0})$, define the Gram matrix

$$\Gamma_{ij} := \operatorname{Tr}(M_{e_i e_j}). \tag{6.17}$$

For $x = \sum_i x_i e_i$,

$$\langle x, e_j\rangle_A = \sum_{i=1}^{n_0} x_i \Gamma_{ij}. \tag{6.18}$$

Hence finite row reduction of Γ computes the coordinate kernel in (6.3).

The nilpotents form an ideal. If $x^q = 0$, then $(ax)^q = 0$; if additionally $y^\ell = 0$, then

$$(x+y)^{q+\ell-1} = \sum_{j=0}^{q+\ell-1} \binom{q+\ell-1}{j} x^j y^{q+\ell-1-j} = 0, \tag{6.19}$$

because every summand contains either x^q or y^ℓ. Its computed K-basis therefore also generates it as an ideal type in A. Row reduction expresses each product of a basis vector of A with one of these generators in the same ideal basis. Thus (6.4) is defined by the finite coordinate construction of Proposition 5.3, whose hypotheses have now been established. Its unit is nonzero because 1 is not nilpotent. Finally,

$$[x]^q_{\mathrm{Nil}(A)} = 0 \Longrightarrow (x^q : \mathrm{Nil}(A)) \Longrightarrow x^{qv} = 0 \text{ for some } v \Longrightarrow [x]_{\mathrm{Nil}(A)} = 0. \tag{6.20}$$

Therefore B is reduced.

For an explicit multiplication table, let $(n_1, \dots, n_{\ell_{\mathrm{nil}}})$ be the basis of $\mathrm{Nil}(A)$ returned by row reduction of Γ. Extend it, again by row reduction, to a basis

$$(n_1, \dots, n_{\ell_{\mathrm{nil}}}, b_1, \dots, b_s) \quad \text{of } A. \tag{6.21}$$

For each i, j, multiplication in A and coordinate reduction in (6.21) give unique scalars

$$b_i b_j = \sum_{\lambda=1}^{\ell_{\mathrm{nil}}} u_{ij}^{\lambda} n_\lambda + \sum_{k=1}^{s} d_{ij}^{k} b_k. \tag{6.22}$$

Writing $\bar{b}_k := [b_k]_{\mathrm{Nil}(A)}$ for the quotient coordinate vector represented by b_k gives

$$B = \bigoplus_{k=1}^{s} K \cdot \bar{b}_k, \qquad \bar{b}_i\, \bar{b}_j = \sum_{k=1}^{s} d_{ij}^{k} \bar{b}_k. \tag{6.23}$$

Thus (6.17), (6.21), and (6.22) compute B solely by finite matrix operations. □

B Square-free reduction and the primitive element

B.1 Square-free reduction

Proof of Lemma 7.1. Normalize u to be monic; this preserves its divisibility relations up to nonzero constant factors. We construct the required polynomial by induction on $d = \deg u$. If $d = 0$, take $u_{\mathrm{sf}} = 1$. For $d > 0$, compute $g = \gcd(u, u')$. If $g = 1$, take $u_{\mathrm{sf}} = u$; then $u \mid u^d$.

Suppose $g \neq 1$. Characteristic zero gives $u' \neq 0$, so

$$u = gv, \qquad 0 < \deg g < d, \qquad 0 < \deg v < d. \tag{7.0a}$$

Apply the induction hypothesis to g and v, obtaining monic polynomials a, b with

$$a \mid g, \quad g \mid a^{\deg g}, \quad \gcd(a, a') = 1, \qquad b \mid v, \quad v \mid b^{\deg v}, \quad \gcd(b, b') = 1.$$

Compute $c = \gcd(a, b)$, write $a = ca_1$, $b = cb_1$, and set

$$h := a_1 b = \frac{ab}{c}. \tag{7.0b}$$

These are finite Euclidean computations. The identities $a' = c'a_1 + ca_1'$ and $\gcd(a, a') = 1$ imply $\gcd(a_1, c) = \gcd(a_1, a_1') = 1$. Dividing a Bézout identity for a, b by c gives $\gcd(a_1, b_1) = 1$,

hence $\gcd(a_1, b) = 1$. For $h' = a_1' b + a_1 b'$, these coprimality relations and $\gcd(b, b') = 1$ give $\gcd(a_1, h') = \gcd(b, h') = 1$, and therefore $\gcd(h, h') = 1$.

