The Quarterly Journal of Mathematics Advance Access published online on 23 May 2005
Quart. J. Math. 56 (2005), 263–300; doi:10.1093/qmath/hah048

BOUNDS AND DEFINABILITY IN POLYNOMIAL RINGS

by MATTHIAS ASCHENBRENNER[†]

(*Department of Mathematics, Statistics and Computer Science, University of Illinois at Chicago,* 851 *S. Morgan Street* (M/C 249)*, Chicago,* IL 60607*, USA*)

[Received 13 February 2004. Revised 9 December 2004]

Abstract

We study questions around the existence of bounds and the dependence on parameters for linear-algebraic problems in polynomial rings over rings of an arithmetic flavour. In particular, we show that the module of syzygies of polynomials $f_1, \dots, f_n \in R[X_1, \dots, X_N]$ with coefficients in a Prüfer domain R can be generated by elements whose degrees are bounded by a number only depending on N, n and the degree of the f_j. This implies that if R is a Bézout domain, then the generators can be parametrized in terms of the coefficients of $f_1, \dots, f_n$ using the ring operations and a certain division function, uniformly in R.

0. Introduction

The main theme of this article is the existence of bounds for basic operations of linear algebra in polynomial rings over (commutative) rings of an arithmetic nature. The following result, shown in section 3 below, is typical.

THEOREM A *Given integers $N, d, n \geq 0$ there exists an integer $\beta = \beta(N, d, n)$ with the following property: for every Prüfer domain R and polynomials $f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of (total) degree at most d, the $R[X]$-submodule of $R[X]^n$ consisting of all solutions to the linear homogeneous equation*

$$f_1 y_1 + \cdots + f_n y_n = 0$$

can be generated by (finitely many) solutions whose components have degree at most β.

A classical theorem due to Hermann [24] states that Theorem A is true if we replace 'Prüfer domain' by 'field'. In this case, it is easy to see that β can be chosen independent of n; Seidenberg [36] computed an explicit (doubly exponential) bound β. In [2] we extended Hermann's result to the class of *almost Dedekind domains* (that is, domains all of whose localizations at maximal ideals are discrete valuation rings) and obtained the bound

$$\beta(N, d) = (2d)^{2^{O(N \log(N+1))}};$$

see [33, 34] for an application of this result. In contrast to [2, 24, 36], the methods employed to prove Theorem A in the present paper are rather non-constructive. They are inspired by the model-theoretic approach (see, for example, [15]) to establish the existence of uniform bounds for ideal-theoretic problems in polynomial rings over fields, one difference being our use of *direct products* rather than *ultraproducts* (or other versions of the Compactness Theorem of

[†] E-mail: maschenb@math.uic.edu

first-order logic). We also work in the more general setting of *semihereditary rings* and rely in an essential way on a theorem of Vasconcelos (see Theorem 3.1 below) on the coherence of polynomial rings over semihereditary rings. Theorem A remains true for certain possibly non-reduced rings as well, in particular for Artinian local rings of fixed length; see Corollary 3.18.

The following theorem, proved in section 4, shows that the analogue of Theorem A for inhomogeneous linear equations holds only in a very restricted setting.

THEOREM B *For a ring R, the following statements are equivalent.*

(1) *The nilradical*

$$\mathrm{Nil}(R) = \{r \in R : r^n = 0 \text{ for some } n \geq 1\}$$

of R is nilpotent, and $R/\mathrm{Nil}(R)$ is von Neumann regular.

(2) *For all integers $N, d, n \geq 0$ there exists an integer $\beta = \beta(N, d, n)$ with the following property: if $f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ are of degree at most d such that*

$$1 = f_1 g_1 + \cdots + f_n g_n$$

for some $g_1, \dots, g_n \in R[X]$, then there exist such g_j of degree at most β.

Moreover, for every $m \geq 1$ and $N, d, n \geq 0$ there exists an integer $\beta(N, d, n, m)$ such that if $\mathrm{Nil}(R)^m = \{0\}$ and $R/\mathrm{Nil}(R)$ is von Neumann regular, then (2) holds with $\beta = \beta(N, d, n, m)$. Condition (1) in Theorem B is satisfied if R is an Artinian local ring, yielding a result on the existence of uniform bounds for the ideal membership problem in polynomial rings over Artinian local rings of bounded length, originally proved by Schoutens [32]. His result applies, in particular, if R is a field. In this special case, which is again due to Hermann [24], the existence of such a uniform bound is equivalent to the following statement: if $f_0, f_1, \dots, f_n$ are polynomials in $\mathbb{Z}[C, X]$ (with $C = (C_1, \dots, C_M)$ being parametric variables), then for each field F the subset

$$\{c \in F^M : f_0(c, X) \in (f_1(c, X), \dots, f_n(c, X))F[X]\} \tag{1}$$

of F^M is *constructible*, that is, a boolean combination of algebraic subsets of F^M. Results on dependence on parameters such as this are most conveniently (and accurately) expressed using the terminology of mathematical logic: rephrased in this way, Hermann's theorem asserts that the set (1) above is definable by a quantifier-free formula in the language $\mathcal{L}_{\mathrm{ring}} = \{0, 1, +, -, \cdot\}$ of rings, uniformly for all fields F (see, for example, [25] for basic notions of first-order logic and model theory). Theorem C below can be seen as an analogue for polynomials with coefficients in $\mathbb{Z}$.

Before we can state this theorem, we have to introduce some more notation. If $a, b \in \mathbb{Z}$ are not both zero, we let $(a : b) := a/\gcd(a, b)$, where $\gcd(a, b)$ is the unique positive generator of the ideal (a, b) of $\mathbb{Z}$. We also put $(0 : 0) := 1$. Moreover, we define a relation rad on pairs (a, b) of integers as follows: $\mathrm{rad}(a, b)$ holds if and only if b divides a^n for some $n \in \mathbb{N} := \{0, 1, 2, \dots\}$. Let $\mathcal{L}_{\mathrm{rad}}$ be the expansion of the language $\mathcal{L}_{\mathrm{ring}}$ by a binary function symbol (:) and a binary predicate symbol rad. We construe the ring $\mathbb{Z}$ as $\mathcal{L}_{\mathrm{rad}}$-structure by interpreting the ring symbols as usual and the symbols (:) and rad as described above.

THEOREM C *Let* $f_0(C,X), f_1(C,X), \dots, f_n(C,X) \in \mathbb{Z}[C,X]$. *The set*

$$\{c \in \mathbb{Z}^M : f_0(c,X) \in (f_1(c,X), \dots, f_n(c,X))\mathbb{Z}[X]\} \tag{2}$$

is definable by a quantifier-free formula in the language $\mathcal{L}_{\mathrm{rad}}$.

It follows that for fixed $f_0(C,X), \dots, f_n(C,X) \in \mathbb{Z}[C,X]$, one can decide in *polynomial time* whether a tuple $c \in \mathbb{Z}^M$ is in the set (2). (This is well known for $N = 0$; see, for example, [14].) The quantifier-free formula in question can even be constructed from the f_j by a primitive recursive algorithm.

Here is an analogue of Theorem C for homogeneous equations. We say that a term $\tau(C,X)$ in a language $\mathcal{L}$ extending the language $\mathcal{L}_{\mathrm{ring}}$ of rings is *polynomial in* X if $\tau(C,X) = f(\varrho(C),X)$ for some polynomial $f \in \mathbb{Z}[V,X]$, where $V = (V_1, \dots, V_L)$ is a tuple of new variables and $\varrho(C)$ an L-tuple of $\mathcal{L}$-terms in the variables C. (In other words, the extra function symbols in $\mathcal{L}\backslash\mathcal{L}_{\mathrm{ring}}$ are applied only to subterms of τ not involving the X-variables.) We let $\mathcal{L}_{\mathrm{gcd}}$ be the sublanguage $\{0, 1, +, \cdot, (:)\}$ of $\mathcal{L}_{\mathrm{rad}}$.

THEOREM D *Let* $f_1(C,X), \dots, f_n(C,X) \in \mathbb{Z}[C,X]$. *There exists a finite family* $\{\varphi^{(\lambda)}(C)\}_{\lambda\in\Lambda}$ *of quantifier-free* $\mathcal{L}_{\mathrm{gcd}}$*-formulae and for each* $\lambda \in \Lambda$ *finitely many* $n \times 1$ *column vectors*

$$y^{(\lambda,1)}(C,X), \dots, y^{(\lambda,K)}(C,X) \quad (K \in \mathbb{N})$$

whose entries are $\mathcal{L}_{\mathrm{gcd}}$*-terms, polynomial in* X, *such that for all* $c \in \mathbb{Z}^M$ *we have* $\mathbb{Z} \vDash \bigvee_{\lambda\in\Lambda} \varphi^{(\lambda)}(c)$, *and if* $\lambda \in \Lambda$ *is such that* $\mathbb{Z} \vDash \varphi^{(\lambda)}(c)$, *then*

$$y^{(\lambda,1)}(c,X), \dots, y^{(\lambda,K)}(c,X) \in \mathbb{Z}[X]^n$$

generate the $\mathbb{Z}[X]$*-module of solutions in* $\mathbb{Z}[X]$ *to the homogeneous equation*

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

In fact, the $\varphi^{(\lambda)}$ and the $y^{(\lambda,k)}$ can be effectively constructed from $f_1, \dots, f_n$. Theorems C and D (suitably adapted) remain true in the more general setting of Bézout domains. It should be remarked that in contrast to Theorem D, it is not possible in general to obtain a parametric solution $(y_1, \dots, y_n) \in \mathbb{Z}[X]^n$ to an inhomogeneous linear equation

$$f_0(c,X) = f_1(c,X)y_1 + \cdots + f_n(c,X)y_n, \tag{3}$$

even for the case $f_0 = 1$. More precisely, by Theorem B (or the example in [2, section 6]) there do *not* exist finitely many n-tuples $(\tau_{1k}(C,X), \dots, \tau_{nk}(C,X))$ of terms in a language $\mathcal{L} \supseteq \mathcal{L}_{\mathrm{ring}}$ such that $\mathbb{Z}$ can be expanded to an $\mathcal{L}$-structure, each $\tau_{ik}(C,X)$ is polynomial in X, and such that if $c \in \mathbb{Z}^M$ with

$$1 \in (f_1(c,X), \dots, f_n(c,X))\mathbb{Z}[X],$$

then $(\tau_{1k}(c,X), \dots, \tau_{nk}(c,X)) \in \mathbb{Z}[X]^n$ is a solution to (3), for some k.

Organization of the paper. Sections 1 and 2 contain preliminary material. Beside fixing notation, we introduce a tool from first-order logic, namely the persistence of Horn formulae under direct products (or, more generally, reduced products). This allows us to shorten some arguments in later sections (although it is not strictly speaking necessary). In section 2 we

discuss coherent modules and rings. Most of the material is standard, but we emphasize issues of uniformity and definability. In section 3 we study bounds for homogeneous systems of linear equations. We introduce a notion (super coherence) related to the notion of 'stable coherence' from [19] and prove Theorems A and D. In section 4 we prove Theorems B and C. The theorems in sections 3 and 4 can be employed to obtain uniformity and definability results for various properties of ideals and algebraic constructions in polynomial rings. In section 5 we illustrate this by means of defining the primeness of an ideal. In the Appendix we give yet another application of the material in section 4 and obtain a characterization of Jacobson domains among Noetherian domains inspired by a characterization of Noetherian domains with the 'Skolem property' in [18].

1. Preliminaries

In this section we collect some definitions and notation used in the sequel. The reader may glance over this part and come back to it for reference when necessary. We also recall some basic facts about Horn formulae which will come in handy in sections 2 and 3.

Rings, ideals and modules. Let R be a ring (throughout: commutative with a unit element 1). We write $(r_1, \dots, r_n)R$ for the ideal generated in R by elements $r_1, \dots, r_n$; we omit R when it is clear from the context. The localization $S^{-1}R$, where S is the set of non-zero-divisors of R, is called the ring of fractions of R, denoted by $\mathrm{Frac}(R)$. For submodules M, M' of an R-module we define the ideal

$$M' : M := \{a \in R : am \in M' \text{ for all } m \in M\}$$

of R. Given an R-module M and $(f_1, \dots, f_n) \in M^n$, the set of solutions in R^n to the homogeneous system of linear equations $y_1 f_1 + \cdots + y_n f_n = 0$ is an R-submodule of R^n, which we call the (first) *module of syzygies of* $(f_1, \dots, f_n)$. If $M = R^m$ and $f_1, \dots, f_n \in R^m$ are the column vectors of a matrix $A \in R^{m \times n}$, we denote the module of syzygies of $(f_1, \dots, f_n)$ by $\mathrm{Sol}_R(A)$ (the module of solutions to the system of homogeneous linear equations $Ay = 0$). If I is an ideal of R, then

$$\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n > 0\}$$

is the nilradical of I. We let $\mathrm{Nil}(R) := \sqrt{(0)}$, the nilradical of R.

Polynomials. Unless otherwise noted, by $X = (X_1, \dots, X_N)$ we always denote a tuple of N distinct indeterminates, where $N \in \mathbb{N}$. The (total) degree of a polynomial $0 \neq f \in R[X] = R[X_1, \dots, X_N]$ is denoted by $\deg(f)$. By convention $\deg(0) := -\infty$ where $-\infty < \mathbb{N}$. We extend this notation to finite tuples $f = (f_1, \dots, f_n)$ of polynomials in $R[X]$ by setting $\deg(f) := \max_j \deg(f_j)$ (the degree of f).

Hereditary, semihereditary, and von Neumann regular rings. A ring R is called *hereditary* if every ideal of R is projective, and *semihereditary* if every finitely generated ideal of R is projective. A ring R is called *von Neumann regular* if every finitely generated ideal of R is generated by an idempotent. In particular, every von Neumann regular ring is semihereditary. Every semihereditary ring is reduced.

If R is a domain, then R is hereditary if and only if R is a Dedekind domain, and R is semihereditary if and only if R is a Prüfer domain [19, p. 27]. If R is hereditary, then for every prime ideal $\mathfrak{p}$ of R, the localization $R_{\mathfrak{p}}$ of R at $\mathfrak{p}$ is a discrete valuation ring (DVR). A ring R is von

Neumann regular if and only if $R_{\mathfrak{m}}$ is a field, for every maximal ideal $\mathfrak{m}$ of R. Also, a ring R is semihereditary if and only if $\mathrm{Frac}(R)$ is von Neumann regular and $R_{\mathfrak{m}}$ is a valuation ring for every maximal ideal m of R [**19**, Corollary 4.2.19].

Reduced products. Let $\mathcal{F}$ be a filter on $\mathbb{N}$, that is, a collection of non-empty subsets of $\mathbb{N}$ closed under taking finite intersections and supersets. For every $k \in \mathbb{N}$ let $R^{(k)}$ be a ring. The *reduced product* $R^* = \prod_{k\in\mathbb{N}} R^{(k)}/\mathcal{F}$ of the family $\{R^{(k)}\}_{k\in\mathbb{N}}$ over $\mathcal{F}$ is the ring R/I, where I is the ideal of $R = \prod_{k\in\mathbb{N}} R^{(k)}$ consisting of all sequences $a = (a^{(k)}) \in R$ with $\{k : a^{(k)} = 0\} \in \mathcal{F}$. We write $a \mapsto a/\mathcal{F} := a + I$ for the canonical homomorphism $R \to R^* = R/I$, and extend it in the usual manner to a homomorphism $R^n \to (R^*)^n$ (for $n \in \mathbb{N}$) which we denote in the same way. If $\mathcal{F} = \{\mathbb{N}\}$, then $a \mapsto a/\mathcal{F}$ is an isomorphism $R \to R^*$. Now suppose in addition that for every $k \in \mathbb{N}$ we are given an $R^{(k)}$-module $M^{(k)}$. Similarly as above, we then define the reduced product $M^* = \prod_{k\in\mathbb{N}} M^{(k)}/\mathcal{F}$ of $\{M^{(k)}\}_{k\in\mathbb{N}}$ over the filter $\mathcal{F}$ by $M^* = M/N$, where N is the submodule of the R-module $M = \prod_k M^{(k)}$ consisting of all sequences $m = (m^{(k)}) \in M$ with $\{k : m^{(k)} = 0\} \in \mathcal{F}$. Then M^* is an R^*-module.

Horn formulae. Let R be a ring and M an R-module. We construe M as a two-sorted structure (in the sense of model theory) in the following way. The two sorts are the *ring sort* with underlying set R and variables $r, s, \ldots$, and the *group sort* with underlying sort M and variables $x, y, \ldots$. The corresponding two-sorted language $\mathcal{L}_{\mathrm{mod}}$ of modules is the disjoint union of

(1) the language $\mathcal{L}_{\mathrm{ring}} = \{0, 1, +, -, \cdot\}$ of rings, interpreted in the obvious way in R;
(2) the language $\{0, +, -\}$ of additive groups, interpreted in the obvious way in M;
(3) a binary function symbol $\cdot$, interpreted as scalar multiplication $(r, x) \to r \cdot x : R \times M \to M$.

A basic Horn formula is an $\mathcal{L}_{\mathrm{mod}}$-formula of the form

$$\sigma_1 = 0 \,\&\, \ldots \,\&\, \sigma_p = 0 \to \tau_1 = 0 \,\&\, \ldots \,\&\, \tau_q = 0,$$

where p and q are natural numbers, $q \geq 1$, and $\sigma_i = \sigma_i(r, x)$, $\tau_j = \tau_j(r, x)$ are $\mathcal{L}_{\mathrm{mod}}$-terms in two collections of distinct indeterminates $r = (r_1, \ldots, r_m)$ (ranging over R) and $x = (x_1, \ldots, x_n)$ (ranging over M). We allow the case $p = 0$, in which case the formula in question is just $\tau_1 = \ldots = \tau_q = 0$. A *Horn formula* is an $\mathcal{L}_{\mathrm{mod}}$-formula consisting of a finite (possibly empty) string of quantifiers, followed by a conjunction of basic Horn formulae. A Horn formula that is an $\mathcal{L}_{\mathrm{mod}}$-sentence is called a *Horn sentence*.

For each $k \in \mathbb{N}$ let $M^{(k)}$ be a module over the ring $R^{(k)}$. Let $\mathcal{F}$ be a filter on $\mathbb{N}$, and let R, M, R^* and M^* be as above. For every K let $a^{(k)} = (a_1^{(k)}, \ldots, a_m^{(k)}) \in (R^{(k)})^m$ and $b^{(k)} = (b_1^{(k)}, \ldots, b_n^{(k)}) \in (M^{(k)})^n$. We put $a_i = (a_i^{(k)}) \in R$, $\quad b_i = (b_i^{(k)}) \in M$ and $a = (a_1, \ldots, a_m)$, $\mathrm{b} = (b_1, \ldots, b_n)$. The following is a special case of a fundamental theorem about Horn formulae due to Chang. (In the case of a direct product, that is, $\mathcal{F} = \{\mathbb{N}\}$, it was first proved by Horn.)

