Michigan Math. J. (Advance Publication)

Big Polynomial Rings with Imperfect Coefficient Fields

DANIEL ERMAN, STEVEN V SAM, & ANDREW SNOWDEN

ABSTRACT. We previously showed that the inverse limit of standard-graded polynomial rings with perfect (or semiperfect) coefficient field is a polynomial ring in an uncountable number of variables. In this paper, we show that the result holds with no hypothesis on the coefficient field. We also prove an analogous result for ultraproducts of polynomial rings.

1. Introduction

1.1. Statement of Results

Let $\mathbf{k}$ be a field, and let $\mathbf{R}$ be the inverse limit of the standard-graded polynomial rings $\mathbf{k}[x_1, \dots, x_n]$ in the category of graded rings; thus $\mathbf{R}$ is a graded ring, and a degree d element of $\mathbf{R}$ is a formal, perhaps infinite, $\mathbf{k}$-linear combination of degree d monomials in the variables $\{x_i\}_{i\geq 1}$. Recall that $\mathbf{k}$ is **perfect** if it has characteristic 0 or if it has positive characteristic p and $\mathbf{k}^p = \mathbf{k}$. We say that $\mathbf{k}$ is **semiperfect** if it has characteristic 0 or if it has characteristic p and $[\mathbf{k} : \mathbf{k}^p] < \infty$. In [ESS1], we proved that $\mathbf{R}$ is (isomorphic to) a polynomial ring (in uncountably many variables) when the field $\mathbf{k}$ is semiperfect, and we demonstrated the utility of this result by using it to give a new proof of Stillman's conjecture; it has also been used by [DLL] to prove a finiteness theorem for Gröbner bases. In this paper, we improve our result by eliminating the hypothesis:

THEOREM 1.1. *For any field* $\mathbf{k}$, *the ring* $\mathbf{R}$ *is a polynomial ring.*

As in [ESS1], we prove an analogous result for an ultraproduct ring and establish some related results; see Section 6 for details.

1.2. Motivation

We offer three pieces of motivation for Theorem 1.1:

(a) Ananyan–Hochster [AH, Theorem B] proved the existence of "small subalgebras" over algebraically closed fields. Utilizing these algebras was one of the key insights in their proof of Stillman's conjecture. In [ESS1], we extended the Ananyan–Hochster theorem by establishing the existence of small subalgebras over perfect fields. Theorem 1.1 allows us to further strengthen this result to all fields. See Section 6.6 for details.

Received May 10, 2019. Revision received July 1, 2020.

DE was partially supported by NSF DMS-1601619. SS was partially supported by NSF DMS-1500069. AS was partially supported by NSF DMS-1453893.

(b) Ananyan and Hochster introduced a notion of "strength" for polynomials that played a central role in their work and has since featured prominently elsewhere (e.g., [AH; BDE; Dr; ESS1; ESS2]). Since strength has proven to be such a useful concept, it is desirable to understand it better. There are some genuine differences as to how strength behaves when the coefficient field is not semiperfect. For example, the results of [AH] imply that if $\mathbf{k}$ is algebraically closed, then an element $f \in \mathbf{R}$ has infinite strength if and only if the ideal of partial derivatives $(\partial f/\partial x_1, \partial f/\partial x_2, \ldots)$ has infinite codimension. This is not true if $\mathbf{k}$ fails to be semiperfect: indeed, if $a_1, a_2, \ldots \in \mathbf{k}$ are linearly independent over $\mathbf{k}^p$, then $f = \sum_{i=1}^{\infty} a_i x_i^p$ is an infinite strength element whose corresponding ideal of partial derivatives is the zero ideal. Nonetheless, Theorem 1.1 shows that some of the pleasant features of strength in the semiperfect case continue to hold for general fields: indeed, Theorem 1.1 is equivalent to the statement that if $f_1, \ldots, f_r$ are homogeneous elements of $\mathbf{R}_+$ such that no homogeneous linear combination has finite strength, then $f_1, \ldots, f_r$ are algebraically independent.