Since $a \mid g$ and $b \mid v$, one has $h \mid ab \mid gv = u$. Also $a \mid h$ and $b \mid h$, so

$$u = gv \mid a^{\deg g} b^{\deg v} \mid h^{\deg g + \deg v} = h^d. \tag{7.0}$$

Take $u_{\mathrm{sf}} = h$. If $\deg h = d$, the monic divisibility $h \mid u$ forces $h = u$, contradicting $\gcd(u, u') \neq 1$. Thus $\deg h < d$ in this case. Each recursive call has smaller positive degree, so the construction terminates by finite induction. □

B.2 Formal coefficient differentiation

Lemma B.1 (Derivations of a formal rational-function field)**.** *Let $L = K(X_1, \ldots, X_\ell)$. For $f, g : K[X]$, $g \neq 0$, the rule*

$$\partial_k \left(\frac{f}{g} \right) := \frac{(\partial_k f) g - f (\partial_k g)}{g^2} \tag{B.1}$$

is independent of the representation f/g. It satisfies

$$\partial_k (u + v) = \partial_k u + \partial_k v, \qquad \partial_k (uv) = (\partial_k u) v + u (\partial_k v). \tag{B.2}$$

For a finite K-algebra B with basis $(e_1, \ldots, e_s)$ and multiplication table $e_i e_j = \sum_k m_{ij}^k e_k$, let $B_L = L^s$ carry the same multiplication table over L. The coefficientwise extension

$$\partial_k \left(\sum_i \lambda_i e_i \right) := \sum_i (\partial_k \lambda_i) e_i \qquad (\lambda_i : L) \tag{B.3}$$

also satisfies (B.2).

Proof. If $f/g = h/u$, then

$$fu = gh. \tag{B.4}$$

Differentiate (B.4):

$$(\partial_k f) u + f (\partial_k u) = (\partial_k g) h + g (\partial_k h). \tag{B.5}$$

After passage to the common denominator $g^2 u^2$, equations (B.4)–(B.5) give

$$\frac{(\partial_k f) g - f (\partial_k g)}{g^2} = \frac{(\partial_k h) u - h (\partial_k u)}{u^2}. \tag{B.6}$$

Thus (B.1) is well-defined. Direct expansion with the finite fraction rules for addition and multiplication proves (B.2). For (B.3), the constants $m_{ij}^k : K$ have derivative zero; expansion of both sides of the product rule in the basis (e_k) gives equality coordinatewise. □

B.3 Primitive-element construction

Proof of Theorem 7.2. Fix a K-basis $(e_1, \ldots, e_s)$ of B, and write

$$e_i e_j = \sum_{k=1}^{s} m_{ij}^k e_k, \qquad m_{ij}^k : K. \tag{7.3a}$$

Introduce formal variables $X = (X_1, \ldots, X_\ell)$ and define

$$L := K(X_1, \ldots, X_\ell), \qquad B_L := L^s, \qquad \dim_L B_L = s. \tag{7.3b}$$

Here L^s denotes the coordinate type of s-tuples over L, written $\sum_{i=1}^s \lambda_i e_i$, with multiplication given by (7.3a).

Let $\Gamma = (\mathrm{Tr}(M_{e_i e_j}))$. Since B is reduced, Theorem 6.2 gives

$$\ker_K \Gamma = 0, \qquad \det \Gamma \neq 0. \tag{7.3c}$$

The same determinant is nonzero in L, so $\ker_L \Gamma = 0$. If $u : B_L$ is nilpotent, the calculation (6.2b)–(6.2e), now over L, gives

$$\mathrm{Tr}(M_{uv}) = 0 \quad (v : B_L).$$

Thus the coordinate vector of u belongs to $\ker_L \Gamma$, and $u = 0$. Therefore

$$\mathrm{Nil}(B_L) = 0. \tag{7.3d}$$

Define the formal linear combination

$$\Theta := \sum_{k=1}^{\ell} X_k \beta_k : B_L. \tag{7.3e}$$

The $s+1$ vectors $1, \Theta, \ldots, \Theta^s$ are linearly dependent over L. Finite row reduction gives their least-degree monic relation

$$\mu(X_0) = X_0^d + \sum_{j=0}^{d-1} a_j(X) X_0^j : L[X_0], \qquad 1 \leq d \leq s, \qquad \mu(\Theta) = 0. \tag{7.3f}$$