THEOREM 1.1 *For any Horn formula $\varphi(r, x)$ as above,*

$$\{k \in \mathbb{N} : M^{(k)} \vDash \varphi(a^{(k)}, b^{(k)})\} \in \mathcal{F} \Rightarrow M^* \vDash \varphi(a/\mathcal{F}, b/\mathcal{F}).$$

We omit the straightforward proof of this theorem (see, for example, [**25** Theorem 9.4.3] and instead, as an illustration of its usefulness, apply it to re-prove a well-known algebraic fact.

LEMMA 1.2 *Every reduced product of a family of semihereditary rings is semihereditary.*

Proof. A ring R is semihereditary if and only if for all $n \geq 1$ and all $f_1, \dots, f_n \in R$ the following holds, with $I := (f_1, \dots, f_n)R$ and $\phi : R^n \to I, \phi(a_1, \dots, a_n) = a_1 f_1 + \cdots + a_n f_n$. There exist n^2 elements $y_{ij} \in R$ such that the map $\psi : I \to R^n$ given by $\psi(f_i) = (y_{i1}, \dots, y_{in})$ is well defined and satisfies $\phi \circ \psi = \mathrm{id}_I$. For given n, this statement can be easily formalized as a Horn sentence. The claim now follows from Theorem 1.1 (in the case where $M^{(k)} = R^{(k)}$ for all k).

Theorem 1.1 also admits a converse: for any sentence ψ in the language of modules which is preserved under reduced products of families of modules there is a Horn sentence which is equivalent to ψ, in any module. This much deeper fact, a special case of a theorem due to Galvin and Keisler, will not be used here; see [9, Theorem 6.2.5].

2. Coherent modules and coherent rings

In this section, R always denotes a ring. An R-module M is *finitely presented* (sometimes also called *finitely related*) if there exists an exact sequence $F_1 \to F_0 \to M \to 0$ of R-linear maps, where F_0, F_1 are finitely generated free R-modules. A finitely generated R-module M is called *coherent* if every finitely generated submodule of M is finitely presented. Every finitely generated submodule of a coherent module is itself a coherent module. If R is Noetherian, then every finitely generated R-module is coherent.

We call a finitely generated R-module M *α-uniformly coherent*, where $\alpha : \mathbb{N} \to \mathbb{N}$ is a function, if for every $n \in \mathbb{N}$ the kernel of every R-module homomorphism $R^n \to M$ is generated by at most $\alpha(n)$ many elements. (Equivalently, the syzygies of every element of M^n can be generated by $\alpha(n)$ elements of R^n, for all $n \in \mathbb{N}$.) In this case, we call the function α a *uniformity function* for M. We say that M is *uniformly coherent* if it is α-uniformly coherent for some uniformity function α; clearly uniformly coherent implies coherent. (Uniformly coherent modules were first defined and studied by Soublin [39]; see also [19, 20].)

We say that an R-module M is *m-generated* (for $m \in \mathbb{N}$) if it is generated by m elements. Being m-generated and α-uniformly coherent is a property of a module (for given m and given uniformity function α) which is preserved under taking reduced products. More precisely we have the following.

PROPOSITION 2.1 *Let $m \in \mathbb{N}$ and $\alpha : \mathbb{N} \to \mathbb{N}$ be a function. Let $\{R^{(k)}\}_{k \in \mathbb{N}}$ be a family of rings, and for every $k \in \mathbb{N}$ let $M^{(k)}$ be an m-generated and α-uniformly coherent $R^{(k)}$-module. Then for every filter $\mathcal{F}$ on $\mathbb{N}$, the module $\prod_k M^{(k)}/\mathcal{F}$ over $\prod_k R^{(k)}/\mathcal{F}$ is m-generated and α-uniformly coherent.*

Proof. By Theorem 1.1, since the condition that a given module is m-generated and α-uniformly coherent can be expressed by a Horn sentence.

COROLLARY 2.2 *For an R-module M, an integer $m \geq 0$ and a function $\alpha : \mathbb{N} \to \mathbb{N}$, the following are equivalent:*

(1) *M is m-generated and α-uniformly coherent;*
(2) *for every filter $\mathcal{F}$ on $\mathbb{Z}$, $M^{\mathbb{N}}/\mathcal{F}$ is an m-generated and α-uniformly coherent $R^{\mathbb{N}}/\mathcal{F}$-module;*
(3) *$M^{\mathbb{N}}$ is an m-generated and α-uniformly coherent $R^{\mathbb{N}}$-module.*

Proposition 2.1 also yields a characterization of uniform coherence due to Soublin.

COROLLARY 2.3 *The following are equivalent, for an R-module M:*

(1) *M is finitely generated and uniformly coherent;*
(2) *for every filter $\mathcal{F}$ on $\mathbb{N}$, $M^{\mathbb{N}}/\mathcal{F}$ is a finitely generated coherent $R^{\mathbb{N}}/\mathcal{F}$-module;*
(3) *$M^{\mathbb{N}}$ is a finitely generated coherent $R^{\mathbb{N}}$-module.*

Proof. The implication (1) $\Rightarrow$ (2) follows from the proposition, and (2) $\Rightarrow$ (3) by taking $\mathcal{F} = \{\mathbb{N}\}$ in (2). It remains to show (3) $\Rightarrow$ (1). So assume that $M^{\mathbb{N}}$ is an m-generated coherent module over $R^{\mathbb{N}}$, for some $m \in \mathbb{N}$. Then M is an m-generated R-module. Suppose for a contradiction that M is not uniformly coherent, that is, there is an integer $n \in \mathbb{N}$ with the following property. For every $k \in \mathbb{N}$ there is $(f_1^{(k)}, \dots, f_n^{(k)}) \in M^n$ whose syzygies cannot be generated by k elements. Let $f_i = (f_i^{(k)}) \in M^{\mathbb{N}}$ for $i = 1, \dots, n$. Then the $R^{\mathbb{N}}$-module of syzygies of $(f_1, \dots, f_n) \in (M^{\mathbb{N}})^n$ is not finitely generated, contradicting the coherence of $M^{\mathbb{N}}$.

A ring R is called coherent if it is coherent as a module over itself, that is, if every finitely generated ideal of R is finitely presented. The following characterizations of coherence are due to Chase **[10]**; for a proof see **[19**, pp. 45–47].

THEOREM 2.4 *The following are equivalent, for a ring R:*

(1) *R is a coherent ring;*
(2) *every finitely presented R-module is coherent;*
(3) *every direct product of flat R-modules is flat;*
(4) *for every non-empty set Λ, the R-module R^{Λ} is flat;*
(5) *for every finitely generated ideal I of R and every $a \in R$, the ideal $I : (a)$ is finitely generated;*
(6) *for every $a \in R$, the ideal $(0) : (a)$ of R is finitely generated, and the intersection of two finitely generated ideals of R is a finitely generated ideal.*

An ideal I of R is called *nilpotent* if there exists an integer $m \geq 1$ such that $I^m = \{0\}$, and the smallest such m is called the *index of nilpotency* of I. Here are some sufficient conditions which ensure the preservation of coherence under ring extensions and quotients; see **[19**, Theorem 4.1.1].

PROPOSITION 2.5 *Let $\phi : R \to S$ be a ring homomorphism making S into a finitely presented R-module.*

(1) *If R is a coherent ring, then S is a coherent ring.*
(2) *If $\ker \phi$ is a finitely presented nilpotent ideal of R and S is a coherent ring, then R is a coherent ring.*

A ring R is called α-uniformly coherent if it is α-uniformly coherent as a module over itself, and uniformly coherent if it is α-uniformly coherent for some $\alpha : \mathbb{N} \to \mathbb{N}$. By Corollary 2.3, R is uniformly coherent if and only if $R^{\mathbb{N}}$ is coherent. Noetherian rings are rarely uniformly coherent. A Noetherian ring R is α-uniformly coherent if and only if $\dim R \leq 2$ and $R_{\mathfrak{m}}$ is α-uniformly coherent, for every maximal ideal $\mathfrak{m}$ of R. In this case one can take $\alpha(n) = n + 2$; see **[19**, Corollary 6.1.21].

The condition of α-coherence only concerns syzygies of tuples of elements of R. However, it implies the existence of a finite bound on the number of generators for the syzygies of tuples of elements of R^m for $m > 1$.

LEMMA 2.6 *For all integers $m, n > 0$ and all $m \times n$-matrices A with entries in an α-uniformly coherent ring R, the module $\mathrm{Sol}_R(A)$ of solutions to the homogeneous system of linear equations $Ay = 0$ is generated by $\alpha^m(n)$ solutions.*

Proof. We proceed by induction on m, the case $m = 1$ just being the definition of α-coherence. Suppose $m > 1$, and let n be a positive integer, R α-uniformly coherent, and A an $m \times n$-matrix with entries from R. Let $(f_1, \dots, f_n)$ be the first row of A and A' be the matrix consisting of the last $m - 1$ rows of A. Let $z_1, \dots, z_\alpha$ be generators for the syzygies of $(f_1, \dots, f_n)$, where $\alpha = \alpha(n)$. Consider the z_i as column vectors and let $B = A' \cdot (z_1, \dots, z_\alpha)$, an $(m-1) \times \alpha$-matrix with entries in R. The solutions to $Ay = 0$ are in one-to-one correspondence with the solutions to $Bu = 0$: every solution $u = (u_1, \dots, u_\alpha)^{\mathrm{tr}} \in R^\alpha$ to $Bu = 0$ gives rise to a solution $y = (y_1, \dots, y_n)^{\mathrm{tr}} \in R^n$ to $Ay = 0$ by setting $y = \sum_i u_i z_i$, and every solution to $Ay = 0$ arises in this way. By inductive hypothesis, there are $\alpha^m(n)$ generators for the module of solutions to $Bu = 0$, giving rise to as many generators for the module of solutions to $Ay = 0$.

DEFINITION 2.7 Let $\mathcal{C}$ be a class of rings. We say that $\mathcal{C}$ is α-uniformly coherent if every member of $\mathcal{C}$ is α-uniformly coherent. We call $\mathcal{C}$ uniformly coherent if it is α-uniformly coherent for some uniformity function α.

The following lemma gives a criterion for a class of rings to be uniformly coherent.

LEMMA 2.8 *Suppose that $\mathcal{C}$ is a class of rings which is closed under direct products. Then $\mathcal{C}$ is uniformly coherent if and only if every $R \in \mathcal{C}$ is coherent.*

Proof. The 'only if' direction is trivial. The proof of the 'if' direction is similar to the proof of (3) $\Rightarrow$ (1) in Corollary 2.3: Suppose for a contradiction that every $R \in \mathcal{C}$ is coherent, but $\mathcal{C}$ is not uniformly coherent. Then there exists some $n \in \mathbb{N}$ such that for every $k \in \mathbb{N}$ there is an $R^{(k)} \in \mathcal{C}$ and $(f_1^{(k)}, \dots, f_n^{(k)}) \in (R^{(k)})^n$ whose syzygies in $(R^{(k)})^n$ cannot be generated by k elements. Let $R^* = \prod_k R^{(k)}$ and $f_i = (f_i^{(k)}) \in R^*$. Then $R^* \in \mathcal{C}$, so R^* is coherent. But the module of syzygies of $(f_1, \dots, f_n)$ in $(R^*)^n$ is not finitely generated, a contradiction.

The typical example of a uniformly coherent class of rings is the class of semihereditary rings.

LEMMA 2.9 *Every semihereditary ring is uniformly coherent with uniformity function $\alpha(n) = n$.*

Proof. Let R be a semihereditary ring and let $f_1, \dots, f_n \in R$. We have to show that the syzygies of $(f_1, \dots, f_n)$ are generated by n elements of R^n. The finitely generated ideal $I := (f_1, \dots, f_n)$ of R is projective. So the short exact sequence

$$0 \to K := \ker \phi \to R^n \xrightarrow{\phi} I \to 0,$$

where $\phi(a_1, \dots, a_n) = a_1 f_1 + \cdots + a_n f_n$ for $(a_1, \dots, a_n) \in R^n$, splits. Hence K is a direct summand of R^n, and thus generated by n elements.

Other examples for uniformly coherent classes of rings can be obtained from rings of finite rank. Inspired by a definition of Cohen **[12]** we say that a ring R has *finite rank* if for some natural number $k > 0$, every finitely generated ideal of R is generated by k elements. (In **[12]**

this definition is only made for Noetherian R.) We call the smallest integer $k > 0$ with this property the *rank* of R. Equivalently, a ring R has rank k if every ideal of R which is generated by $k+1$ elements is generated by k elements, but there exists a finitely generated ideal of R which cannot be generated by fewer than k elements. For example, the domains of rank 1 are exactly the Bézout domains. Any reduced product of a family of rings of rank at most k has itself rank at most k, by Theorem 1.1.

LEMMA 2.10 *Let R be a coherent ring of rank k. Then every finitely generated submodule of R^n can be generated by nk elements.*

This lemma appears in [12] for Noetherian R; the proof given there goes through for coherent R.

COROLLARY 2.11 *The class of coherent rings of rank k is uniformly coherent with uniformity function $\alpha(n) = nk$.*

Proof. Let R be a coherent ring of rank k, and let $\phi : R^n \to R$ be an R linear map. Since R is coherent, $\ker \phi$ is finitely generated. By Lemma 2.10, $\ker \phi$ can be generated by nk elements.

Let us mention some classes of coherent rings with finite rank. First note that every Artinian ring R has finite rank, equal to the length of R. A Noetherian domain R has finite rank if and only if $\dim R \leq 1$ [12, Theorem 9]; see [4] for information about Noetherian domains of rank 2.

PROPOSITION 2.12 *Let R be a ring of finite Krull dimension d.*

(1) *If each localization of R has rank at most k, then R has rank at most $d + k$.*
(2) *If each localization of R is uniformly coherent with common uniformity function $n \mapsto \alpha(n)$, then R is uniformly coherent with uniformity function $n \mapsto d + \alpha(n)$.*

Proof. We use the following fact, which is the culmination of work of Forster [17], Swan [40], Eisenbud and Evans [16] (for Noetherian rings) and Heitmann [22, 23] (in the general case). Let M be a finitely generated R-module, and $k \in \mathbb{N}$. If for each prime ideal $\mathfrak{p}$ of R, the $R_\mathfrak{p}$-module $M_\mathfrak{p} = M \otimes_R R_\mathfrak{p}$ can be generated by k elements, then the R-module M can be generated by $d + k$ elements.

The first part of the proposition now follows immediately. For the second part, let $\phi : R^n \to R$ be an R-linear map. Then $\ker(\phi \otimes_R \mathrm{id}_{R_\mathfrak{p}}) = (\ker \phi) \otimes_R R_\mathfrak{p}$ can be generated by $\alpha(n)$ elements, for every prime ideal $\mathfrak{p}$ of R. Hence $\ker \phi$ can be generated by $d + \alpha(n)$ elements.

REMARKS By part (1) in the proposition it follows that a hereditary ring R has rank at most 2, since $\dim R = 1$ and each localization of R, being a DVR, has rank at most 1. In contrast, there exist Prüfer domains of finite rank greater than 2 [35], and even of infinite rank [41]. As to part (2), note that the assumption $\dim R < \infty$ cannot be dropped: there exists a ring R all of whose localizations are valuation rings, but R is not coherent [19, p. 54].

Model-theoretic aspects. Let $\mathcal{L}$ be a language extending the language $\mathcal{L}_{\mathrm{ring}} = \{0, 1, +, -, \cdot\}$ of rings, and let $\mathcal{C}$ be a class of $\mathcal{L}$-structures whose $\mathcal{L}_{\mathrm{ring}}$-reducts are rings. Fix $\alpha : \mathbb{N} \to \mathbb{N}$, and suppose that for every integer $n \geq 1$ there is a finite family $\{\varphi^{(\lambda)}(C)\}_{\lambda \in \Lambda}$ of $\mathcal{L}$-formulae $\varphi^{(\lambda)}(C)$, where $C = (C_1, \ldots, C_n)$ is an n-tuple of distinct variables, and for each $\lambda \in \Lambda$ finitely many $n \times 1$ column vectors

$$y^{(\lambda,1)}(C), \ldots, y^{(\lambda,\alpha(n))}(C)$$

whose entries are $\mathcal{L}$-terms, with the following properties. For every $R \in \mathcal{C}$ and every $a = (a_1, \dots, a_n) \in R^n$, we have

(1) $R \vDash \bigvee_{\lambda \in \Lambda} \varphi^{(\lambda)}(a)$;
(2) if $\lambda \in \Lambda$ is such that $R \vDash \varphi^{(\lambda)}(a)$, then the vectors
$$y^{(\lambda,1)}(a), \dots, y^{(\lambda,\alpha(n))}(a) \in R^n$$
generate the R-module of syzygies of a.

In particular, R is α-uniformly coherent. Then, by the proof of Lemma 2.6, for all integers $m, n > 0$ and every $m \times n$-matrix $A = (a_{ij}) \in R^{m \times n}$ there exists a similar parametrization of generators for the R-module $\mathrm{Sol}_R(A)$ by $\alpha^m(n)$ many column vectors whose entries are $\mathcal{L}$-terms, which is uniform in R and the a_{ij}. Moreover, if the $\varphi^{(\lambda,j)}$ can be chosen quantifier-free (for all n), then the corresponding formulae describing the parametrization of the generators for $\mathrm{Sol}_R(A)$ can also be chosen quantifier-free.

Below, we consider two important examples for $\mathcal{C}$: the class of Bézout domains and the class of valuation rings. We begin with a preliminary observation, valid for any ring R. For this fix $a = (a_1, \dots, a_n) \in R^n$, and consider the homogeneous linear equation

$$a_1 y_1 + \cdots + a_n y_n = 0. \tag{2.1}$$

We have the following.

PROPOSITION 2.13 *Suppose that $\lambda_1, \dots, \lambda_n \in R$ are such that*

$$u = \lambda_1 a_1 + \cdots + \lambda_n a_n$$

is a unit in R. Then the module of solutions to (2.1) *in R^n is generated by the n special solutions*

$$y^{(i)} = \left[\lambda_1 a_i, \dots, \lambda_{i-1} a_i, -\sum_{k \neq i} \lambda_k a_k, \lambda_{i+1} a_i, \dots, \lambda_n a_i\right]^{\mathrm{tr}}, \quad i = 1, \dots, n.$$

Proof. We have

$$a y^{(i)} = \sum_{j \neq i} (\lambda_j a_i) a_j - \left(\sum_{k \neq i} \lambda_k a_k\right) a_i = 0,$$

so $y^{(i)}$ is a solution to (2.1) for $i = 1, \dots, n$. Let $y = (y_1, \dots, y_n)^{\mathrm{tr}} \in R^n$ be any solution to (2.1). The ith component of the vector $y_1 y^{(1)} + \cdots + y_n y^{(n)}$ is given by

$$\sum_{j \neq i} y_j \cdot (\lambda_i a_j) - y_i \cdot \left(\sum_{k \neq i} \lambda_k a_k\right) = -\lambda_i a_i y_i - y_i(1 - \lambda_i a_i) = -u y_i.$$

Hence $y = -u^{-1}(y_1 y^{(1)} + \cdots + y_n y^{(n)})$, showing that the $y^{(j)}$ generate the module of solutions to (2.1) in R^n.