(c) In [ESS1, Section 5], we gave a geometric proof of Stillman's conjecture. The basic idea is as follows. Let X be the space of tuples $(f_1, \ldots, f_r)$ where $f_1, \ldots, f_r$ are homogeneous polynomials in infinitely many variables of fixed degrees $d_1, \ldots, d_r$. At each point $x = (f_1, \ldots, f_r)$ in X, there is a corresponding ideal $I_x = (f_1, \ldots, f_r)$ in the polynomial ring. Using the polynomiality result for $\mathbf{R}$ (or, really, the bounded version $\mathbf{R}^\flat$ discussed in Section 6.2), we proved a generic version of Stillman's conjecture: for any closed subset Z of X, the ideal I_x has bounded projective dimension for generic $x \in Z$. Appealing to Draisma's theorem [Dr] that X is $\mathbf{GL}_\infty$-Noetherian, we then deduced Stillman's conjecture from the generic version.

The generic version of Stillman's conjecture for Z involves the ring $\mathbf{R}^\flat$ where $\mathbf{k}$ is the function field of Z. In positive characteristic, this field is typically not semiperfect: for example, when Z is the entire space X, the field $\mathbf{k}$ is a rational function field in infinitely many indeterminates. Since our previous polynomiality result did not hold in this setting, our proof had some extra steps: we passed to the algebraic closure of $\mathbf{k}$ (which is perfect), carried out our argument using the polynomiality of $\mathbf{R}^\flat$ there, and then descended. Theorem 1.1 is partially motivated by the desire to eliminate this complication. We are only partially successful: we show that $\mathbf{R}^\flat$ is polynomial in some situations (such as when $Z = X$), but not all the ones used in our geometric proof of Stillman's conjecture.

Nevertheless, as we believe that the general strategy we used in our geometric approach to Stillman's conjecture can be useful in other situations, it is worth trying to simplify the details. Theorem 1.1 (and its generalizations) are a significant step in this direction.

1.3. Overview of Proof

Our proof of Theorem 1.1 is an adaptation of the method used in [ESS1, Section 2] to treat the perfect and semiperfect cases, so we first recall that. The main idea is to

characterize polynomial rings using derivations in a manner that can be applied to $\mathbf{R}$. To describe this abstract characterization, let R be a graded ring with $R_0 = \mathbf{k}$.

First, suppose that $\mathbf{k}$ has characteristic 0. We say that R has **enough derivations** if for every nonzero homogeneous element x of positive degree, there is a homogeneous derivation ∂ of R of negative degree with $\partial(x) \neq 0$. We prove [ESS1, Theorem 2.2] that R is a polynomial ring if and only if it has enough derivations. It is easy to see that the inverse limit ring $\mathbf{R}$ has enough derivations: in fact, derivatives with respect to the variables are all we need. Thus $\mathbf{R}$ is a polynomial ring.

Now suppose that $\mathbf{k}$ has positive characteristic p. Since any derivation annihilates any pth power, we cannot carry over our previous characterization of polynomial rings verbatim. Recall that a **Hasse derivation** of R is a sequence $\{\partial^n\}_{n\geq 0}$ of linear endomorphisms of R such that ∂^1 is a derivation and ∂^n behaves like $\frac{1}{n!}(\partial^1)^n$; see Definition 3.1 for the exact definition. We say that R has **enough Hasse derivations** if for every homogeneous element x that is not in the $\mathbf{k}$-span of the set R^p, there is a homogeneous Hasse derivation ∂ of negative degree such that $\partial^1(x) \neq 0$. We show [ESS1, Theorem 2.11] that R is a polynomial ring if and only if it has enough Hasse derivations. This abstract theorem does not require $\mathbf{k}$ to be perfect; see [ESS1, Remark 2.12]. When $\mathbf{k}$ is perfect, it is easy to see that $\mathbf{R}$ has enough Hasse derivations: the Hasse derivatives with respect to the variables are all we need. Thus, in this case, we see that $\mathbf{R}$ is a polynomial ring. (This reasoning can be extended to the case where $\mathbf{k}$ is semiperfect; see [ESS1, Remark 5.4].)