For every $g : L[X_0]$, Euclidean division by μ and minimality give

$$g(\Theta) = 0 \quad \Longleftrightarrow \quad \mu \mid g. \tag{7.3g}$$

We claim $\gcd(\mu, \mu') = 1$. Otherwise Lemma 7.1, applied over L with

$$\nu := \mu_{\mathrm{sf}},$$

gives

$$0 \neq \nu, \qquad \deg \nu < d, \qquad \mu \mid \nu^d. \tag{7.3h}$$

Consequently

$$\nu(\Theta)^d = 0.$$

Equation (7.3d) gives $\nu(\Theta) = 0$, whereas (7.3g) and $\deg \nu < \deg \mu$ give $\nu(\Theta) \neq 0$, a contradiction. Hence

$$\gcd(\mu, \mu') = 1. \tag{7.3i}$$

Euclidean back-substitution computes $u_0, v_0 : L[X_0]$ with

$$u_0(X_0)\mu(X_0) + v_0(X_0)\mu'(X_0) = 1.$$

At $X_0 = \Theta$ this becomes

$$v_0(\Theta)\mu'(\Theta) = 1, \qquad \mu'(\Theta)^{-1} = v_0(\Theta) : L[\Theta]. \tag{7.3j}$$

Use the derivation of Lemma B.1. Thus, for $f, g : K[X]$ with $g \neq 0$,

$$\partial_k \left(\frac{f}{g} \right) := \frac{(\partial_k f) g - f(\partial_k g)}{g^2}, \qquad \partial_k := \frac{\partial}{\partial X_k}. \tag{7.3k}$$

By Lemma B.1, this is well-defined, obeys the product rule, and extends coefficientwise to B_L with $\partial_k(e_i) = 0$. Equation (7.3e) gives

$$\partial_k \Theta = \beta_k. \tag{7.3l}$$

Differentiate the expanded identity

$$\Theta^d + \sum_{j=0}^{d-1} a_j(X)\Theta^j = 0.$$

The finite product rule gives

$$\begin{aligned} 0 &= d\Theta^{d-1}\beta_k + \sum_{j=0}^{d-1}(\partial_k a_j)(X)\Theta^j + \sum_{j=1}^{d-1} j a_j(X)\Theta^{j-1}\beta_k \\ &= \mu'(\Theta)\beta_k + (\partial_k\mu)(\Theta). \end{aligned} \tag{7.3m}$$

Set $r_k(X_0) := -v_0(X_0)(\partial_k\mu)(X_0) : L[X_0]$. Equations (7.3j)–(7.3m) give

$$\boxed{\beta_k = -v_0(\Theta)(\partial_k\mu)(\Theta) = r_k(\Theta)} \qquad (1 \le k \le \ell). \tag{7.4}$$

The generating property of $\beta_1, \dots, \beta_\ell$ gives, for each vector of the fixed basis, a finite polynomial expression $e_i = H_i(\beta_1, \dots, \beta_\ell)$. Substitute the polynomials r_k from (7.4) and divide $H_i(r_1(X_0), \dots, r_\ell(X_0))$ by $\mu(X_0)$. Since $\mu(\Theta) = 0$, the remainders give coefficients $w_{ji} : L$ with

$$e_i = \sum_{j=0}^{d-1} w_{ji}\Theta^j \qquad (1 \le i \le s).$$

Conversely, the multiplication table computes the coordinates $\Theta^j = \sum_{i=1}^{s} u_{ij}e_i$ for $0 \le j < d$. Form the two finite matrices

$$\mathsf{U} = (u_{ij})_{\substack{1\le i\le s,\\ 0\le j<d}}, \qquad \mathsf{W} = (w_{ji})_{\substack{0\le j<d.\\ 1\le i\le s}}$$

Substituting the coordinates of the powers into the expressions for the e_i, uniqueness of coordinates in the fixed basis gives

$$\mathsf{UW} = \mathsf{I}_s, \qquad s = \operatorname{rank}(\mathsf{UW}) \le d \le s. \tag{7.4a}$$

The last inequality follows from (7.3f). Moreover, minimality of μ shows that $1, \Theta, \dots, \Theta^{d-1}$ are linearly independent, since a nonzero relation among them would have degree below d. Consequently

$$d = s, \qquad (1, \Theta, \dots, \Theta^{s-1}) \text{ is an } L\text{-basis of } B_L. \tag{7.4b}$$

For $0 \le j < s$, write the coordinates of Θ^j in the fixed basis:

$$\Theta^j = \sum_{i=1}^{s} v_{ij}(X)e_i, \qquad v_{ij}(X) : K[X_1, \dots, X_\ell]. \tag{7.4c}$$