Bézout domains. Let $\mathcal{L}_{\mathrm{gcd}} = \{0, 1, +, -, \cdot, (:)\}$ be the language obtained by augmenting the language $\mathcal{L}_{\mathrm{ring}}$ of rings by a binary function symbol (:). Every Bézout domain R can be

construed as an $\mathcal{L}_{\gcd}$-structure by interpreting (:) in the following way. For $a, b \in R$ let $\gcd(a, b)$ be a generator of the ideal (a, b) generated by a and b, chosen in such a way that

$$\gcd(a, b) = \gcd(b, a). \tag{2.2}$$

(For example, for $R = \mathbb{Z}$ we may choose $\gcd(a, b)$ to be the unique non-negative generator of (a, b).) The element

$$(a : b) := \begin{cases} \dfrac{a}{\gcd(a, b)} & \text{if } a \neq 0 \text{ or } b \neq 0, \\ 1 & \text{otherwise} \end{cases}$$

generates the ideal $(a) : (b) = \{c \in R : bc \in (a)\}$.

Note that by (2.2) for all $a, b \in R$,

$$b \cdot (a : b) = a \cdot (b : a) \tag{2.3}$$

and hence

$$(a : b) \cdot (bc : ac) = (b : a) \cdot (ac : bc) \quad \text{for all non-zero } c \in R. \tag{2.4}$$

LEMMA 2.14 *If R is a Bézout domain and $a = (a_1, \dots, a_n) \in R^n, a \neq 0$, then the module of solutions in R^n to* (2.1) *is generated by the special solutions*

$$y^{(i,j)} = [0, \dots, 0, (a_j : a_i), 0, \dots, 0, -(a_i : a_j), 0, \dots, 0]^{\mathrm{tr}} \in R^n, \quad 1 \leq i < j \leq n.$$

Proof. Suppose that R is a Bézout domain. Clearly the $y^{(i,j)}$ are solutions to (2.1), by (2.3). Let $0 \neq d \in R$ be a generator for $(a_1, \dots, a_n)R$. Then the linear homogeneous equation

$$\frac{a_1}{d} y_1 + \cdots + \frac{a_n}{d} y_n = 0$$

over R has the same solutions in R^n as (2.1), and for all $1 \leq i, j \leq n$ there exists a unit u of R such that $(a_i / d : a_j / d) = u \cdot (a_i : a_j)$ and $(a_j / d : a_i / d) = u \cdot (a_j : a_i)$, by (2.4). So replacing a_i by a_i / d for all i, if necessary, we may assume that

$$1 = \lambda_1 a_1 + \cdots + \lambda_n a_n \quad \text{for some } \lambda_1, \dots, \lambda_n \in R.$$

Let $y^{(1)}, \dots, y^{(n)}$ be as in the previous proposition. One shows easily that

$$y^{(i)} = \sum_{j=1}^{i=1} \lambda_i \gcd(a_i, a_j) \cdot y^{(j,i)} - \sum_{j=i+1}^{n} \lambda_j \gcd(a_i, a_j) \cdot y^{(i,j)}$$

for all $i = 1, \dots, n$. Therefore, since the $y^{(1)}, \dots, y^{(n)}$ generate the solution module of (2.1), so do the $y^{(i,j)}$ $(1 \leq i < j \leq n)$.

Lemma 2.14 and the discussion at the beginning of this subsection (applied to $\mathcal{L} = \mathcal{L}_{\gcd}$) yield the following fact. Here and below $C = (C_1, \dots, C_M)$.

COROLLARY 2.15 *Let $A(C) \in \mathbb{Z}[C]^{m\times n}$. One can construct elementary recursively (from A) a finite family $\{\varphi^{(\lambda)}(C)\}_{\lambda\in\Lambda}$ of quantifier-free $\mathcal{L}_{\mathrm{gcd}}$-formulae $\varphi^{(\lambda)}(C)$ and for each $\lambda \in \Lambda$ finitely many $n \times 1$ column vectors*

$$y^{(\lambda,1)}(C), \dots, y^{(\lambda,n)}(C)$$

whose entries are $\mathcal{L}_{\mathrm{gcd}}$-terms, such that for all Bézout domains R and $c \in R^M$, we have $R \vDash \bigvee_\lambda \varphi^{(\lambda)}(c)$, and if $\lambda \in \Lambda$ is such that $R \vDash \varphi^{(\lambda)}(c)$, then the vectors

$$y^{(\lambda,1)}(c), \dots, y^{(\lambda,n)}(c) \in R^n$$

are in $\mathrm{Sol}_R(A(c))$ and generate the R-module $\mathrm{Sol}_R(A(c))$.

This corollary slightly improves [**14**, Corollary 5.4], where a similar parametrization was given using terms in a larger language.

Valuation rings. Using Proposition 2.13 one shows the following easily.

LEMMA 2.16 *Let R be a valuation ring, $a = (a_1, \dots, a_n) \in R^n$, and $i \in \{1, \dots, n\}$ such that $a_i \neq 0$ divides a_j for all $j = 1, \dots, n$. The module of solutions to (2.1) in R^n is generated by*

$$y^{(j)} = [0, \dots, 0, a_j/a_i, 0, \dots, 0, -1, 0, \dots, 0]^{\mathrm{tr}} \in R^n, \quad j = 1, \dots, n,\ j \neq i.$$

(The ith component of $y^{(j)}$ is a_j/a_i and the jth component is -1.)

Let $\mathcal{L}_{\mathrm{div}}$ be $\mathcal{L}_{\mathrm{ring}} = \{0, 1, +, -, \cdot\}$ augmented by a binary predicate $|$, to be interpreted in every ring R as divisibility, that is, $a|b :\Leftrightarrow ac = b$ for some $c \in R$. Let also $\mathcal{L}_{\mathrm{div},D} = \mathcal{L}_{\mathrm{div}} \cup \{D\}$, where D is a 2-place function symbol, to be interpreted in every integral domain R as $D(a, b) := a/b$ if $b \neq 0$ and b divides a in R, and $D(a, b) := 0$ otherwise. Similarly to Corollary 2.15, the Lemma 2.16 yields the following.

COROLLARY 2.17 *Let $A(C) \in \mathbb{Z}[C]^{m\times n}$. One can construct elementary recursively (from A) a finite family $\{\psi^{(\lambda)}(C)\}_{\lambda\in\Lambda}$ of quantifier-free $\mathcal{L}_{\mathrm{div}}$-formulae $\psi^{(\lambda)}(C)$ and for each $\lambda \in \Lambda$ finitely many $n \times 1$ column vectors*

$$z^{(\lambda,1)}(C), \dots, z^{(\lambda,n)}(C)$$

whose entries $z_j^{(\lambda,i)}$ are $\mathcal{L}_{\mathrm{div},D}$-terms, such that for every valuation ring R and $c \in R^M$, we have $R \vDash \bigvee_\lambda \psi^{(\lambda)}(c)$, and if $\lambda \in \Lambda$ is such that $R \vDash \psi^{(\lambda)}(c)$, then the vectors

$$z^{(\lambda,1)}(c), \dots, z^{(\lambda,n)}(c) \in R^n$$

are in $\mathrm{Sol}_R(A(c))$ and generate the R-module $\mathrm{Sol}_R(A(c))$.

A flatness result. We finish this section by proving a fact about subrings of direct products of rings (Corollary 2.19 below) which is used in the next section.

Let $\{R^{(k)}\}_{k\in\mathbb{N}}$ be a family of rings and $R^* = \prod_k R^{(k)}$ its direct product. Given $k \in \mathbb{N}$ we identify $r \in R^{(k)}$ with the sequence $(r^{(l)}) \in R^*$ given by $r^{(l)} = 0$ for $l \neq k$ and $r^{(l)} = r$ for $l = k$. In this way, $R^{(k)}$ becomes an ideal of R^*. We write $\pi^{(k)} : R^* \to R^{(k)}$ for the projection onto the kth component: $\pi^{(k)}(y) = y^{(k)}$ for $y = (y^{(k)}) \in R^*$. We extend $\pi^{(k)}$ in the natural

way to a ring homomorphism $(R^*)^n \to (R^{(k)})^n$, denoted by the same symbol. Let S be a subring of R^*.

LEMMA 2.18 *Let M be a finitely generated S-submodule of S^n and M^* be an R^*-submodule of $(R^*)^n$ with $M^* \supseteq M$. If $\pi^{(k)}(M^*) = \pi^{(k)}(M)$ for all k, then $M^* = R^*M$ ($=$ the R^*-submodule of M^* generated by M).*

Proof. Let $g_1, \dots, g_m \in M$ be generators for the S-module M, and let $y \in M^*$. Then for every $k \in \mathbb{N}$ we can write $y^{(k)} = a_1^{(k)} g_1^{(k)} + \cdots + a_m^{(k)} g_m^{(k)}$ for some $a_i^{(k)} \in R^{(k)}$. Putting $a_i = (a_i^{(k)}) \in R^*$ we obtain $y = a_1 g_1 + \cdots + a_m g_m \in R^*M$ as required.

COROLLARY 2.19 *Suppose that S is coherent and contains $\bigoplus_k R^{(k)}$. Then R^* is a flat S-module.*

Proof. Let M^* be the module of syzygies in $(R^*)^n$ of a tuple $(f_1, \dots, f_n) \in S^n$, so $M = M^* \cap S^n$ is a finitely generated S-module. We have to show $R^*M = M^*$, and hence, by Lemma 2.18, that $\pi^{(k)}(M) = \pi^{(k)}(M^*)$ for every k. For this, let $y = (y_1, \dots, y_n) \in M^*$, so that $f_1 y_1 + \cdots + f_n y_n = 0$ Then $f_1 y_1^{(k)} + \cdots + f_n y_n^{(k)} = 0$ in R^* and hence $\pi^{(k)}(y) \in M^* \cap (R^{(k)})^n$. Since $R^{(k)} \subseteq S$ this yields $\pi^{(k)}(y) \in M$ and hence $\pi^{(k)}(y) = \pi^{(k)}(\pi^{(k)}(y)) \in \pi^{(k)}(M)$ as required.

3. Homogeneous linear equations in polynomial rings

In this section we will be concerned with the existence of uniform bounds for the degrees of generators for syzygy modules over polynomial rings. We define a *super coherent* class of rings to be one for which such bounds exist. This notion is related to 'stable coherence' introduced in [19]. We show that the class of semihereditary rings is super coherent, yielding Theorem A from the Introduction. We also prove Theorem D and discuss some strengthenings of Theorem A.

Stable coherence and super coherence. A ring R is called *stably coherent* if for every $N \geq 0$ the ring of polynomials $R[X_1, \dots, X_N]$ over R is coherent. We say that a class $\mathcal{C}$ of rings is stably coherent if every $R \in \mathcal{C}$ is stably coherent. For example, the class of Noetherian rings is stably coherent, by virtue of the Hilbert Basis Theorem. There exist coherent rings R which are not stably coherent [38]. We have the following theorem proved by Vasconcelos [21], after a conjecture by Sabbagh [31, p. 502]. For an efficient proof based on work of Alfonsi see [19, Chapter 7].

THEOREM 3.1 *The class of semihereditary rings is stably coherent.*

For the purpose of this section we introduce a notion related to stable coherence.

DEFINITION 3.2 Let $\alpha : \mathbb{N} \to \mathbb{N}$ and $\beta : \mathbb{N}^3 \to \mathbb{N}$. We call a ring $R(\alpha, \beta)$-*super coherent* if R is α-uniformly coherent, and for given N, d, $n \in \mathbb{N}$ and $f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of degree at most d, every solution to the homogeneous linear equation

$$f_1 y_1 + \cdots + f_n y_n = 0$$

is a linear combination of solutions of degree at most $\beta(N, d, n)$. We say that R is *super coherent* if it is (α, β)-super coherent for some functions α and β as above.

REMARKS Let R be (α, β)-super coherent. The localization R_U of R at a multiplicative subset U of R is (α, β)-super coherent. If I is a finitely generated ideal of R, then R/I is super coherent. If R is a faithfully flat extension of an α-uniformly coherent subring S, then S is (α, β)-super coherent. (These facts are immediate consequences of the definition.)

A super coherent ring is stably coherent. In fact we have the following.

LEMMA 3.3 *Given $\alpha : \mathbb{N} \to \mathbb{N}$ and $\beta : \mathbb{N}^3 \to \mathbb{N}$ there exists a function $\gamma : \mathbb{N}^3 \to \mathbb{N}$ with the property that for all (α, β)-super coherent rings R and all $f_1, \dots, f_n \in R[X]$ of degree at most d, the module of solutions in $R[X]$ to the homogeneous linear equation*

$$f_1 y_1 + \cdots + f_n y_n = 0 \tag{3.1}$$

is generated by $\gamma(N, d, n)$ many solutions of degree at most $\beta(N, d, n)$.

Proof. The R-module of solutions to the homogeneous linear equation (3.1) in $R[X]^n$ which have degree at most $\beta = \beta(N, d, n)$ is isomorphic to the module of solutions to a certain system of $m' := \binom{N + \beta + d}{N}$ homogeneous linear equations over R in $n' := n \cdot \binom{N + \beta}{N}$ indeterminates. Hence by Lemma 2.6 the former module can be generated by $\gamma(N, d, n) := \alpha^{m'}(n')$ many elements. These elements will then also generate the $R[X]$-module of solutions to (3.1) in $R[X]^n$.

If R is (α, β)-super coherent and of finite rank k, then we can take $\alpha(n) = nk$ (Corollary 2.11), and the function $(N, d, n) \mapsto \beta(N, d, n)$ and hence also the function $(N, d, n) \mapsto \gamma(N, d, n)$ can be chosen so as to not depend on n. For if we have a bound $\beta = \beta(N, d, n)$ for $n = \binom{N + d}{N} \cdot k$, then this β will also be a bound for all other values of n (by Lemma 2.10).

Lemma 3.3 extends to systems of homogeneous linear equations.

COROLLARY 3.4 *For any given $N, d, m, n \in \mathbb{N}$, $m, n \geq 1$ there exist natural numbers $\beta_m = \beta_m(N, d, n)$ and $\gamma_m = \gamma_m(N, d, n)$ with the property that for all (α, β)-super coherent rings R and all $m \times n$-matrices A with entries in $R[X] = R[X_1, \dots, X_N]$ of degree at most d, the module $\mathrm{Sol}_{R[X]}(A)$ is generated by γ_m elements of degree at most β_m.*

Proof. We proceed by induction on m, similar to the proof of Lemma 2.6. Clearly $\beta_1 = \beta$ and $\gamma_1 = \gamma$ as in Lemma 3.3 work for $m = 1$. Suppose $m > 1$, and let $N, d, n \in \mathbb{N}$ with $n \geq 1$. Let R be (α, β)-super coherent and A an $m \times n$-matrix with entries from $R[X] = R[X_1, \dots, X_N]$. Let $(f_1, \dots, f_n)$ be the first row of A and A' be the matrix consisting of the last $m - 1$ rows of A. Let the column vectors $z_1, \dots, z_\gamma$ of degree at most β generate the syzygies of $(f_1, \dots, f_n)$, and put $B = A' \cdot (z_1, \dots, z_\gamma)$, an $(m - 1) \times \gamma$-matrix with entries in $R[X]$. Here $\beta = \beta(N, d, n)$, and $\gamma = \gamma(N, d, n)$ is as in Lemma 3.3. Every solution $u = (u_1, \dots, u_\gamma)^{\mathrm{tr}} \in R[X]^\gamma$ to $Bu = 0$ gives rise to a solution $y = (y_1, \dots, y_n)^{tr} \in R[X]^n$ to $Ay = 0$ by setting $y = \sum_i u_i z_i$. This yields a one-to-one correspondence between the solutions to $Bu = 0$ and the solutions to $Ay = 0$. The degrees of the entries of B are bounded from above by $\beta + d$. By inductive hypothesis, there are $\gamma_{m-1}(N, \beta + d, \gamma)$ generators of degree at most $\beta_{m-1}(N, \beta + d, \gamma)$ for the module of solutions to $Bu = 0$. These give rise to $\gamma_{m-1}(N, \beta + d, \gamma)$ generators of degree at most $\beta \cdot \beta_{m-1}(N, \beta + d, \gamma)$ for the module of solutions to $Ay = 0$. Hence we can take $\beta_m(N, d, n) = \beta \cdot \beta_{m-1}(N, \beta + d, \gamma)$ and $\gamma_m(N, d, n) = \gamma_{m-1}(N, \beta + d, \gamma)$.

REMARK The proof shows that if $(N, d, n) \mapsto \beta(N, d, n)$ does not depend on n, then $\beta_m(N, d, n)$ and $\gamma_m(N, d, n)$ can be chosen independent of n, for all $m \geq 1$.

Let R be a ring. We say that an $R[X]$-submodule of $R[X]^m$ is *of type* (n, d) (where $n, d \in \mathbb{N}$) if it is generated by n elements of degree at most d. Corollary 3.4 and standard arguments (see, for example [**2**, proof of Proposition 4.7]) yield the following.

COROLLARY 3.5 *Given $\alpha : \mathbb{N} \to \mathbb{N}$ and $\beta : \mathbb{N}^3 \to \mathbb{N}$ there exists a function $\tau : \mathbb{N}^4 \to \mathbb{N}^2$ with the following properties: if R is an (α, β)-super coherent ring and M, M' are finitely generated submodules of the free $R[X]$-module $R[X]^m$ of type (n, d), then the $R[X]$-module $M \cap M'$ and the ideal $M' : M$ of $R[X] = R[X_1, \dots, X_N]$ are of type $\tau(N, d, m, n)$. If $\beta(N, d, n)$ does not depend on n, then $\tau(N, d, m, n)$ also does not depend on n.*

A class $\mathcal{C}$ of rings is called (α, β)-*super coherent* if every ring $R \in \mathcal{C}$ is (α, β)-super coherent. We say that $\mathcal{C}$ is *super coherent* if $\mathcal{C}$ is (α, β)-super coherent for some α, β as above. The main result of this section is the following.

THEOREM 3.6 *Let $\mathcal{C}$ be a class of rings which is closed under direct products. Then $\mathcal{C}$ is super coherent if and only if $\mathcal{C}$ is stably coherent.*

In particular, it then follows that a ring R is super coherent if and only if $R^{\mathbb{N}}$ is stably coherent. The theorem together with Lemma 1.2 and Theorem 3.1 imply the following.

COROLLARY 3.7 *The class of semihereditary rings is super coherent.*

REMARKS Corollary 3.7 implies Theorem A stated in the Introduction. By Lemma 2.9 and [**2**, Theorem 4.1], the class of hereditary rings is (α, β)-super coherent with $\alpha(n) = n$ and $\beta(N, d) = (2d)^{2^{O(N \log(N+1))}}$.