Here is the main kind of problem that arises when $\mathbf{k}$ is not semiperfect. Suppose that $\mathbf{k} = \mathbf{F}_p(t_1, t_2, \ldots)$ is the field of rational functions in the infinitely many variables $\{t_i\}_{i\geq 1}$, which is not semiperfect. Consider the element $f = \sum_{i\geq 1} t_i x_i^p$ of $\mathbf{R}$. This element f is not a pth power and even not a $\mathbf{k}$-linear combination of pth powers. Thus, if we wanted to prove that $\mathbf{R}$ is a polynomial ring using the criterion of the previous paragraph, we would need to produce a Hasse derivation ∂ such that $\partial^1(f) \neq 0$. However, if ∂^1 is continuous with respect to the inverse limit topology, then it commutes with the infinite sum defining f, and so $\partial^1(f) = 0$. Since all obvious Hasse derivations of $\mathbf{R}$ are continuous, it is not clear how to proceed.

Our strategy is to give a new characterization of polynomial rings via Hasse derivations that can accommodate the issue seen before. The "problem elements" in $\mathbf{R}$ (i.e., those annihilated by ∂^1 for all the obvious Hasse derivations ∂) are exactly those elements in which all variables appear with exponent divisible by p. When $\mathbf{k}$ is perfect, this is exactly $\mathbf{R}^p$; when $\mathbf{k}$ is semiperfect, it is exactly the $\mathbf{k}$-span of $\mathbf{R}^p$. However, in general, these elements cannot be directly characterized from the $\mathbf{k}$-algebra structure on $\mathbf{R}$. We therefore introduce a new piece of structure that detects these elements. Define the ring endomorphisms ϕ and σ of $\mathbf{R}$ by

$$\phi\left(\sum c_e x^e\right) = \sum c_e^p x^e, \qquad \sigma\left(\sum c_e x^e\right) = \sum c_e x^{pe},$$

where the sum is over multi-indices e. Thus ϕ raises the coefficients to the pth power, whereas σ raises the variables to the pth power. The "problem elements" are exactly those elements in the image of σ. For example, the element f defined above is $\sigma(\sum_{i\geq 1} t_i x_i)$.

Returning to the abstract setting, we define an **F-factorization** on the graded ring R to be a pair (ϕ, σ) similar to the above: ϕ is degree preserving, σ is $\mathbf{k}$-linear, and $\phi \circ \sigma = \sigma \circ \phi$ is the Frobenius map F. (There is one additional condition we demand of an F-factorization; see Definition 2.1.) Fix such a structure on R, and let $\mathcal{D}$ be a collection of Hasse derivations on R. We define the notion of admissibility for $\mathcal{D}$ (Definition 4.1). One of the key conditions is (or implies) that for every homogeneous element of R that is not in the image of σ, there exists a Hasse derivation $\partial \in \mathcal{D}$ of negative degree such that $\partial^1(x) \neq 0$.

We then show (Theorem 5.1) that R is a polynomial ring if and only if it admits an F-factorization with an admissible set $\mathcal{D}$ of Hasse derivations. The proof of Theorem 5.1, which is the heart of the paper, is similar to the proof of [ESS1, Theorem 2.11]. Essentially, we consider a hypothetical algebraic relation among a minimal generating set and use one of the given Hasse derivations to produce a relation of lower degree, eventually yielding a contradiction. The argument in this paper is somewhat more complicated due to the more limited properties of the Hasse derivations in the set $\mathcal{D}$.