The entries are polynomials, not rational functions: expansion of (7.3e) and repeated use of (7.3a) give

$$\deg v_{ij} \le j. \tag{7.4d}$$

Let

$$\mathsf{V}(X) := (v_{ij}(X))_{\substack{1\le i\le s,\\ 0\le j<s}}, \qquad h(X) := \det \mathsf{V}(X). \tag{7.5}$$

By (7.4b), the columns are linearly independent over L; hence

$$h(X) : K[X_1, \dots, X_\ell], \qquad h(X) \neq 0. \tag{7.5a}$$

Every summand in the determinant chooses one entry from each column, so

$$\deg h \le \sum_{j=0}^{s-1} j = \frac{s(s-1)}{2} = E_s. \tag{7.5b}$$

Lemma 3.2 finds, by at most $(E_s+1)^\ell$ tests,

$$c \in \{0, 1, \dots, E_s\}^\ell, \qquad h(c) \neq 0. \tag{7.5c}$$

Under $X \mapsto c$, the columns of $\mathsf{V}(c)$ are the coordinates of

$$1, \theta, \dots, \theta^{s-1}, \qquad \theta = \sum_{k=1}^{\ell} c_k \beta_k. \tag{7.5d}$$

Since $\det \mathsf{V}(c) \neq 0$, these s vectors form a K-basis of B, and $B = K[\theta]$.

Finite row reduction in this basis gives unique coefficients

$$\theta^s = \sum_{j=0}^{s-1} a_j \theta^j, \qquad \beta_k = \sum_{j=0}^{s-1} b_{kj} \theta^j. \tag{7.6}$$

Define

$$p(X_0) := X_0^s - \sum_{j=0}^{s-1} a_j X_0^j, \qquad \varphi_k(X_0) := \sum_{j=0}^{s-1} b_{kj} X_0^j. \tag{7.7}$$

Then $p(\theta) = 0$ and $\beta_k = \varphi_k(\theta)$. No nonzero polynomial of degree below s annihilates θ, because $1, \theta, \dots, \theta^{s-1}$ are linearly independent. For any supplied $g : K[X_0]$, divide g by p and evaluate its remainder at θ. This defines the finite coordinate map

$$\begin{aligned} \Psi : K[X_0]/\langle p \rangle &\longrightarrow B, \\ [g]_{\langle p \rangle} &\longmapsto g(\theta). \end{aligned} \tag{7.8}$$

Changing the representative by a multiple of p leaves its value unchanged because $p(\theta) = 0$, and evaluation preserves the algebra operations. The map sends the finite coordinate basis $([1]_{\langle p \rangle}, \dots, [X_0^{s-1}]_{\langle p \rangle})$ to $(1, \theta, \dots, \theta^{s-1})$; its inverse is obtained by solving for coordinates in this basis. Hence Ψ is the asserted algebra isomorphism between two finite-dimensional coordinate types. □

Acknowledgments

We acknowledge the use of the Math AI agents Rethlas and Archon (developed by Bin Dong's group at Peking University), utilizing GPT-5.6-sol and Deepseek-V4-Flash, to assist in reasoning and verification for portions of this work. All outputs were independently evaluated and refined by the authors, who retain full responsibility for the results.

References

[1] Thomas Becker and Volker Weispfenning, in cooperation with Heinz Kredel, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Graduate Texts in Mathematics 141, Springer, 1993.

[2] Liang Zhang and Xiaohua (Michael) Xuan, *An Elementary Proof of Fundamental Theorem of Algebra over Rationals*, Hexagon preprint, hexagon:2611.00320v1, 2026. https://hexagonmath.org/2611.00320v1.

[3] N. J. Wildberger, *Divine Proportions: Rational Trigonometry to Universal Geometry*, Wild Egg Pty Ltd, Australia, 2005. ISBN 0-9757492-0-X.

[4] N. J. Wildberger, *What is the Fundamental Theorem of Algebra, Really?*, Abstract Algebra Math Foundations 217, online lecture, 2017. https://www.youtube.com/watch?v=qoSGtoy7DlI.

[5] S. Basu and D. J. Velleman, On Gauss's first proof of the fundamental theorem of algebra, *The American Mathematical Monthly* **124** (2017), no. 8, 688–694.

[6] J. Stevens, *Early proofs of Hilbert's Nullstellensatz*, arXiv:2309.14024, 2023. https://arxiv.org/abs/2309.14024.

[7] D. Hilbert, Ueber die vollen Invariantensysteme, *Mathematische Annalen* **42** (1893), 313–373. https://doi.org/10.1007/BF01444162.