Before we give a proof of Theorem 3.6, we establish some auxiliary facts. Let $\mathcal{F}$ be a filter on $\mathbb{N}$ and $\{R^{(k)}\}_{k \in N}$ a family of rings indexed by $\mathbb{N}$. Let $R = \prod_k R^{(k)}$ and $R^* = \prod_k R^{(k)} / \mathcal{F}$. Let $R^*[X]$ be the ring of polynomials in indeterminates $X = (X_1, \dots, X_N)$ with coefficients from R^*, and put $R[X]^* = \prod_k R^{(k)}[X] / \mathcal{F}$. We have a natural embedding of R^*-algebras $R^*[X] \to R[X]^*$ induced by $X_i \mapsto X_i / \mathcal{F} \in R[X]^*$ for $i = 1, \dots, N$. We consider $R^*[X]$ as a subring of $R[X]^*$ via this embedding. Note that if $\mathcal{F} = \{\mathbb{N}\}$, then $R^*[X] = \left(\prod_k R^{(k)}\right)[X]$ becomes identified in this way with the R-subalgebra of the direct product $R[X]^* = \prod_k R^{(k)}[X]$ consisting of all sequences $(f^{(k)})$ of polynomials whose degrees are bounded, that is, such that there exists $d \in \mathbb{N}$ with $\deg f^{(k)} \leq d$ for all k.

LEMMA 3.8 *The following are equivalent, for a uniformly coherent class $\mathcal{C}$ of rings:*

(1) *$\mathcal{C}$ is super coherent;*
(2) *for every family $\{R^{(k)}\}_{k \in \mathbb{N}}$ of rings in $\mathcal{C}$, every filter $\mathcal{F}$ on $\mathbb{N}$ and every $N \in \mathbb{N}$, the ring $R[X]^*$ is flat over $R^*[X]$, where $X = (X_1, \dots, X_N)$;*
(3) *for every family $\{R^{(k)}\}_{k \in \mathbb{N}}$ of rings in $\mathcal{C}$ and every $N \in \mathbb{N}$, the ring $\prod_k R^{(k)}[X]$ is flat over $\left(\prod_k R^{(k)}\right)[X]$, with $X = (X_1, \dots, X_N)$.*

(*In particular, a uniformly coherent ring R is super coherent if and only if $R[X]^{\mathbb{N}}$ is flat over $R^N[X]$.*)

Proof. Suppose $\mathcal{C}$ is (α, β)-super coherent, let $N, d, n \in \mathbb{N}$, $n \geq 1$, be fixed, and let $\gamma = \gamma(N, d, n)$ be as in Lemma 3.3. Let

$$f_1(C, X), \dots, f_n(C, X) \in \mathbb{Z}[C, X]$$

be general polynomials of degree d in the indeterminates $X = (X_1, \dots, X_N)$, where $C = (C_1, \dots, C_M)$ are parametric variables. It is easy to write down a Horn formula $\varphi(C)$ (where C is considered as a tuple of variables of the ring sort) which, for a given ring R and $c \in R^M$, holds

in $R[X]$ (considered as a module over itself) for c exactly if there exist γ solutions to the equation

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

in $R[X]$ of degree at most β from which every solution to this homogeneous equation in $R[X]$ can be obtained as an $R[X]$-linear combination. Hence (2) is a consequence of Theorem 1.1. The implication (2) $\Rightarrow$ (3) follows by taking $\mathcal{F} = \{\mathbb{N}\}$. For (3) $\Rightarrow$ (1) suppose for a contradiction that (3) holds but $\mathcal{C}$ is not super coherent. So there exist $N, d, n \in \mathbb{N}$ with $n \geq 1$, and for every $k \in \mathbb{N}$ a ring $R^{(k)} \in \mathcal{C}$ and polynomials $f_1^{(k)}, \ldots, f_n^{(k)} \in R^{(k)}[X] = R^{(k)}[X_1, \ldots, X_N]$ of degree at most d such that the module of solutions in $R^{(k)}[X]$ to the homogeneous linear equation

$$f_1^{(k)}y_1 + \cdots + f_n^{(k)}y_n = 0 \tag{3.2}$$

cannot be generated by elements of degree k or less, that is, there exists a column vector

$$y^{(k)} = \left[y_1^{(k)}, \ldots, y_n^{(k)}\right]^{\mathrm{tr}} \in R^{(k)}[X]^n$$

with

$$f_1^{(k)}y_1^{(k)} + \cdots + f_n^{(k)}y_n^{(k)} = 0$$

which is not an $R^{(k)}[X]$-linear combination of solutions of degree at most k. Put

$$R^* := \prod_k R^{(k)}, \quad R[X]^* := \prod_k R^{(k)}[X].$$

Write each polynomial $f_i^{(k)}$ as

$$f_i^{(k)} = \sum_\nu a_{i,\nu}^{(k)} X^\nu,$$

where the sum ranges over all $\nu = (\nu_1, \ldots, \nu_N) \in \mathbb{N}^N$ and $a_{i,\nu}^{(k)} \in R^{(k)}, X^\nu = X_1^{\nu_1} \cdots X_N^{\nu_N}$. We have $a_{i,\nu}^{(k)} = 0$ if $|\nu| := \nu_1 + \cdots + \nu_N > d$. Hence

$$f_i = \sum_\nu a_{i,\nu} X^\nu \in R^*[X],$$

where $a_{i,\nu} = (a_{i,\nu}^{(k)})_{k\in\mathbb{N}} \in R^*$, with $a_{i,\nu} = 0$ if $|\nu| > d$. The column vector $y = [y_1, \ldots, y_n]^{\mathrm{tr}}$, where $y_i = (y_i^{(k)}) \in R[X]^*$, is a solution to the homogeneous linear equation

$$f_1y_1 + \cdots + f_ny_n = 0.$$

Since $R[X]^*$ is flat over $R^*[X]$, y is an $R[X]^*$-linear combination of certain solutions $z_1, \ldots, z_m \in (R^*[X])^n$. Let k be an integer larger than the degrees of $z_1, \ldots, z_m$. It follows that $y^{(k)} = \pi^{(k)}(y)$ is a linear combination of the solutions

$$\pi^{(k)}(z_1), \ldots, \pi^{(k)}(z_m) \in (R^{(k)}[X])^n$$

to (3.2) which have degree at most k. This is a contradiction to the choice of $y^{(k)}$.

We now prove Theorem 3.6. Let $\mathcal{C}$ be a class of rings which is closed under direct products. We have already remarked that any super coherent ring is stably coherent. Suppose conversely that $\mathcal{C}$ is stably coherent. By Lemma 2.8, $\mathcal{C}$ is uniformly coherent. In order to show that $\mathcal{C}$ is super coherent, we have to prove that for every family $\{R^{(k)}\}_{k\in\mathbb{N}}$ of rings in $\mathcal{C}$ and every integer $N \geq 0$, $R[X]^* = \prod_k R^{(k)}[X]$ is flat over $R^*[X] = \left(\prod_k R^{(k)}\right)[X]$, with $X = (X_1, \ldots, X_N)$ (by Lemma 3.8). Since $\mathcal{C}$ is closed under direct products and stably coherent, $R^*[X]$ is coherent. The subring $R^*[X]$ of $R[X]^*$ contains $\oplus_k(R^{(k)}[X])$. The claim now follows from Corollary 2.19.

REMARK The hypothesis of Theorem 3.6 is cannot be dropped, as the class $\mathcal{G}_2$ of coherent rings of global dimension 2 shows. (See, for example **[19]** for the definition of the global dimension of a ring.) By a theorem of Greenberg and Vasconcelos **[21]**, $\mathcal{G}_2$ is stably coherent. However, there exist rings in $\mathcal{G}_2$ which are not super coherent. For example let $R = \mathbb{Q}[[U, V]]$, where U, V are distinct indeterminates, and consider the ideals

$$I = (U - VX), \quad J_d = (UV^d, U^d - 2V^d)$$

of the polynomial ring $R[X]$, where X is a single indeterminate and $d \geq 4$. Then $I \cap J_d$ cannot be generated by polynomials of degree less than d, see **[38]**. By Corollary 3.5 it follows that R is not super coherent.

Model-theoretic consequences. Let now $A(C, X) = (a_{ij}(C, X))$ be an $m \times n$-matrix with entries $a_{ij}(C, X) \in \mathbb{Z}[C, X]$, where $C = (C_1, \ldots, C_M)$. The following fact is an immediate consequence of Corollaries 2.15 and 3.7.

COROLLARY 3.9 *There exists a finite family* $\{\varphi^{(\lambda)}(C)\}_{\lambda\in\Lambda}$ *of quantifier-free* $\mathcal{L}_{\mathrm{gcd}}$*-formulae* $\varphi^{(\lambda)}(C)$ *and for each* $\lambda \in \Lambda$ *finitely many* $n \times 1$ *column vectors*

$$y^{(\lambda,1)}(C, X), \ldots, y^{(\lambda,K)}(C, X) \quad (K \in \mathbb{N})$$

whose entries are $\mathcal{L}_{\mathrm{gcd}}$*-terms in the variables (C,X), polynomial in X, such that for all Bézout domains R and* $c \in R^M$*, we have* $R \vDash \bigvee_\lambda \varphi^{(\lambda)}(c)$*, and if* $\lambda \in \Lambda$ *is such that* $R \vDash \varphi^{(\lambda)}(c)$*, then the vectors*

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

are in $\mathrm{Sol}_{R[X]}(A(c, X))$ *and generate the* $R[X]$*-module* $\mathrm{Sol}_{R[X]}(A(c, X))$.

REMARK The case $m = 1$, $R = \mathbb{Z}$ of the corollary yields Theorem D of the Introduction.

For the case of valuation rings, combining Corollaries 2.17 and 3.7 yields the following.

COROLLARY 3.10 *There exists a finite family* $\{\psi^{(\lambda)}(C)\}_{\lambda\in\Lambda}$ *of quantifier-free* $\mathcal{L}_{\mathrm{div}}$*-formulae* $\psi^{(\lambda)}(C)$ *and for each* $\lambda \in \Lambda$ *finitely many column vectors*

$$z^{(\lambda,1)}(C, X), \ldots, z^{(\lambda,K)}(C, X) \quad (K \in \mathbb{N})$$

whose entries are $\mathcal{L}_{\mathrm{div},D}$*-terms, polynomial in X, such that for all valuation rings R and* $c \in R^M$*,*

we have $R \models \bigvee_\lambda \psi^{(\lambda)}(c)$, *and if* $\lambda \in \Lambda$ *is such that* $R \models \psi^{(\lambda)}(c)$, *then*

$$z^{(\lambda,1)}(c,X), \dots, z^{(\lambda,K)}(c,X) \in R[X]^n$$

are in $\mathrm{Sol}_{R[X]}(A(c,X))$ *and generate* $\mathrm{Sol}_{R[X]}(A(c,X))$.

REMARK The remark following Corollary 3.7 shows that from $A(C,X)$ one can (elementary recursively) *construct* a finite family $\{\varphi^{(\lambda)}(C)\}$ of quantifier-free $\mathcal{L}_{\mathrm{gcd}}$-formulae and corresponding column vectors $y^{(\lambda,k)}$ which satisfy the property expressed in Corollary 3.9 *for every principal ideal domain R*. Similarly, from $A(C,X)$ one can explicitly construct the objects $\psi^{(\lambda)}$ and $z^{(\lambda,k)}$ having the properties stated in the previous corollary *for every DVR R*.

Let $A'(C,X) \in \mathbb{Z}[C,X]^{m\times n'}$, where $n' \in \mathbb{N}$, $n' \geq 1$. For each ring R and $c \in R^M$, we may consider the $R[X]$-submodules $M(c,X)$ and $M'(c,X)$ of the free $R[X]$-module $R[X]^m$ generated by the columns of $A(c,X)$ and $A'(c,X)$, respectively. Corollary 3.10 immediately implies the uniformity of certain module-theoretic operations on $M(c,X)$ and $M'(c,X)$.

COROLLARY 3.11 *There exists a finite family* $\{\theta^{(\lambda)}(C)\}_{\lambda\in\Lambda}$ *of quantifier-free* $\mathcal{L}_{\mathrm{div}}$*-formulae, and for each* $\lambda \in \Lambda$ *an integer* $K \geq 1$, *an* $m \times K$ *matrix* $B^{(\lambda)}(C,X)$ *consisting of* $\mathcal{L}_{\mathrm{div,D}}$*-terms, polynomial in X, and* $\mathcal{L}_{\mathrm{div,D}}$*-terms*

$$u^{(\lambda,1)}(C,X), \dots, u^{(\lambda,K)}(C,X),$$

polynomial in X, with the following property: For every valuation ring R and $c \in R^M$, *we have* $R \models \bigvee_{\lambda\in\Lambda} \theta^{(\lambda)}$, *and if* $R \models \theta^{(\lambda)}(c)$, *then the* $R[X]$*-module* $M(c,X) \cap M'(c,X)$ *is generated by the columns of the matrix* $B^{(\lambda)}(c,X)$, *and the ideal* $M'(c,X) : M(c,X)$ *of* $R[X]$ *is generated by* $u^{(\lambda,1)}(c,X), \dots, u^{(\lambda,K)}(c,X) \in R[X]$.

We leave it to the reader to formulate a similar result for Bézout domains, using Corollary 3.9.

Extremely coherent rings. In the following lemma, let $\mathcal{C}$ be a class of rings which is closed under direct products and (α,β)-super coherent, and let $\gamma : \mathbb{N}^3 \to \mathbb{N}$ be as in Lemma 3.3.

LEMMA 3.12 *There exists a function* $\delta : \mathbb{N}^4 \to \mathbb{N}$ *with the following property. Given* $R \in \mathcal{C}$ *and* $f_1, \dots, f_n \in R[X]$ *of degree at most d, where* $X = (X_1, \dots, X_N)$, *there exist solutions* $y^{(1)}, \dots, y^{(\gamma)} \in R[X]^n$ *of degree at most* $\beta(N,d,n)$ *to the homogeneous linear equation*

$$f_1 y_1 + \cdots + f_n y_n = 0 \tag{3.3}$$

in $R[X]^n$ *such that every solution* $y \in R[X]^n$ *to (3.3) can be written as*

$$y = a_1 y^{(1)} + \cdots + a_\gamma y^{(\gamma)} \quad (\gamma = \gamma(N,d,n))$$

with $a_1, \dots, a_\gamma \in R[X]$ *of degree at most* $\delta(N,d,e,n)$, *where* $e = \deg(y)$.

Proof. In order to establish the existence of a function δ with the required property, we first note that it suffices to show the following seemingly weaker statement.

(*) For any $N,d,e,n \in \mathbb{N}$, $n \geq 1$, there exists an integer $\delta = \delta(N,d,e,n) \geq 0$ such that given $R \in \mathcal{C}$ and $f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of degree at most d, where $X = (X_1, \dots, X_N)$, every solution $y \in R[X]^n$ to (3.3) of degree at most e can be written as

$$y = b_1 z^{(1)} + \cdots + b_\gamma z^{(\gamma)} \quad (\gamma = \gamma(N,d,n))$$

with certain solutions $z^{(1)}, \dots, z^{(\gamma)} \in R[X]^n$ of degree at most $\beta(N,d,n)$ and $b_1, \dots, b_\gamma \in R[X]$ of degree at most δ.

For suppose we have established this statement, and let $R \in \mathcal{C}$ and $f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of degree at most d be given. Consider the R-submodule M of $R[X]^n$ consisting of those solutions to (3.3) which have degree at most $\beta(N,d,n)$. By the proof of Lemma 3.3, the R-module M is generated by $\gamma = \gamma(N,d,n)$ of its elements, say $y^{(1)}, \dots, y^{(\gamma)}$. By (*) any solution $y \in R[X]^n$ to (3.3) of degree at most e can be written in the form $y = b_1 z^{(1)} + \cdots + b_\gamma z^{(\gamma)}$ with certain solutions $z^{(1)}, \dots, z^{(\gamma)} \in R[X]^n$ of degree at most $\beta(N,d,n)$ and $b_1, \dots, b_\gamma \in R[X]$ of degree at most δ. Then $z^{(i)} \in M$, so expressing each $z^{(i)}$ as an R-linear combination of the $y^{(j)}$ yields y as an $R[X]$-linear combination of $y^{(1)}, \dots, y^{(\gamma)}$ with coefficients of degree at most δ, as required.

Now suppose for a contradiction that (*) is false, that is, there exist $N, d, e, n \in \mathbb{N}$, $n \geq 1$, such that for every $k \in \mathbb{N}$ we find a ring $R^{(k)} \in \mathcal{C}$, $f_1^{(k)}, \dots, f_n^{(k)} \in R^{(k)}[X] = R^{(k)}[X_1, \dots, X_N]$ of degree at most d, and a solution $y^{(k)} \in R^{(k)}[X]^n$ to the equation $f_1^{(k)} y_1 + \cdots + f_n^{(k)} y_n = 0$ of degree at most e which cannot be written as a linear combination of $\gamma(N,d,n)$ solutions of degree at most $\beta(N,d,n)$ with coefficients in $R^{(k)}[X]$ of degree at most k. Put $R^* = \prod_k R^{(k)}$ and $f_i = (f_i^{(k)}) \in R^*[X]$, $y_i = (y_i^{(k)}) \in R^*[X]$. Then $y = [y_1, \dots, y_n]^{\mathrm{tr}}$ is a solution to the homogeneous equation $f_1 y_1 + \cdots + f_n y_n = 0$ which cannot be written as a linear combination of $\gamma(N,d,n)$ solutions of degree at most $\beta(N,d,n)$. By virtue of Lemma 3.3, this contradicts the fact that $R^* \in \mathcal{C}$ is (α,β)-coherent.

REMARK The proof shows that if there exists an integer $k > 0$ such that every $R \in \mathcal{C}$ is of finite rank at most k, then the function $(N,d,e,n) \mapsto \delta(N,d,e,n)$ can be chosen not to depend on n.

Let us call a class $\mathcal{C}$ of rings (α, β, δ)-*extremely coherent* if $\mathcal{C}$ is (α,β)-super coherent and $\delta : \mathbb{N}^4 \to \mathbb{N}$ satisfies the conclusion of the previous lemma, with γ as in Lemma 3.3. We say that $\mathcal{C}$ is extremely coherent if it is (α, β, δ)-extremely coherent for some choice of uniformity functions α, β, δ. The last lemma yields a refinement of the 'if' direction of Theorem 3.6:

COROLLARY 3.13 *A class of rings which is closed under direct products and stably coherent is extremely coherent.*

We say that a ring R is (α, β, δ)-extremely coherent if the class $\mathcal{C} = \{R\}$ is (α, β, δ)-extremely coherent.