Returning to $\mathbf{R}$, we have already defined an F-factorization on it. Let $\mathcal{D}$ be the set of Hasse derivatives with respect to the variables x_i. It is not too difficult to verify that $\mathcal{D}$ is admissible, and so we conclude that $\mathbf{R}$ is a polynomial ring. In essence, Theorem 5.1 enables us to work with a smaller set of Hasse derivatives than [ESS1, Theorem 2.11], thereby bypassing any need to construct discontinuous Hasse derivations on $\mathbf{R}$.

1.4. Notation and Conventions

Throughout, "graded" means graded by the nonnegative integers. The symbol p will always denote a prime number. Most of the rings we consider will have characteristic p.

2. F-Factorizations

For a ring R of characteristic p, let $F = F_R$ be the pth-power homomorphism $R \to R$. When $R = \mathbf{k}[x_i]_{i\in I}$ is a polynomial ring, F can be factored into two separate operations: raising the coefficients to the pth power and raising the monomials to the pth power. The following definition is an abstraction of this.

DEFINITION 2.1. Let R be a graded ring of characteristic p. An **F-factorization** on R is a pair (ϕ, σ) satisfying the following:

(F1) $\phi\colon R \to R$ is an injective homomorphism of graded rings satisfying $\phi|_{R_0} = F_{R_0}$.
(F2) $\sigma\colon R \to R$ is a ring homomorphism satisfying $\sigma|_{R_0} = \mathrm{id}_{R_0}$.
(F3) The maps ϕ and σ commute and satisfy $\phi \circ \sigma = F_R$.

(F4) For any $\varepsilon_1, \dots, \varepsilon_s \in R_0$, we have

$$\operatorname{im}(\sigma) \cap \sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi) = \sum_{j=1}^{s} \varepsilon_j R^p.$$

REMARK 2.2. Let (ϕ, σ) be an F-factorization on R. Then we have the following:

(a) If $a \in R_0$ and $x \in R$, then $\phi(ax) = a^p \phi(x)$.
(b) If $a \in R_0$ and $x \in R$, then $\sigma(ax) = a\sigma(x)$, that is, σ is a homomorphism of R_0-algebras.
(c) If $x \in R_0$ is homogeneous of degree d, then $\sigma(x)$ is homogeneous of degree pd. Indeed, ϕ is injective and preserves degree, and $\phi(\sigma(x)) = x^p$ is homogeneous of degree pd.

REMARK 2.3. Regarding condition (F4), we note that the inclusion $\supseteq$ follows from the other axioms. The key content of the axiom is thus the other direction, which relates elements in the $\mathbf{k}$-span of R^p to σ and ϕ.

PROPOSITION 2.4. *Let S be a graded ring of characteristic p with $S_0 = \mathbf{F}_p$, let $\mathbf{k}$ be a field of characteristic p, and let $R = \mathbf{k} \otimes_{\mathbf{F}_p} S$. Put $\phi = F_{\mathbf{k}} \otimes \mathrm{id}_S$ and $\sigma = \mathrm{id}_{\mathbf{k}} \otimes F_S$. Then (ϕ, σ) is an F-factorization on R.*

Proof. Conditions (F1), (F2), and (F3) are easy to see directly. We prove (F4). Let $\varepsilon_1, \dots, \varepsilon_s \in R_0$; we may assume, without loss of generality, that they are linearly independent over R_0^p. The inclusion $\sum_j \varepsilon_j R^p \subseteq \operatorname{im}(\sigma) \cap \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi)$ holds since every element in R^p is in the image of both σ and ϕ. Conversely, suppose that f is an element of $\operatorname{im}(\sigma) \cap \sum_j \varepsilon_j \operatorname{im}(\phi)$. Write $f = \sum a_e x^e$, where the sum is over multi-indices e, and $a_e \in \mathbf{k}$. Since $f \in \operatorname{im}(\sigma)$, we have $a_e = 0$ unless $p \mid e$. Since $f \in \sum_j \varepsilon_j \operatorname{im}(\phi)$, we can write $f = \sum_j \varepsilon_j \phi(g_j)$ for some $g_j \in R$. Write $g_j = \sum b_{j,e} x^e$. Equating the coefficients, we find $a_e = \sum_{j=1}^s \varepsilon_j b_{j,e}^p$. If $p \nmid e$, then this vanishes; since ε_j are linearly independent over $\mathbf{k}^p$, it follows that each $b_{j,e}$ vanishes as well. We conclude that all monomials appearing in g_j with nonzero coefficient are pth powers; in other words, we can write $g_j = \sigma(h_j)$ where $h_j = \sum b_{j,pe} x^e$. We thus find $f = \sum_{j=1}^s \varepsilon_j \phi(\sigma(h_j)) \in \sum_{j=1}^s \varepsilon_j R^p$. □