LEMMA 3.14 *Let α, β, γ and δ be as above.*

(1) *Let $\{R^{(k)}\}_{k \in \mathbb{N}}$ be a family of (α, β, δ)-extremely coherent rings. For any filter $\mathcal{F}$ on $\mathbb{N}$, the reduced product $\prod_k R^{(k)} / \mathcal{F}$ is (α, β, δ)-extremely coherent.*
(2) *Let $R \subseteq S$ be a faithfully flat ring extension. If R is α-uniformly coherent and S is (α, β, δ)-extremely coherent, then R is (α, β, δ)-extremely coherent.*

Proof. Part (1) follows from Theorem 1.1 on Horn formulae. For (2) suppose that S is an (α, β, δ)-extremely coherent ring, faithfully flat over the α-uniformly coherent subring R. Then R is (α,β)-super coherent; see the remarks following Definition 3.2. Let $f_1, \dots, f_n \in R[X]$ be of degree at most d. By Lemma 3.3 there exist generators $y^{(1)}, \dots, y^{(\gamma)} \in R[X]^n$ of degree at most $\beta(N,d,n)$ for the module of syzygies of $f = (f_1, \dots, f_n)$ in $R[X]$; here $\gamma = \gamma(N,d,n)$. Since S is (α, β, δ)-extremely coherent, there also exist syzygies $z^{(1)}, \dots, z^{(\gamma)} \in S[X]^n$ of f of degree at

most $\beta(N,d,n)$ such that every syzygy $y \in S[X]^n$ of f can be written as a linear combination

$$y = b_1 z^{(1)} + \cdots + b_\gamma z^{(\gamma)}$$

with $b_1, \ldots, b_\gamma \in S[X]$ of degree at most $\delta(N,d,e,n)$, where $\gamma = \gamma(N,d,n)$ and $e = \deg(y)$. By faithful flatness of S over R, every $z^{(j)}$ is an S-linear combination of $y^{(1)}, \ldots, y^{(\gamma)}$, and if we have $y \in R[X]^n$, then $y = a_1 y^{(1)} + \cdots + a_\gamma y^{(\gamma)}$ for some $a_1, \ldots, a_\gamma \in R[X]$ of degree at most $\delta(N,d,e,n)$ where $\gamma = \gamma(N,d,n)$.

Question. Is the class of (α,β)-super coherent rings closed under direct products? Equivalently, is there $\delta : \mathbb{N}^4 \to \mathbb{N}$ such that every (α,β)-super coherent ring is (α,β,δ)-extremely coherent? (The equivalence follows from part (1) of the previous lemma and Corollary 3.13 applied to $\mathcal{C} =$ the class of all (α,β)-coherent rings.)

Before we give a list of examples and further questions, let us remark that if R is a coherent ring, then the canonical embedding of R into the direct product $S = \prod_{\mathfrak{m}} R_{\mathfrak{m}}$ of its localizations $R_{\mathfrak{m}}$ at maximal ideals $\mathfrak{m}$ of R makes S into a faithfully flat R-module; see, for example [**31**, pp. 502–503].

EXAMPLES

(1) By the results of Hermann [**24**] and Seidenberg [**36**], the class of fields is extremely coherent with uniformity functions $\alpha(n) = n$, $\beta(N,d) = (2d)^{2^{N-1}}$ and $\delta(N,d,e) = (2d')^{2^{N-1}}$ for $N > 0$, where $d' = \max\{e, \beta(N,d)\}$.

(2) The localization $R_{\mathfrak{m}}$ of a von Neumann regular ring R at one of its maximal ideals $\mathfrak{m}$ is a field. By the above remark, Lemma 3.14 and example (1), this implies that the class of von Neumann regular rings is extremely coherent with the same uniformity functions as in (1). (This was first observed by Sabbagh [31].)

(3) The class of DVRs is extremely coherent, by [**2**, proof of Theorem 4.1]; see also the remark following Corollary 3.7.

(4) The class of hereditary rings is extremely coherent with the same uniformity functions as in example (3), by the remark above and Lemma 3.14.

(5) The class $\mathcal{S}$ of semihereditary rings is extremely coherent, by Corollary 3.13. The nature of the associated uniformity functions β and δ is somewhat mysterious. Can they be chosen to be doubly exponential similar to the ones in example (1)? (In trying to answer this question it is enough to restrict to the subclass of $\mathcal{S}$ consisting of all *valuation rings*).

Rings with nilpotents. So far, we have concentrated on classes of *reduced* rings, such as the class $\mathcal{S}$ of semihereditary rings. We will now exhibit certain extremely coherent classes of rings extending $\mathcal{S}$ which also contain rings with non-zero nilradical. We say that a module M over a ring R is *m-presented* (for a given $m \geq 1$) if there exists an exact sequence $R^m \to R^m \to M \to 0$ of R-linear maps. Using Theorem 1.1 it is routine to show the following.

LEMMA 3.15 *Let $\{R^{(k)}\}_{k\in\mathbb{N}}$ be a family of rings and for each k let $M^{(k)}$ be an m-presented $R^{(k)}$-module. Then $M = \prod_k M^{(k)}$ is an m-presented R-module, where $R = \prod_k R^{(k)}$.*

EXAMPLE If R is a Noetherian local ring of embedding dimension e, then any finitely generated R-module of length m is em-presented. (An easy consequence of Nakayama's lemma.)

DEFINITION 3.16 For fixed $m \geq 1$ let $\mathcal{S}_m$ be the class of rings R such that

(1) Nil(R)is nilpotent of index at most m, that is, $\mathrm{Nil}(R)^m = \{0\}$;
(2) Nil(R) is m-presented;
(3) R/Nil(R) is semihereditary.

Clearly we have $\mathcal{S} = \mathcal{S}_1 \subseteq \mathcal{S}_m$ for every $m \geq 1$.

PROPOSITION 3.17 *The class $\mathcal{S}_m$ is closed under direct products and extremely coherent. It contains all Artinian rings of length at most $\sqrt{m}$.*

Proof. Let $R^{(k)}(k \in \mathbb{N})$ be rings whose nilradical is nilpotent of index at most m. Then the same is true for $R = \prod_k R^{(k)}$, and $\mathrm{Nil}(R) = \prod_k \mathrm{Nil}(R^{(k)})$. Moreover, if each $\mathrm{Nil}(R^{(k)})$ is an m-presented $R^{(k)}$-module, then Nil(R) is an m-presented R-module, by Lemma 3.15. If each quotient ring $R^{(k)}/\mathrm{Nil}(R^{(k)})$ is semihereditary, then so is $R/\mathrm{Nil}(R) \cong \prod_k R^{(k)}/\mathrm{Nil}(R^{(k)})$, by Lemma 1.2. It follows that $\mathcal{S}_m$ is closed under direct products.

In order to show that $\mathcal{S}_m$ is extremely coherent, it remains to show (by Corollary 3.13) that for every $R \in \mathcal{S}_m$ and every integer $N \geq 0$ the polynomial ring $R[X] = R[X_1, \ldots, X_N]$ is coherent. Since $R/\mathrm{Nil}(R)$ is semihereditary, the ring $(R/\mathrm{Nil}(R))[X]$ is coherent, by Theorem 3.1. The natural surjection $R \to R/\mathrm{Nil}(R)$ induces a ring homomorphism

$$\phi : R[X] \to (R/\mathrm{Nil}(R))[X]$$

with finitely generated nilpotent kernel $\ker \phi = \mathrm{Nil}(R)R[X]$. Now Nil($R$) is a finitely presented R-module, hence $\mathrm{Nil}(R)R[X]$ is a finitely presented $R[X]$-module (since the ring extension $R \to R[X]$ is faithfully flat). It follows that $R[X]$ is coherent, by part (2) of Proposition 2.5.

Every Artinian ring is isomorphic to a finite direct product of local Artinian rings. Hence, since $\mathcal{S}_m$ is closed under direct products, it suffices to show that $\mathcal{S}_m$ contains all local Artinian rings $(R,\mathfrak{m})$ of length at most $\sqrt{m}$. In this case we have $\mathrm{Nil}(R) = \mathfrak{m}$ and $\mathfrak{m}^m = \{0\}$. By the remark before Lemma 3.15, $\mathfrak{m}$ is m-presented. Moreover $R/\mathrm{Nil}(R) = R/\mathfrak{m}$ is a field, hence semihereditary. Therefore $R \in \mathcal{S}_m$.

COROLLARY 3.18 *For each triple $(N, d, l) \in \mathbb{N}^3$ there exists a natural number $\beta = \beta(N, d, l)$ such that for every Artinian ring R of length at most l and polynomials $f_1, \ldots, f_n \in R[X] = R[X_1, \ldots, X_N]$ of degree at most d, the module of syzygies of $(f_1, \ldots, f_n)$ in $R[X]$ can be generated by elements of $R[X]^n$ of degree at most β.*

REMARK For Artinian local rings, Corollary 3.18 was first proved by Schoutens [32].

4. Inhomogeneous linear equations in polynomial rings

The main purpose of this section is to show Theorems B and C from the Introduction. On our way to proving Theorem C we will also treat the question of defining membership in the nilradical of a finitely generated ideal in a polynomial ring over an arbitrary ring.

Uniform rings. Let $\beta : \mathbb{N}^3 \to \mathbb{N}$. We say that a ring R is *β-uniform* if for given $N, d, n \in \mathbb{N}$ and $f_1, \ldots, f_n \in R[X] = R[X_1, \ldots, X_N]$ of degree at most d, if $1 \in (f_1, \ldots, f_n)R[X]$, then there exist $g_1, \ldots, g_n \in R[X]$ of degree at most $\beta(N, d, n)$ such that

$$1 = f_1 g_1 + \cdots + f_n g_n.$$

We say that R is *uniform* if R is β-uniform for some function β as above. A class $\mathcal{C}$ of rings is called β-uniform if every $R \in \mathcal{C}$ is β-uniform, and we say that $\mathcal{C}$ is uniform if $\mathcal{C}$ is β-uniform for some β.

If a ring R is uniform and of finite rank, then R is β-uniform for some function $(N, d, n) \mapsto \beta(N, d, n)$ which does not depend on n; see the remark following Lemma 3.3. The proof of the next lemma is similar to the proof of Lemma 3.8. We leave the details to the reader.

LEMMA 4.1 *Let $\mathcal{C}$ be a class of rings. The following are equivalent:*

(1) *$\mathcal{C}$ is uniform;*
(2) *for every family $\{R^{(k)}\}_{k\in\mathbb{N}}$ of rings in $\mathcal{C}$, every filter $\mathcal{F}$ on $\mathbb{N}$ and every $N \in \mathbb{N}$, if I is a finitely generated ideal of $R^*[X]$ with $1 \notin I$, then $1 \notin IR[X]^*$, where $X = (X_1, \dots, X_N)$;*
(3) *for every family $\{R^{(k)}\}_{k\in\mathbb{N}}$ of rings in $\mathcal{C}$ and every $N \in \mathbb{N}$, a finitely generated proper ideal of $\left(\prod_k R^{(k)}\right)[X]$ remains proper after extension to $\prod_k R^{(k)}[X]$, with $X = (X_1, \dots, X_N)$.*

Of particular interest are classes of rings which are both uniform and super coherent. Standard arguments (see, for example, **[2]**) show the following.

LEMMA 4.2 *Let $\mathcal{C}$ be a uniform and super coherent class of rings. Then, for any given N, d, m, $n \in \mathbb{N}, m, n \geq 1$, there exists a natural number $\beta_m = \beta_m(N, d, n)$ with the property that for all $R \in \mathcal{C}$, all $m \times n$-matrices A and all column vectors b with entries in $R[X] = R[X_1, \dots, X_N]$ of degree at most d, if the system $Ay = b$ is solvable in $R[X]$, then it has a solution in $R[X]$ all of whose entries have degree bounded from above by β_m. (In particular, $\mathcal{C}$ is extremely coherent.)*

Using the fact that a ring extension $R \subseteq S$ is faithfully flat if and only if S is a flat R-module and $IS \neq S$ for every finitely generated ideal $I \neq R$ of R, Lemmas 3.8 and 4.1 imply the following.

COROLLARY 4.3 *Let $\mathcal{C}$ be a uniformly coherent class of rings. The following are equivalent:*

(1) *$\mathcal{C}$ is uniform and super coherent;*
(2) *for every family $\{R^{(k)}\}_{k\in\mathbb{N}}$ of rings in $\mathcal{C}$, every filter $\mathcal{F}$ on $\mathbb{N}$ and every $N \in \mathbb{N}$, the ring $R[X]^*$ is faithfully flat over $R^*[X]$, where $X = (X_1, \dots, X_N)$;*
(3) *for every family $\{R^{(k)}\}_{k\in\mathbb{N}}$ of rings in $\mathcal{C}$ and every integer $N \geq 0$, the ring $\prod_k R^{(k)}[X]$ is faithfully flat over its subring $\left(\prod_k R^{(k)}\right)[X]$, with $X = (X_1, \dots, X_N)$.*

The first goal of this section is to show that uniformity is a rather serious restriction.

THEOREM 4.4 *A class $\mathcal{C}$ of rings is uniform if and only if there exists $m \geq 1$ such that for every $R \in \mathcal{C}$, the nilradical $\mathrm{Nil}(R)$ of R is nilpotent of index at most m and $R/\mathrm{Nil}(R)$ is von Neumann regular.*

Before we begin the proof, we establish several lemmas. For a proof of the first one see **[11**, Lemma 2.3**]**. An element r of a ring R is called *von Neumann regular* if r^2 divides r in R. If r is both von Neumann regular and nilpotent, then $r = 0$. A ring R is von Neumann regular if and only if every $r \in R$ is von Neumann regular.

LEMMA 4.5 *Let R be a ring, $r \in R$, $m \in \mathbb{N}$. Then r^{m+1} divides r^m if and only if $r = r_1 + s$ with $r_1 \in R$ von Neumann regular and $s \in R$ with $s^m = 0$.*

The next lemma shows that the class of von Neumann regular rings is uniform.

LEMMA 4.6 *Let R be a von Neumann regular ring, $N \geq 0$, and $f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of degree at most d. If $1 \in (f_1, \dots, f_n)R[X]$, then there exist polynomials $g_1, \dots, g_n \in R[X]$ of degree at most $\beta(N,d) = d^{N+1}$ such that $1 = f_1 g_1 + \cdots + f_n g_n$.*

Proof. Since R is von Neumann regular, R can be embedded into a direct product $S = \prod_{i \in I} K_i$ of a family of fields with S faithfully flat over R. Hence $S[X]$ is faithfully flat over $R[X]$. Replacing R by S if necessary we can therefore assume that R is a direct product of a family of fields, and in this case the lemma follows from the effective Nullstellensatz of Kollár [**26**].

Recall the familiar multinomial formula. For $e, M \in \mathbb{N}$, $M \geq 1$,

$$(Y_1 + \cdots + Y_M)^e = \sum_{e_1 + \cdots + e_M = e} \binom{e}{e_1, \dots, e_M} Y_1^{e_1} \cdots Y_M^{e_M}, \tag{4.1}$$

where $Y_1, \dots, Y_M$ are distinct indeterminates over $\mathbb{Z}$ and $\binom{e}{e_1, \dots, e_M} = \dfrac{e!}{e_1! \dots e_M!}$ for all $(e_1, \dots, e_M) \in \mathbb{N}^M$ with $e_1 + \cdots + e_M = e$. We record the following immediate consequence.

LEMMA 4.7 *Let R be a ring whose nilradical* Nil(R) *is nilpotent of index m. If $f \in \mathrm{Nil}(R[X])$ is of degree at most d, then $f^D = 0$ with $D := \binom{N+d}{N} \cdot m$.*

We can now prove Theorem 4.4. The 'only if' direction is implicit in the proof of [**3**, Proposition 5]. For the convenience of the reader we repeat the argument. Suppose that $\mathcal{C}$ is β-uniform, let $R \in \mathcal{C}$ and $r \in R$ be arbitrary, $n \in \mathbb{N}$, and consider the following elements of $R[X]$ (where X is a single indeterminate): $P(X) = rX + 1$, $P_n(X) = r^n$. Then obviously $P_n = r^n P - X P_{n+1}$, hence $1 \in (P, P_n)$. Put $m := \beta(1,1,2) + 1$, so there are polynomials $Q(X), Q_m(X) \in R[X]$ of degree less than m such that $1 = PQ + P_m Q_m$. A computation now shows that r^{m+1} divides r^m. Hence by Lemma 4.5 $r = r_1 + s$ with r_1 von Neumann regular and $s^m = 0$. Hence Nil(R) is nilpotent of index at most m, and R/Nil(R) is von Neumann regular.

Conversely, suppose that there exists some $m \geq 1$ such that for every $R \in \mathcal{C}$, Nil(R) is nilpotent of index at most m and R/Nil(R) is von Neumann regular. Let $R \in \mathcal{C}$, $N \geq 1$, and $f_1, \dots, f_n \in R[X_1, \dots, X_N] = R[X]$ of degree at most d with $1 \in (f_1, \dots, f_n)R[X]$. Hence $1 \in (\overline{f_1}, \dots, \overline{f_n})R/\mathrm{Nil}(R)[X]$, where $\overline{f}$ denotes the image of the polynomial $f \in R[X]$ under the canonical surjection $R[X] \to (R/\mathrm{Nil}(R))[X]$. By Lemma 4.6, there exist $g_1, \dots, g_n \in R[X]$ of degree at most d^{N+1} such that

$$h := 1 + f_1 g_1 + \cdots + f_n g_n \in \mathrm{Nil}(R)R[X].$$

The degree of h is at most d^{N+2}. By Lemma 4.7 it follows that $h^D = 0$, where $D = \binom{N + d^{N+2}}{N} \cdot m$. On the other hand we have, by letting $M = n + 1$ in (4.1) and specializing Y_1 to 1 and $Y_2, \dots, Y_M$ to $f_1 g_1, \dots, f_n g_n$, respectively,

$$h^D = 1 - (f_1 h_1 + \cdots + f_n h_n)$$

with $h_1, \dots, h_n \in R[X]$ of degree at most Dd^{N+2}. Hence R is β-uniform with

$$\beta(N,d) = \binom{N + d^{N+2}}{N} \cdot md^{N+2}.$$

This finishes the proof of Theorem 4.4. (Note that β does not depend on n and is even *linear* in the upper bound m on the nilpotency index.)

COROLLARY 4.8 *Let R be a ring, and put $R_{\mathrm{red}} := R/\mathrm{Nil}(R)$.*

(1) *Suppose that* $\mathrm{Nil}(R)$ *is finitely generated. Then R is super coherent if and only if* $\mathrm{Nil}(R)$ *is finitely presented and R_{red} is semihereditary, and R is uniform if and only if R_{red} is von Neumann regular. In particular, R is super coherent and uniform if and only if* $\mathrm{Nil}(R)$ *is finitely presented and R_{red} is von Neumann regular.*
(2) *Suppose that R is Noetherian. Then R is uniform if and only if R_{red} is semisimple (that is, isomorphic to a finite direct product of fields). In particular, a Noetherian uniform ring is super coherent.*

Proof. For the first part use Proposition 3.17 and Theorem 4.4, plus the fact that von Neumann regular $\Rightarrow$ semihereditary. For the second part note that the semisimple rings are exactly the Noetherian von Neumann regular rings.

Combining Theorem 4.4 with Corollary 3.18 yields the following result.

COROLLARY 4.9 *For each triple $(N,d,l) \in \mathbb{N}^3$ there exists $\beta = \beta(N,d,l) \in \mathbb{N}$ such that for every Artinian ring R of length at most l and polynomials $f_0, f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of degree at most d, if $f_0 \in (f_1, \dots, f_n)R[X]$, then*

$$f_0 = f_1 g_1 + \cdots + f_n g_n$$

for some $g_1, \dots, g_n \in R[X]$ of degree at most β.

Proof. Let R be an Artinian ring of length at most l, and $f_0, f_1, \dots, f_n \in R[X] = R[X_1, \dots, X_N]$ of degree at most d. Consider the homogeneous linear equation

$$f_0 y_0 + f_1 y_1 + \cdots + f_n y_n = 0. \tag{4.2}$$

By Corollary 3.18 we find generators $y^{(1)}, \dots, y^{(K)} \in R[X]^{n+1}$ for the module of solutions to (4.2) whose degrees are uniformly bounded in terms of N, d, l (independent of R and $f_0, \dots, f_n$). For $g_1, \dots, g_n \in R[X]$ we have $f_0 = f_1 g_1 + \cdots + f_n g_n$ if and only if $(1, -g_1, \dots, -g_n)^{\mathrm{tr}}$ is a solution to (4.2). Write $y^{(k)} = (y_0^{(k)}, \dots, y_n^{(k)})^{\mathrm{tr}}$. By Theorem 4.4, if $1 \in (y_0^{(1)}, \dots, y_0^{(K)})R[X]$, then there exist $h_1, \dots, h_K \in R[X]$ with $1 = y_0^{(1)} h_1 + \cdots + y_0^{(K)} h_K$ whose degrees are uniformly bounded in terms of N, d and l. The corollary follows.

REMARK Corollary 4.9 was first proved by Schoutens [32] (for local Artinian rings). For $l = 1$ and R local, we recover Hermann's theorem quoted after Theorem A.

We now turn to issues of definability.

Definability of membership in the radical. In the rest of this section we let $C = (C_1, \dots, C_M)$ be a tuple of parametric variables. Let $f_0(C,X), f_1(C,X), \dots, f_n(C,X) \in \mathbb{Z}[C,X]$.

For any field K and $c \in K^M$, we have

$$f_0(c,X) \in \sqrt{(f_1(c,X),\dots,f_n(c,X))K[X]} \quad \Leftrightarrow \text{for all}$$
$$a \in (K^{\text{alg}})^N : (f_1(c,a) = 0 \wedge \cdots \wedge f_n(c,a) = 0) \Rightarrow f_0(c,a) = 0, \tag{4.3}$$

by Hilbert's Nullstellensatz. (Here K^{alg} denotes an algebraic closure of K.) Hence, using primitive recursive quantifier elimination for the theory of algebraically closed fields, we may find, primitive recursively in $f_0,\dots,f_n$, a family (p_{ij},q_i) with $p_{ij}(C) \in \mathbb{Z}[C], q_i \in \mathbb{Z}[C]$, such that for all fields K and $c \in K^M$,

$$f_0(c,X) \in \sqrt{(f_1(c,X),\dots,f_n(c,X))K[X]} \Leftrightarrow$$
$$\bigwedge_{i=1}^{m} (p_{i1}(c) = 0 \wedge \cdots \wedge p_{ik}(c) = 0 \Rightarrow q_i(c) = 0). \tag{4.4}$$

In other words we have, for all fields K and $c \in K^M$,

$$f_0(c,X) \in \sqrt{(f_1(c,X),\dots,f_n(c,X))K[X]} \quad \Leftrightarrow$$
$$q_i(c) \in \sqrt{(p_{i1}(c),\dots,p_{ik}(c))K} \quad \text{for all } i = 1,\dots,m$$

(since in a field K, the nilradical of an ideal is either equal to K or to (0)). We now want to show that this equivalence in fact holds for *all* rings R in place of K and parameter tuples $c \in R^M$. (This was pointed out to us by van den Dries.)

In the following let R be an arbitrary ring. For $c \in R$ and $\mathfrak{p} \in \operatorname{Spec} R$ we write $c/\mathfrak{p} := c + \mathfrak{p} \in R/\mathfrak{p}$; more generally, if $c = (c_1,\dots,c_M) \in R^M$, then we write $c/\mathfrak{p}$ for $(c_1/\mathfrak{p},\dots,c_M/\mathfrak{p}) \in (R/\mathfrak{p})^M$. For a polynomial $f \in R[X] = R[X_1,\dots,X_N]$ and an ideal I of $R[X]$ we denote by $f_{(\mathfrak{p})}$ and $I_{(\mathfrak{p})}$ the image of f and I, respectively, under the canonical homomorphism

$$R[X] \to (R/\mathfrak{p})[X] \hookrightarrow k_{\mathfrak{p}}[X],$$

where $\mathfrak{p} \in \operatorname{Spec} R$, $k_{\mathfrak{p}} := \operatorname{Frac}(R/\mathfrak{p})$.

LEMMA 4.10 *For $f \in R[X]$ and an ideal I of $R[X]$, we have*

$$f \in \sqrt{I} \quad \Leftrightarrow \quad f_{(\mathfrak{p})} \in \sqrt{I_{(\mathfrak{p})}} \quad \text{for all } \mathfrak{p} \in \operatorname{Spec} R \text{ with } \mathfrak{p} \supseteq I \cap R.$$

Proof. The direction $\Rightarrow$ is trivial. Suppose $f \notin \sqrt{I}$. Then there exists a prime ideal $\mathfrak{P} \supseteq I$ such that $f \notin \mathfrak{P}$. Let $\mathfrak{p} = \mathfrak{P} \cap R$, and let $\overline{X}_1,\dots,\overline{X}_N$ be the images of $X_1,\dots,X_N$ under the canonical homomorphism $R[X] \to R[X]/\mathfrak{P} = S$. We may naturally identify $R/\mathfrak{p}$ with a subring of S and thus $k_{\mathfrak{p}}$ with a subfield of $\operatorname{Frac}(S)$. We define a $k_{\mathfrak{p}}$-homomorphism $k_{\mathfrak{p}}[X] \to \operatorname{Frac}(S)$ by $X_i \mapsto \overline{X}_i$ for $i = 1,\dots,N$. The image of $I_{(\mathfrak{p})}$ under this homomorphism is (0), so $(\overline{X}_1,\dots,\overline{X}_N) \in S^N$ is a zero of $I_{(\mathfrak{p})}$, whereas the image of $f_{(\mathfrak{p})}$ is $0 \neq f/\mathfrak{P} \in S$, so $(\overline{X}_1,\dots,\overline{X}_N)$ is not a zero of $f_{(\mathfrak{p})}$. Thus $f_{(\mathfrak{p})} \notin \sqrt{I_{(\mathfrak{p})}}$.

We now obtain the desired result.

PROPOSITION 4.11 *For all $c \in R^M$, we have*

$$f_0(c,X) \in \sqrt{(f_1(c,X),\dots,f_n(c,X))R[X]} \quad \Leftrightarrow \quad q_i(c) \in \sqrt{(p_{i1}(c),\dots,p_{ik}(c))R}$$

$$\text{for all } i = 1,\dots,m.$$

(*Here, the p_{ij} and q_i are as in* (4.4).)

Proof. Let $I := (f_1(c,X),\dots,f_n(c,X))R[X]$ and $f := f_0(c,X)$. Suppose $f \in \sqrt{I}$. Then, for every $i \in \{1,\dots,m\}$ and $\mathfrak{p} \in \operatorname{Spec} R$ with $\mathfrak{p} \supseteq (p_{i1}(c),\dots,p_{ik}(c))R$ we have

$$p_{i1}(c/\mathfrak{p}) = \cdots = p_{ik}(c/\mathfrak{p}) = 0$$

in $R/\mathfrak{p}$, hence $q_i(c/\mathfrak{p}) = 0$ by (4.4). Thus $q_i(c) \in \mathfrak{p}$. This shows that $q_i(c) \in \sqrt{(p_{i1}(c),\dots,p_{ik}(c))R}$ for all i. Suppose that $f \notin \sqrt{I}$. Then there exists $\mathfrak{p} \in \operatorname{Spec} R$ such that $f_{(\mathfrak{p})} \notin \sqrt{I_{(\mathfrak{p})}}$, by the lemma; thus for some $i \in \{1,\dots,m\}$, we have

$$p_{i1}(c/\mathfrak{p}) = \cdots = p_{ik}(c/\mathfrak{p}) = 0, \quad q_i(c/\mathfrak{p}) \neq 0,$$

by (4.4). Therefore $q_i(c) \notin \sqrt{(p_{i1}(c),\dots,p_{ik}(c))R}$.

REMARK The ideal $c(f)$ of R generated by the coefficients of a polynomial $f \in R[X]$ is called the *content* of f. Lemma 4.10 may also be used to obtain a quick proof of the following generalization of Gauss's lemma:

$$\sqrt{c(fg)} = \sqrt{c(f)} \cdot \sqrt{c(g)} \text{ for all } f,g \in R[X].$$

To see this, note first that it suffices to show the inclusion $\supseteq$. Moreover, it is enough treat the case where $R = \mathbb{Z}$ and the coefficients of f and g are pairwise distinct indeterminates over $\mathbb{Z}[X]$. Fixing an enumeration $X^{\mu_1},\dots,X^{\mu_M}$ of all monomials of degree at most d we may therefore write

$$f(C,X) = \sum_i C_i X^{\mu_i} \in \mathbb{Z}[C,X], \quad g(C',X) = \sum_i C_i X^{\mu_i} \in \mathbb{Z}[C',X]$$
$$\text{where} \quad C = (C_1,\dots,C_M), \quad C' = (C'_1,\dots,C'_M), \quad \text{and} \quad M = \binom{N+d}{N}.$$

By Lemma 4.10 (applied to $\mathbb{Z}[C,C']$ in place of $R[X]$) we may further reduce to the case where $R = K$ is a prime field (that is $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ for some prime p). Since for all $c = (c_1,\dots,c_M), c' = (c'_1,\dots,c'_M) \in (K^{\mathrm{alg}})^M$ we have

$$f(c,X) \cdot g(c',X) = 0 \quad \Leftrightarrow \quad f(c,X) = 0 \quad \text{or} \quad g(c',X) = 0,$$

the algebraic subset V of $(K^{\mathrm{alg}})^{2M}$ defined by the vanishing of the coefficients of $f(C,X) \cdot g(C',X)$ is the union

$$V = \{(c,c') : c_1 = \cdots = c_M = 0\} \cup \{(c,c') : c'_1 = \cdots = c_M = 0\}.$$

The Nullstellensatz now yields the claim. (See **[28]** for a different proof.)

Let $\mathcal{L}^*_{\mathrm{rad}}$ be the language of rings augmented by a $(k+1)$-ary predicate symbol rad_k, for each $k > 0$. We construe a ring R as an $\mathcal{L}^*_{\mathrm{rad}}$-structure by interpreting the ring symbols as usual

and the symbols rad_k, for $k > 0$, by

$$R \vDash \mathrm{rad}_k(r_0, r_1, \dots, r_k) \quad :\Leftrightarrow \quad r_0 \in \sqrt{(r_1, \dots, r_k)R},$$

for $r_0, \dots, r_k \in R$.

REMARK If R is a Bézout domain and $r_0, r_1, \dots, r_k \in R$, then

$$r_0 \in \sqrt{(r_1, \dots, r_k)R} \quad \Leftrightarrow \quad r_0 \in \sqrt{\gcd(r_1, \dots, r_k)R}.$$

In particular, if R is a DVR with associated valuation v, then

$$r_0 \in \sqrt{(r_1, \dots, r_k)R} \quad \Leftrightarrow \quad v(r_0) > 0 \vee \bigvee_{i=1}^{k} v(r_i) = 0,$$

so the relations rad_k are quantifier-free definable in the $\mathcal{L}_{\mathrm{div}}$-structure R.

By the discussion above, we obtain the following.

COROLLARY 4.12 *From the polynomials $f_0(C, X), \dots, f_n(C, X) \in \mathbb{Z}[C, X]$ one can primitive recursively construct a quantifier-free $\mathcal{L}^*_{\mathrm{rad}}$-formula $\varphi(C)$ such that for all rings R and all $c \in R^M$,*

$$R \vDash \varphi(c) \quad \Leftrightarrow \quad f_0(c, X) \in \sqrt{(f_1(c, X), \dots, f_n(c, X))R[X]}.$$

In particular, from the polynomials $f_1(C, X), \dots, f_n(C, X) \in \mathbb{Z}[C, X]$ one can primitive recursively construct a quantifier-free $\mathcal{L}^*_{\mathrm{rad}}$-formula $\varphi(C)$ such that for every ring R, the set

$$\{c \in R^M : 1 \in (f_1(c, X), \dots, f_n(c, X))R[X]\}$$

is defined by φ.

REMARK The relation rad_1 is indispensable for defining membership in the nilradical of an ideal in $R[X]$ in a quantifier-free way, as in the previous corollary. This can be shown by a modification of the example in [2, section 6]. Let a, b be elements of a ring R, and suppose that X is a single indeterminate. Then

$$1 \in (1 - aX, bX)R[X] \quad \Leftrightarrow \quad a \in \sqrt{bR}.$$

Proof. If $a^n = bc$ for some $n \in \mathbb{N}$, $n > 0$, and $c \in R$, then

$$1 = (1 + aX + \cdots + a^{n-1}X^{n-1}) \cdot (1 - aX) + cX^{n-1} \cdot bX,$$

exhibiting 1 as an element of $(1 - aX, bX)R[X]$. Conversely, suppose that we have $1 \in (1 - aX, bX)R[X]$. Then $1 - \bar{a}X$ is a unit in the ring $(R/bR)[X]$, where $\bar{a} = a + bR$. But in the formal power series ring $(R/bR)[[X]]$, the element $1 - \bar{a}X$ has multiplicative inverse

$$1 + \bar{a}X + \bar{a}^2X^2 + \bar{a}^3X^3 + \cdots.$$

By uniqueness of inverses in $(R/bR)[[X]]$ it follows that $a \in \sqrt{bR}$ as required.

Suppose R is a computable ring such that for given elements $r_0, \dots, r_k$ of R one can decide whether $r_0 \in \sqrt{(r_1, \dots, r_k)R}$. Then the computable ring $R[X]$ also has this property, that is, given $f_0, \dots, f_n \in R[X]$ one can effectively decide whether $f_0 \in \sqrt{(f_1, \dots, f_n)R[X]}$. For $R = \mathbb{Z}$, we have an even better result. Namely, given $r_0, r_1, \dots, r_k \in \mathbb{Z}$, we can check in polynomial time whether $r_0 \in \sqrt{(r_1, \dots, r_k)\mathbb{Z}}$: we first find $a \in \mathbb{Z}$ such that $(r_1, \dots, r_k)\mathbb{Z} = a\mathbb{Z}$, by the Euclidean algorithm, and then we check whether $a|(r_0)^e$, where e is the integral part $[\log_2|a|]$ if $a \neq 0$, $e = 1$ otherwise. Thus validity of quantifier-free $\mathcal{L}^*_{\mathrm{rad}}$-formulae in $\mathbb{Z}$ can be checked in polynomial time. This, together with Corollary 4.12, shows that for fixed $f_0(C,X), \dots, f_n(C,X) \in \mathbb{Z}[C,X]$, membership in the set

$$\left\{c \in \mathbb{Z}^M : f_0(c,X) \in \sqrt{(f_1(c,X), \dots, f_n(c,X))\mathbb{Z}[X]}\right\}$$

is decidable in polynomial time. Moreover, we have a primitive recursive algorithm which, upon input of $f_0, \dots, f_n \in \mathbb{Z}[X]$, decides whether $f_0 \in \sqrt{(f_1, \dots, f_n)\mathbb{Z}[X]}$.

Definability of ideal membership. We let

$$A(C,X) = (a_{ij}(C,X))$$

be an $m \times n$-matrix with entries $a_{ij}(C,X) \in \mathbb{Z}[C,X]$, and

$$b(C,X) = \begin{bmatrix} b_1(C,X) \\ \vdots \\ b_m(C,X) \end{bmatrix}$$

with $b_i(C,X) \in \mathbb{Z}[C,X]$. Given a ring R and an M-tuple $c \in R^M$ we ask when the set

$$\{c \in R^M : A(c,X)y = b(c,X) \text{ is solvable in } R[X]\} \tag{4.5}$$

can be defined by a quantifier-free formula $\varphi(C)$ in a (natural) expansion of $\mathcal{L}_{\mathrm{ring}}$. Similar to the proof of Corollary 4.9, using Corollary 3.9 and the remarks following Corollary 4.12, one easily shows the following.

THEOREM 4.13 *There exists a quantifier-free $\mathcal{L}_{\mathrm{rad}}$-formula $\varphi(C)$ which, for every Bézout domain R, defines the set* (4.5)*, that is, for every Bézout domain R and for every $c \in R^M$, the system $A(c,X)y = b(c,X)$ is solvable in $R[X]$ if and only if $R \models \varphi(c)$.*

REMARK The case $m = 1$, $R = \mathbb{Z}$ yields Theorem C of the Introduction. The remark about polynomial-time computability after Theorem C is a consequence of the discussion following Corollary 4.12.

From the pair (A,b) one can *construct* (primitive recursively) a quantifier-free $\mathcal{L}_{\mathrm{rad}}$-formula $\varphi(C)$ which defines the set (4.5) *in every PID R* (by the remark after Corollary 3.10). Specializing even further to DVRs (and using Corollary 3.10 instead of Corollary 3.9) we get the following result.

COROLLARY 4.14 *From (A,b) one can primitive recursively construct a quantifier-free $\mathcal{L}_{\mathrm{div}}$-formula which, for every DVR R, defines the set* (4.5).

If all polynomials $a_{ij}(C,X)$ and $b_i(C,X)$ are *homogeneous* in the indeterminates $X=(X_1,\dots,X_N)$, we can improve these results.

COROLLARY 4.15 *Suppose that all a_{ij} and b_i are homogeneous in X. Then one can primitive recursively construct a quantifier-free $\mathcal{L}_{\mathrm{gcd}}$-formula which defines* (4.5) *for every Bézout domain R, and one can primitive recursively construct a quantifier-free $\mathcal{L}_{\mathrm{div}}$-formula which defines* (4.5) *for every valuation ring R.*

Proof. If $N=0$, then this follows from [14] or more directly from a theorem of I. Heger, 1856 (see [29]): if R is a Prüfer domain, $B\in R^{m\times n}$ has rank m (considered as a matrix over the fraction field of R) and $d\in R^m$ is a column vector, then $By=d$ has a solution $y\in R^n$ if and only if the ideal of R generated by all $m\times m$-minors of B coincides with the ideal of R generated by all $m\times m$-minors of (B,d). For the general case note that for homogeneous $f_0,f_1,\dots,f_n\in R[X]$ with coefficients in R we have $f_0\in(f_1,\dots,f_n)R[X]$ if and only if $f_0=f_1g_1+\cdots+f_ng_n$ for homogeneous polynomials $g_1,\dots,g_n\in R[X]$, with $g_j=0$ if $\deg f_j>\deg f_0$ and $\deg g_j=\deg f_0-\deg f_j$ otherwise, for every j. This observation allows us to replace the system $A(c,X)y=b(c,X)$ over $R[X]$ by a certain system $A'(c)z=b'(c)$ over R without changing the set (4.5), uniformly in R and c. In this way we can reduce to the case $N=0$.

5. Prime ideals

Let $f_1(C,X),\dots,f_n(C,X)\in\mathbb{Z}[C,X]$, where again $C=(C_1,\dots,C_M)$. In this final section, we want to apply the results obtained so far to study instances of the following problem. Given a ring R, find a description by a first-order formula (in a natural language) of the set

$$\{c\in R^M:(f_1(c,X),\dots,f_n(c,X))R[X]\text{ is a prime ideal}\}. \tag{5.1}$$

We first consider this question in the case that $R=K$ is a field. By [15, (2.10) (ii), (iv)], there exist natural numbers $\alpha>1$ and β (only depending on the degrees of the f_j) such that for all fields K, $c\in K^M$, and the ideal $I=(f_1(c,X),\dots,f_n(c,X))$ of $K[X]$, we have

$$I\text{ is radical}\quad\Leftrightarrow\quad\text{for all }f\in K[X]\text{ of degree at most }\beta: f^\alpha\in I\Rightarrow f\in I$$

and

$$I\text{ is primary}\quad\Leftrightarrow$$

$$1\notin I,\ \text{and for all } f,g\in K[X]\text{ of degree at most }\beta: fg\in I\Rightarrow f\in I\text{ or }g^\alpha\in I.$$

In particular, there is a *universal* formula in the language $\mathcal{L}_{\mathrm{ring}}=\{0,1,+,-,\cdot\}$ of rings defining the set of coefficients $c\in K^M$ such that the ideal in $K[X]$ generated by $f_1(c,X),\dots,f_n(c,X)$ is radical, for every field K; similarly for 'primary' in place of 'radical'. (If we restrict ourselves to algebraically closed K, then these formulae may even be chosen quantifier-free, by quantifier-elimination for the theory of algebraically closed fields.) Since an ideal of a ring is

prime if and only if it is radical and primary, we also get

$$I \text{ is prime} \quad \Leftrightarrow$$

$$1 \notin I, \text{ and for all } f, g \in K[X] \text{ of degree at most } \beta : fg \in I \Rightarrow f \in I \text{ or } g \in I,$$

and there exists a universal $\mathcal{L}_{\text{ring}}$-formula defining the set (5.1) for all fields $R = K$. In [**13**, Chapter IV, §3], it was shown that (5.1) may even be defined quantifier-free in a certain natural extension of $\mathcal{L}_{\text{ring}}$, uniformly for all fields $R = K$. We give a brief account of this result, simplifying it in the process by replacing some of the Skolem functions used in the extension of the language $\mathcal{L}_{\text{ring}}$ by certain *predicate symbols* for zeros of separable polynomials, and extending it to define the properties *primary* and *radical*.

Prime ideals in polynomial rings over fields. Let K be a field and $p = \text{char } K$ if char $K > 0$, $p = 1$ if char $K = 0$. A field extension $L|K$ is called

(1) *separable* if L^p and K are linearly disjoint over K^p,
(2) *primary* if the separable algebraic closure of K in L equals K, and
(3) *regular* if it is both separable and primary.

The following lemma and its corollary below are well known.

LEMMA 5.1 *Let A be a K-algebra and $B = A \otimes_K L$, an L-algebra.*

(1) *If $L|K$ is separable and A is reduced, then B is reduced.*
(2) *If $L|K$ is primary and* Nil(A) *is a prime ideal of A, then* Nil(B) *is a prime ideal of B.*
(3) *If $L|K$ is regular and A is an integral domain, then B is an integral domain.*

Proof. Part (1) follows from [**6**, Proposition 5 of Chapter V, §15]. For (2), note that replacing A by $A/\text{Nil}(A)$ we may assume that A is an integral domain. Now it follows from [**6**, Chapter V, §17, Corollary to Proposition 1], that Nil(B) is prime in B. Since a ring is an integral domain if and only if it is reduced and the set of its nilpotent elements is a prime ideal, (3) follows from (1) and (2).

COROLLARY 5.2 *Let I be an ideal of $K[X]$.*

(1) *If $L|K$ is separable and I is a radical ideal, then $IL[X]$ is a radical ideal.*
(2) *If $L|K$ is primary and I is a primary ideal, then $IL[X]$ is a primary ideal.*
(3) *If $L|K$ is regular and I is a prime ideal, then $IL[X]$ is a prime ideal.*

REMARK From (1) of the Corollary 5.2 it follows that the condition that $f_1(c, X), \ldots, f_n(c, X)$ generate a radical ideal in $K[X]$ is definable by a quantifier-free $\mathcal{L}$-condition on $c \in K^M$, uniformly for all *perfect* fields K.

Let $\mathcal{L}_1$ be the language $\mathcal{L}_{\text{ring}}$ of rings augmented by a unary function symbol $^{-1}$ and, for every $m \geq 1$, an m-ary predicate symbol Z_m. We let T_1 be the extension of the theory of rings (formulated in the language $\mathcal{L}_{\text{ring}}$) by the defining axiom

$$\forall x((x = 0 \wedge x^{-1} = 0) \vee (x \neq 0 \wedge x \cdot x^{-1} = 1)) \tag{5.2}$$

and, for each $m \geq 1$, an axiom saying that for every model of T_1 with underlying field K

and $(a_1, \dots, a_m) \in K^m$,

$$K \vDash Z_m(a_1, \dots, a_m) \Leftrightarrow T^m + a_1 T^{m-1} + \cdots + a_m \in K[T] \text{ is separable and has a zero in } K.$$

Every field can be expanded uniquely to a model of T_1, and a substructure of a model of T_1 is a field (but not necessarily a model of T_1). Note that we include the symbol $^{-1}$ for convenience only: in T_1, every quantifier-free $\mathcal{L}_1$-formula is equivalent to a quantifier-free $\mathcal{L}_0$-formula, where $\mathcal{L}_0 = \mathcal{L}_1 \backslash \{^{-1}\}$. This can be seen using the following model-theoretic fact, which is proved by a standard application of the Compactness Theorem; we leave the proof to the reader.

LEMMA 5.3 *Let $\mathcal{L}$ and $\mathcal{L}^*$ be languages (in the sense of first-order logic) with $\mathcal{L} \subseteq \mathcal{L}^*$, and let T^* be an $\mathcal{L}^*$-theory. For an $\mathcal{L}^*$-formula $\varphi^*(x)$, $x = (x_1, \dots, x_n)$, the following are equivalent.*

(1) *There exists a quantifier-free $\mathcal{L}$-formula $\varphi(x)$ such that $T^* \vDash \forall x(\varphi^* \leftrightarrow \varphi)$.*
(2) *For all models $\mathbf{A}^*$ and $\mathbf{B}^*$ of T^* whose reducts to $\mathcal{L}$ have a common $\mathcal{L}$-substructure $\mathbf{C} = (C, \dots)$, and for all $c \in C^n$,*

$$\mathbf{A}^* \vDash \varphi^*(c) \quad \Leftrightarrow \quad \mathbf{B}^* \vDash \varphi^*(c).$$

REMARK Suppose that one of the equivalent conditions in the lemma holds for an $\mathcal{L}^*$-formula $\varphi^*(x)$. If $\mathcal{L}^*$ and T^* are recursively enumerable, then a quantifier-free $\mathcal{L}$-formula φ as in (1) can be found effectively, by Gödel's Completeness Theorem.

For a field K, we denote the separable algebraic closure of K (in a fixed algebraic closure of K) by K_{sep}.

LEMMA 5.4 *Suppose E and F are the underlying fields of models of T_1 having a common $\mathcal{L}_1$-substructure with underlying field K. There exists an isomorphism $E \cap K_{\text{sep}} \to F \cap K_{\text{sep}}$ which is the identity on K.*

This lemma is due to Ax ([**3**, §3, Lemma 5]). We use it to show the following.

COROLLARY 5.5 *There exists a quantifier-free $\mathcal{L}_0$-formula $\varphi_{\text{primary}}(C)$ such that for every field K and all $c \in K^M$,*

$$K \vDash \varphi_{\text{primary}}(c) \quad \Leftrightarrow \quad (f_1(c, X), \dots, f_n(c, X))K[X] \text{ is primary.}$$

Proof. By the above discussion, there exists an $\mathcal{L}_{\text{ring}}$-formula $\varphi(C)$ (possibly involving quantifiers) such that for all fields K and $c \in K^M$,

$$K \vDash \varphi(c) \quad \Leftrightarrow \quad (f_1(c, X), \dots, f_n(c, X))K[X] \text{ is primary.}$$

Suppose now that E and F are the underlying fields of models of T_1 having a common substructure with underlying field K, and suppose $c \in K^M$ is such that $E \vDash \varphi(c)$, that is, the ideal $IE[X]$ is primary, where

$$I := (f_1(c, X), \dots, f_n(c, X))K[X].$$

Then, by faithful flatness of $E[X]$ as module over $(E \cap K_{\text{sep}})[X]$,

$$IE[X] \cap (E \cap K_{\text{sep}})[X] = I(E \cap K_{\text{sep}})[X]$$

is primary, and hence so is $I(F \cap K_{\mathrm{sep}})[X]$, by Lemma 5.4. Since the field extension $F \supseteq F \cap K_{\mathrm{sep}}$ is primary, we get $F \models \varphi(c)$, by Corollary 5.2 (2). Using Lemma 5.3 it follows that φ is equivalent to a quantifier-free $\mathcal{L}_0$-formula in T_1.

Using Corollary 5.5 and the remark following Corollary 5.2 we get the following.

COROLLARY 5.6 *There exists a quantifier-free $\mathcal{L}_0$-formula $\psi_{\mathrm{prime}}(C)$ such that for all perfect fields K and $c \in K^M$,*

$$K \models \psi_{\mathrm{prime}}(c) \;\Leftrightarrow\; (f_1(c,X), \dots, f_n(c,X))K[X] \text{ is prime.}$$

Let now $\mathcal{L}_2$ be the language $\mathcal{L}_{\mathrm{ring}}$ augmented by function symbols $^{-1}$ (unary) and λ_{mi} (m-ary), for all $1 \le i \le m$. We extend the theory of rings to an $\mathcal{L}_2$-theory T_2 by adding the defining axiom (5.2) and for each $m \ge 1$ an axiom saying that for any model of T_2 with underlying field K and $a = (a_1, \dots, a_m) \in K^m$, the vector $\lambda_m(a) = (\lambda_{m1}(a), \dots, \lambda_{mm}(a)) \in K^m$ is a non-trivial solution of the equation

$$a_1 Y_1^p + \cdots + a_m Y_m^p = 0$$

if there is such a solution and $\mathrm{char}\, K = p > 0$. Every field may be expanded to a model of T_2. Note that T_2 is a *universal* theory, and if $K \subseteq L$ are the underlying fields of an extension of models of T_2, then $L|K$ is a separable field extension. Along the lines of the proof of Corollary 5.5, using part (1) of Corollary 5.2 instead of (2), one shows the following.

COROLLARY 5.7 *There exists a quantifier-free $\mathcal{L}_2$-formula $\varphi_{\mathrm{radical}}(C)$ such that for every field K and all $c \in K^M$,*

$$K \models \varphi_{\mathrm{radical}}(c) \;\Leftrightarrow\; (f_1(c,X), \dots, f_n(c,X))K[X] \text{ is radical.}$$

Hence in particular, the quantifier-free formula $\varphi_{\mathrm{prime}} = \varphi_{\mathrm{primary}} \wedge \varphi_{\mathrm{radical}}$ in the language $\mathcal{L}_1 \cup \mathcal{L}_2$ defines the set (5.1) for all fields $R = K$.

Prime ideals in polynomial rings over some arithmetical rings. Based on the previous results, it is now more or less straightforward to produce numerous corollaries about the definability of primality for ideals in polynomial rings $R[X]$, where R is a DVR, a PID, etc. In order to keep the notational effort minimal, we restrict ourselves to treating the following two situations:

(1) R is a DVR with perfect residue and fraction fields;
(2) $R = \mathbb{Z}$.

Given any integral domain R with fraction field F and a finitely generated ideal I of $R[X]$, there exists a non-zero $\delta \in R$ such that $IF[X] \cap R[X] = I : \delta R[X]$. (In particular, $I \cap R \neq (0) \Leftrightarrow \delta \in I$.) This is trivial if R is Noetherian. The general case is a consequence of Hermann's method as described in [**2**, section 3, in particular Corollary 3.5]. In fact, analysing the proof of that corollary shows that δ can be chosen in a uniform way.

LEMMA 5.8 *There exists a finite family $\{\gamma^{(\lambda)}(C)\}_{\lambda \in \Lambda}$ of quantifier-free $\mathcal{L}_{\mathrm{ring}}$-formulae $\gamma^{(\lambda)}(C)$ and a finite family $\{\delta^{(\lambda)}(C)\}_{\lambda \in \Lambda}$ of polynomials $\delta^{(\lambda)}(C) \in \mathbb{Z}[C]$, such that for every integral domain R with fraction field F and $c \in R^M$ we have $R \models \bigvee_{\lambda \in \Lambda} \gamma^{(\lambda)}(c)$, and if $\lambda \in \Lambda$ is such that*

$R \models \gamma^{(\lambda)}(c)$, *then* $\delta^{(\lambda)}(c) \neq 0$ *and*

$$I(c)F[X] \cap R[X] = I(c) : \delta^{(\lambda)}(c)R[X],$$

where $I(c) := (f_1(c, X), \ldots, f_n(c, X))R[X]$.

This yields the following.

COROLLARY 5.9 *There exists a quantifier-free* $\mathcal{L}_{\mathrm{div}}$*-formula* $\varrho_{\mathrm{div}}(C)$ *such that for every DVR* R *with fraction field* F *and every* $c \in R^M$, *we have*

$$R \models \varrho_{\mathrm{div}}(c) \quad \Leftrightarrow \quad I(c)F[X] \cap R[X] = I(c). \tag{5.3}$$

Also, there exists a quantifier-free $\mathcal{L}_{\mathrm{rad}}$*-formula* $\varrho_{\mathrm{rad}}(C)$ *such that for every Bézout domain* R *with fraction field* F *and every* $c \in R^M$, *we have*

$$R \models \varrho_{\mathrm{rad}}(c) \quad \Leftrightarrow \quad I(c)F[X] \cap R[X] = I(c).$$

Proof. By Lemma 5.8 and Corollaries 3.11, 4.14 we initially obtain a quantifier-free $\mathcal{L}_{\mathrm{div},D}$-formula $\varrho_{\mathrm{div},D}(C)$ satisfying (5.3) for every DVR R and $c \in R^M$, with $\varrho_{\mathrm{div},D}$ in place of ϱ_{div}. However, every quantifier-free $\mathcal{L}_{\mathrm{div},D}$-formula is equivalent to a quantifier-free $\mathcal{L}_{\mathrm{div}}$-formula, in the $\mathcal{L}_{\mathrm{div},D}$-theory of valuation rings. (Use Lemma 5.3.) The first statement now follows. The second statement is obtained from Lemma 5.8, the remark following Corollary 3.11, and Theorem 4.13.

The next lemma is fundamental for what follows; we leave its proof to the reader.

LEMMA 5.10 *Let* R *be an integral domain with fraction field* F, *and let* I *be an ideal of* $R[X]$. *Then* I *is a prime ideal if and only if one of the following holds:*

(1) $IF[X]$ *is a prime ideal of* $F[X]$ *and* $IF[X] \cap R[X] = I$;
(2) *the ideal* $I \cap R$ *is a non-zero prime ideal of* R, *and the image of* I *under the canonical homomorphism* $R[X] \to (R/I \cap R)[X]$ *is a prime ideal.*

REMARK If R is a unique factorization domain and δ is as above, then we may replace (2) in Lemma 5.10 by

(2′) there exists a prime factor π of δ with $\pi \in I$, and the image of I under the canonical homomorphism $R[X] \to (R/\pi R)[X]$ is a prime ideal.

Prime ideals in polynomial rings over valuation rings. Let now $\mathcal{L}^*_{\mathrm{div}}$ be the language

$$\mathcal{L}^*_{\mathrm{div}} = \mathcal{L}_{\mathrm{div}} \cup \{Z_m : m \geq 1\} \cup \{\overline{Z}_m : m \geq 1\},$$

where Z_m and $\overline{Z}_m$ are m-ary predicate symbols, for $m \geq 1$. We construe a valuation ring R (with fraction field F and residue field $\overline{R}$) as an $\mathcal{L}^*_{\mathrm{div}}$-structure as follows: we interpret the symbols of $\mathcal{L}_{\mathrm{div}}$ as usual, and for $a_1, \ldots, a_m \in R$, $m \geq 1$, we put

$$R \models Z_m(a_1, \ldots, a_m) :\Leftrightarrow T^m + a_1 T^{m-1} + \cdots + a_m \in R[T] \text{ has a zero in } F$$

and

$$R \vDash \overline{Z}_m(a_1, \dots, a_m) :\Leftrightarrow T^m + \overline{a}_1 T^{m-1} + \cdots + \overline{a}_m \in \overline{R}[T] \text{ has a zero in } \overline{R}.$$

From Corollaries 5.6, 5.9 and the remark following Lemma 5.10, we obtain the following.

COROLLARY 5.11 *There exists a quantifier-free $\mathcal{L}^*_{\mathrm{div}}$-formula $\varphi_{\mathrm{prime,DVR}}(C, T)$ such that for all DVRs R with maximal ideal $\mathfrak{m}$, perfect residue field $\overline{R} = R/\mathfrak{m}$ and perfect fraction field F, all generators π of $\mathfrak{m}$ and all $c \in R^M$,*

$$R \vDash \varphi_{\mathrm{prime,DVR}}(c, \pi) \;\Leftrightarrow\; (f_1(c, X), \dots, f_n(c, X))R[X] \text{ is a prime ideal.}$$

Corollary 5.11 applies in particular to the ring $R = \mathbb{Z}_p$ of p-adic integers (with finite residue field $\mathbb{F}_p$ and fraction field $\mathbb{Q}_p$ of characteristic zero). Let $\mathcal{L}_{\mathrm{pow}}$ be the language obtained by augmenting the language $\mathcal{L}_{\mathrm{ring}}$ by a unary predicate symbols P_n, for each $n > 0$. We construe $\mathbb{Z}_p$ as an $\mathcal{L}_{\mathrm{pow}}$-structure by interpreting the ring symbols as usual and P_n by the set of all nth powers of elements of $\mathbb{Z}_p$. By Macintyre's theorem [27], the complete $\mathcal{L}_{\mathrm{pow}}$-theory of $\mathbb{Z}_p$ admits quantifier-elimination. The relations on $\mathbb{Z}_p^m$ given by Z_m and $\overline{Z}_m$ are definable in the $\mathcal{L}_{\mathrm{pow}}$-structure $\mathbb{Z}_p$. Hence we have the following.

COROLLARY 5.12 *For each prime p, there exists a quantifier-free $\mathcal{L}_{\mathrm{pow}}$-formula $\varphi_{\mathrm{prime,p}}(C)$ such that for all $c \in \mathbb{Z}_p^M$*

$$\mathbb{Z}_p \vDash \varphi_{\mathrm{prime},p}(c) \;\Leftrightarrow\; (f_1(c, X), \dots, f_n(c, X))\mathbb{Z}_p[X] \text{ is a prime ideal.}$$

EXAMPLE Let R be a valuation ring whose value group is a $\mathbb{Z}$-group (that is, elementarily equivalent to $\mathbb{Z}$, as an ordered abelian group), and let π be an element of R with smallest positive valuation. Put $R_\pi := \{a\pi^{-n} : a \in R, n \in \mathbb{N}\}$, a valuation ring of $\mathrm{Frac}(R)$ containing R as a subring. Then R_π has no prime ideal of the form cR_π with $c \in R$ $c \neq 0$. For $c \in R$ consider the ideal $I_c = (\pi(1 - \pi X), \pi c X)$ of $R[X]$, where X is a single indeterminate. We claim that I_c is prime if and only if $c = 0$ or $\pi \in \sqrt{cR}$. To see this, note first that by the remark following Corollary 4.12 we have $\pi \in I_c$, if and only if $\pi \in \sqrt{cR}$. If $\pi \in I_c$, then $I_c = (\pi)$, and if $c = 0$, then $I_c = (1 - \pi X)$; in both cases I_c clearly is prime. Conversely, suppose that I_c is prime, and assume for a contradiction that $\pi \notin I_c$, hence $I_c = (1 - \pi X, cX)$, and $c \neq 0$. The R-homomorphism $\mathrm{R}[X] \to R_\pi$ given by $X \mapsto \pi^{-1}$ has kernel $(1 - \pi X)$, and the image cR_π of I_c under this homomorphism is a non-zero prime ideal of R_π, a contradiction.

Letting R range over all p-adically closed valuation rings (= models of the complete $\mathcal{L}_{\mathrm{pow}}$-theory of $\mathbb{Z}_p$) and taking $\pi = p$, this claim implies that there does not exist an $\mathcal{L}_{\mathrm{pow}}$-formula $\varphi(C)$ with the property that for all p-adically closed valuation rings and all $c \in R$, we have $R \vDash \varphi(c)$ if and only if I_c is a prime ideal of $R[X]$.

For homogeneous ideals, however, we do have a more uniform version of Corollary 5.12.

PROPOSITION 5.13 *Suppose that $f_1(C, X), \dots, f_n(C, X) \in \mathbb{Z}[C, X]$ are homogeneous in $X = (X_1, \dots, X_N)$. Then there exists a quantifier-free $\mathcal{L}_{\mathrm{pow}}$-formula $\varphi^{\mathrm{hom}}_{\mathrm{prime},p}(C)$ such that for all p-adically closed valuation rings R and all $c \in R^M$,*

$$R \vDash \varphi^{\mathrm{hom}}_{\mathrm{prime},\,p}(c) \Leftrightarrow (f_1(c, X), \dots, f_n(c, X))R[X] \text{ is a prime ideal.}$$

Proof. Let R be a p-adically closed valuation ring, and let π be a generator for the maximal ideal $\mathfrak{m}$ of R. Then the only principal prime ideals of R are (0) and $\mathfrak{m} = \pi R$. If moreover I is a homogeneous ideal of $R[X]$, then $I \cap R$ is principal. Hence in this case, we may replace (2) in Lemma 5.10 by

(2″) we have $p \in I$, and the image of I under the canonical homomorphism $R[X] \to (R/\pi R)[X]$ is a prime ideal.

The proposition now follows from Lemma 5.8 and Corollaries 3.11, 4.15 and 5.6.

Prime ideals in polynomial rings over $\mathbb{Z}$. We extend $\mathcal{L}_{\mathrm{rad}}$ to a language $\mathcal{L}^*_{\mathrm{rad}}$ by adjoining, for each $m \geq 1$, an $(m+1)$-ary predicate symbol Z_m. We expand the $\mathcal{L}_{\mathrm{rad}}$-structure $\mathbb{Z}$ to an $\mathcal{L}^*_{\mathrm{rad}}$-structure by interpreting the Z_m as follows: for $p, a_1, \ldots, a_m \in \mathbb{Z}$,

$$\mathbb{Z} \models Z_m(p, a_1, \ldots, a_m) \;\Leftrightarrow\; p \text{ is a prime and } T^m + \overline{a}_1 T^{m-1} + \cdots + \overline{a}_m \in \mathbb{F}_p[T]$$

$$\text{has a zero in } \mathbb{F}_p, \text{ or } p = 0 \text{ and } T^m + a_1 T^{m-1} + \cdots + a_m \in \mathbb{Z}[T]$$

$$\text{has a zero in } \mathbb{Q}.$$

Let us call an $\mathcal{L}^*_{\mathrm{rad}}$-formula $\varphi(C)$ *special* if it is of the form

$$\varphi(C) = \exists U(\text{`}U \text{ is a prime dividing } \delta(C)\text{'} \wedge \psi(C, U)),$$

where U is a single new variable, $\delta(C) \in \mathbb{Z}[C]$, and $\psi(C, U)$ a quantifier-free $\mathcal{L}^*_{\mathrm{rad}}$-formula. Using the remark after Lemma 5.10 and Corollaries 5.6, 5.9, we get the following.

COROLLARY 5.14 *There exists a finite disjunction* $\varphi_{\mathrm{prime},\mathbb{Z}}(C)$ *of special* $\mathcal{L}^*_{\mathrm{rad}}$*-formulae such that for all* $c \in \mathbb{Z}^M$

$$Z \models \varphi_{\mathrm{prime},\mathbb{Z}}(c) \;\Leftrightarrow\; (f_1(c, X), \ldots, f_n(c, X))\mathbb{Z}[X] \text{ is a prime ideal.}$$

Acknowledgements

Parts of this paper derive from my Ph. D. Thesis [1]. I would like to thank Lou van den Dries for his guidance during the writing of that thesis, in particular for pointing out Proposition 4.11. I am also grateful to the University of California at Berkeley and the Mathematical Sciences Research Institute for their support, and to the referee for corrections and helpful remarks.

References

1. M. Aschenbrenner, *Ideal membership in polynomial rings over the integers*, Ph. D. Thesis, University of Illinois at Urbana-Champaign, 2001.
2. M. Aschenbrenner, Ideal membership in polynomial rings over the integers, *J. Amer. Math. Soc.* **17** (2004), 407–441 (electronic).
3. J. Ax, Solving diophantine problems modulo every prime, *Ann. of Math.* **85** (1967), 161–183.
4. H. Bass, Torsion free and projective modules, *Trans. Amer. Math. Soc.* **102** (1962), 319–327.
5. N. Bourbaki, *Éléments de Mathématique. Algèbre Commutative*, Hermann, Paris, 1964.

6. N. Bourbaki, *Éléments de Mathématique. Algèbre*, Lecture Notes in Mathematic 864, Masson, Paris, 1981, Chapters 4–7.
7. D. Brizolis, A theorem on ideals in Prüfer rings of integral-valued polynomials, *Comm. Algebra* **7** (1979), 1065–1077.
8. P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Mathematical Surveys and Monographs **48**, American Mathematical Society, Providence, 1997.
9. C. C. Chang and H. J. Keisler, *Model Theory*, Studies in Logic and the Foundations of Mathematics **73**, North–Holland, Amsterdam, 1973.
10. S. U. Chase, Direct products of modules, *Trans. Amer. Math. Soc.* **97** (1960), 457–473.
11. G. Cherlin, Algebraically closed commutative rings, *J. Symbolic Logic* **38** (1973), 493–499.
12. I. S. Cohen, Commutative rings with restricted minimum condition, *Duke Math J.* **17** (1950), 27–42.
13. L. van den Dries, *Model theory of fields*, Ph. D. Thesis, R.U. Utrecht, 1978.
14. L. van den Dries and J. Holly, Quantifier elimination for modules with scalar variables, *Ann. Pure Appl. Logic* **57** (1992), 161–179.
15. L. van den Dries and K. Schmidt, Bounds in the theory of polynomial rings over fields. A nonstandard approach, *Invent. Math.* **76** (1984), 77–91.
16. D. Eisenbud and E. G. Evans, Generating modules efficiently: theorems from algebraic K-theory, *J. Algebra* **27** (1973), 278–305.
17. O. Forster, Über die Anzahl der Erzeugenden eines Ideals in einem noetherschen Ring, *Math. Z.* **84** (1964), 80–87.
18. S. Frisch, Nullstellensatz and Skolem properties for integer-valued polynomials, *J. Reine Angew. Math.* **536** (2001), 31–42.
19. S. Glaz, *Commutative Coherent Rings*, Lecture Notes in Mathematics **1371**, Springer, Berlin, 1989.
20. S. Glaz, Commutative coherent rings: historical perspective and current developments, *Nieuw Arch. Wisk.* **10**, 4 (1992), 37–56.
21. B. Greenberg and W. Vasconcelos, Coherence of polynomial rings, *Proc. Amer. Math. Soc.* **54** (1976), 59–64.
22. R. Heitmann, Generating ideals in Prüfer domains, *Pacific J. Math.* **62** (1976), 117–126.
23. R. Heitmann, Generating non-noetherian modules efficiently, *Michigan Math. J.* **31** (1984), 167–180.
24. G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.* **95** (1926), 736–788.
25. W. Hodges, *Model Theory*, Encyclopedia of Mathematics and its Applications 42, Cambridge University Press, Cambridge, 1993.
26. J. Kollár, Sharp effective Nullstellensatz, *J. Amer. Math. Soc.* **1** (1988), 963–975.
27. A. Macintyre, On definable subsets of p-adic fields, *J. Symbolic Logic* **41** (1976), 605–610.
28. D. G. Northcott, A generalization of a theorem on the content of polynomials, *Proc. Cambridge Philos. Soc.* **55** (1959), 282–288.
29. R. O'Leary and J. Vaaler, Small solutions to inhomogeneous linear equations over number fields, *Trans. Amer. Math. Soc.* **336** (1993), 915–931.
30. A. Prestel and J. Schmid, Existentially closed domains with radical relations, *J. Reine Angew. Math.* **407** (1990), 178–201.
31. G. Sabbagh, Coherence of polynomial rings and bounds in polynomial ideals, *J. Algebra* **31** (1974), 499–507.

32. H. Schoutens, *Bounds in polynomial rings over Artinian local rings*, manuscript, 2002.
33. H. Schoutens, *Asymptotic homological conjectures in mixed characteristic,* preprint, 2003.
34. H. Schoutens, Mixed characteristic homological theorems in low degrees, *C.R. Math. Acad. Sci. Paris* **336** (2003), 463–466.
35. H. W. Schülting, Über die Erzeugendenanzahl invertierbarer Ideale in Prüferringen, *Comm. Algebra* **7** (1979), 1331–1349.
36. A. Seidenberg, Constructions in algebra, *Trans. Amer. Math. Soc.* **197** (1974), 273–313.
37. T. Skolem, Ein Satz über ganzwertige Polynome, *Norske Vid. Selsk. Forh.* **9** (1936), 111–113.
38. J.-P. Soublin, Un anneau cohérent dont l'anneau des polynomes n'est pas cohérent, *C.R. Acad. Sci. Paris Sér. A* **267** (1968), 241–243.
39. J.-P. Soublin, Anneaux et modules cohérents, *J. Algebra* **15** (1970), 455–472.
40. R. Swan, The number of generators of a module, *Math. Z.* **102** (1967), 318–322.
41. R. Swan, *n*-generator ideals in Prüfer domains, *Pacific J. Math.* **111** (1984), 433–446.

A. APPENDIX

We would like to point out another application of the useful Proposition 4.11, to a characterization of Jacobson domains among Noetherian domains. A *Jacobson ring* is a ring each of whose prime ideals is an intersection of maximal ideals. A Jacobson domain is a Jacobson ring which happens to be a domain. Examples for Jacobson domains include $\mathbb{Z}$ (or more generally: any PID with infinitely many pairwise non-associated primes), and every polynomial ring $R[X]$ over a Jacobson domain R; see [**5**, IV.3.4]. For a domain R, we denote the integral closure of R in an algebraic closure of its fraction field by R^+.

PROPOSITION A.1 *Let R be a Jacobson domain and $f_0, \dots, f_n \in R[X]$. Then*

$$f_0 \in \sqrt{(f_1, \dots, f_n)R[X]} \Leftrightarrow f_0(a) \in \sqrt{(f_1(a), \dots, f_n(a))R^+} \text{ for all } a \in (R^+)^N.$$

Proof. The implication $\Rightarrow$ is clear. To prove $\Leftarrow$, assume $f_0 \notin \sqrt{I}$, where $I = (f_1, \dots, f_n)R[X]$. We have to find $a \in (R^+)^N$ such that $f_0(a) \notin \sqrt{(f_1(a), \dots, f_n(a))R^+}$.
We write $f_i(X)$ as $f_i(c, X)$, with $f_i(C, X) \in \mathbb{Z}[C, X]$, $c \in R^M$, for $i = 0, \dots, n$. By Proposition 4.11, there exists $i \in \{1, \dots, m\}$ with $q_i(c) \notin \sqrt{(p_{i1}(c), \dots, p_{ik}(c))R}$.
Take a maximal ideal $\mathfrak{m}$ of R that contains $\sqrt{(p_{i1}(c), \dots, p_{ik}(c))R}$ but not $q_i(c)$, and a maximal ideal $\mathfrak{m}^+$ of R^+ lying above $\mathfrak{m}$. Then by (4.3) and (4.4) for the algebraically closed field $K = R^+/\mathfrak{m}^+$, there exists $a \in (R^+)^N$ with

$$f_0(c, a) \notin \mathfrak{m}^+, f_1(c, a), \dots, f_n(c, a) \in \mathfrak{m}^+.$$

Hence $f_0(c, a) \notin \sqrt{(f_1(c, a), \dots, f_n(c, a))R^+}$.

REMARK The case $R = \mathbb{Z}$ of Proposition A.1 is [**30**, Theorem 5.3.] (The proof in [**30**] is much longer.)

COROLLARY A.2 *Let R be a Noetherian domain. The following are equivalent:*

(1) *R is a Jacobson domain;*
(2) *for all $N \in \mathbb{N}$ and $f_0, f_1, \dots, f_n \in R[X_1, \dots, X_N]$, if*

$$f_0(a) \in \sqrt{(f_1(a), \dots, f_n(a))R^+} \text{ for all } a \in (R^+)^N,$$

then $f_0 \in \sqrt{(f_1, \dots, f_n)R[X]}$;

(3) *for polynomials* $f_1, \dots, f_n \in R[X]$ *in the single indeterminate* X*, if*

$$1 \in (f_1(a), \dots, f_n(a))R^+ \text{ for all } a \in R^+$$

then $1 \in (f_1, \dots, f_n)R[X]$.

Proof. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) do not need the assumption that R be Noetherian: (1) $\Rightarrow$ (2) follows from the proposition, and (2) $\Rightarrow$ (3) is trivial. Assume now that R is a Noetherian domain, and (3) holds. In order to show that R is Jacobson it then suffices to show the following: if $r_1, \dots, r_n, r \in R$, have the property that $r \in \mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of R which contains $r_1, \dots, r_n$, then $r \in \sqrt{(r_1, \dots, r_n)R}$. For this we may assume $r \neq 0$, and we consider the polynomials $r_1, \dots, r_n, 1 - rX$ in the single indeterminate X. We claim that for every $a \in R^+$, we have $1 \in (r_1, \dots, r_n, 1 - ra)R^+$. Suppose otherwise, and let $a \in R^+$ with $1 \notin (r_1, \dots, r_n, 1 - ra)R^+$. Let n be a maximal ideal of R^+ containing $r_1, \dots, r_n, 1 - ra$. Then $\mathfrak{m} := \mathfrak{n} \cap R$ is a maximal ideal of R (by the going-up property for integral ring extensions). Since $r_1, \dots, r_n \in \mathfrak{m}$ we get $r \in \mathfrak{m}$ and hence $1 \in \mathfrak{n}$, a contradiction. By (3), this implies that there exists a relation

$$1 = r_1 g_1 + \cdots + r_n g_n + (1 - rX)g,$$

where $g_1, \dots, g_n, g \in R[X]$. Substituting $1/r$ for X and multiplying both sides by r^d, where d is the maximum of the degrees of the g_i, we get $r^d \in (r_1, \dots, r_n)R$ (Rabinowitsch's trick). Hence $r \in \sqrt{(r_1, \dots, r_n)R}$ as desired.

The following easily proved lemma (applied to $R = S = \mathbb{Z}^+$) gives an example which shows that Proposition A.1 is false without the radicals $\sqrt{\cdots}$.

LEMMA A.3 *Let* R *be a Prüfer domain and*

$$f_0(X, Y) = X^2, f_1(X, Y) = X^2 + Y^2, f_2(X, Y) = XY,$$

where X *and* Y *are single indeterminates. Then* $f_0(x, y) \in (f_1(x, y), f_2(x, y))R$ *for all* $(x, y) \in R^2$*, but* $f_0 \notin (f_1, f_2)S[X, Y]$ *for every domain* S *extending* R*.*

For the polynomials $f_1 = -2, f_2 = X^2 + X + 1 \in \mathbb{Z}[X]$ (where X is a single indeterminate) we have $1 \in (f_1(a), f_2(a))\mathbb{Z}$ for every $a \in \mathbb{Z}$, but $1 \notin (f_1, f_2)\mathbb{Z}[X]$. This (well-known) example shows that in Proposition A.1 we cannot replace R^+ by R. On the other hand, we do have $1 = gf_1 + f_2$ where $g = \frac{1}{2}(X + 1)$ is integer-valued, that is, $g(\mathbb{Z}) \subseteq \mathbb{Z}$. Indeed, Skolem [37] showed in general this result (see also [8]).

PROPOSITION A.4 *If* $f_0, f_1, \dots, f_n \in \mathbb{Z}[X] = \mathbb{Z}[X_1, \dots, X_N]$ *satisfy*

$$f_0(a) \in \sqrt{(f_1(a), \dots, f_n(a))\mathbb{Z}} \text{ for all } a \in \mathbb{Z}^N,$$

then $f_0 \in \sqrt{(f_1, \dots, f_n)\mathrm{Int}(\mathbb{Z}^N)}$*, where*

$$\mathrm{Int}(\mathbb{Z}^N) = \{f(X) \in \mathbb{Q}[X] : f(a) \in \mathbb{Z} \text{ for all } a \in \mathbb{Z}^N\}$$

denotes the subring of $\mathbb{Q}[X]$ *of integer-valued polynomials.*

One says that the integral domain $\mathbb{Z}$ has the *Skolem property*. See [18] for a characterization of the Noetherian domains with the Skolem property similar in spirit to Corollary A.2. In [7] it is shown that for $N = 1$, the radicals $\sqrt{\cdots}$ in Skolem's theorem may be omitted. Lemma A.3 (for $R = \mathbb{Z}$, $S = \mathbb{Q}$) shows that for $N = 2$ we cannot omit the $\sqrt{\cdots}$. This gives a negative answer to a question posed in [7].