EXAMPLE 2.5. Let $R = \mathbf{k}[x_i]_{i \in I}$ be a polynomial ring where each x_i is homogeneous of positive degree. Letting $S = \mathbf{F}_p[x_i]_{i \in I}$, we have $R = \mathbf{k} \otimes_{\mathbf{F}_p} S$. Proposition 2.4 provides an F-factorization on R, which we call the **standard F-factorization** on R. We note that it depends on the choice of variables, that is, it is not invariant under automorphisms of R (in the category of graded $\mathbf{k}$-algebras).

PROPOSITION 2.6. *Let R be a graded ring with an F-factorization (ϕ, σ). Then R is reduced if and only if σ is injective.*

Proof. The ring R is reduced if and only if $F = F_R$ is injective. Since F factors as $\phi \circ \sigma$ and ϕ is injective, we see that F is injective if and only if σ is injective. □

PROPOSITION 2.7. *Let R be a reduced graded ring with an F-factorization (ϕ, σ). Let $\varepsilon_1, \dots, \varepsilon_s \in R_0$, and let $x \in R$. Suppose that $\sigma(x) \in \sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$. Then $x \in \sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$.*

Proof. The element $\sigma(x)$ belongs to $\operatorname{im}(\sigma) \cap \sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$, which is equal to $\sum_{j=1}^{s} \varepsilon_j R^p$ by (F4). We can thus write $\sigma(x) = \sum_{j=1}^{s} \varepsilon_j y_j^p$ for elements $y_j \in R$. Since $y_j^p = \sigma(\phi(y_j))$ and σ is injective (Proposition 2.6), we see that $x = \sum_{j=1}^{s} \varepsilon_j \phi(y_j)$. □

DEFINITION 2.8. Let R be a graded ring with an F-factorization (ϕ, σ). We define a decreasing filtration $\{\mathcal{F}^r R\}_{r \geq 0}$ on R by $\mathcal{F}^r R = \operatorname{im}(\sigma^r)$. We call this the **level filtration**. We define the **level** of $x \in R$ to be the supremum of the set $\{r \in \mathbf{N} \mid x \in \mathcal{F}^r R\}$. For a subspace V of R, we let $\mathcal{F}^r V = V \cap \mathcal{F}^r R$.

REMARK 2.9. If x is nonzero and of positive degree d, and p^t is the maximum power of p dividing d, then x has level at most t. Thus the level filtration on R_d is finite, that is, $\mathcal{F}^r R_d = 0$ for $r \gg d$ (in fact, $r > t$).

3. Hasse Derivations

DEFINITION 3.1. Let R be a ring. A **Hasse derivation** on R is a collection $\partial = \{\partial^n\}_{n \in \mathbf{N}}$ of additive endomorphisms of R such that $\partial^0 = \mathrm{id}$ and the identity

$$\partial^n(xy) = \sum_{i+j=n} \partial^i(x) \partial^j(y)$$

holds for all $x, y \in R$. If R has characteristic p, then we write $\partial^{[r]}$ in place of ∂^{p^r}.

DEFINITION 3.2. Let R be a graded ring, and let ∂ be a Hasse derivation on R. We say that ∂ is **homogeneous of degree** d if for all homogeneous elements x of R, the element $\partial^n(x)$ is homogeneous of degree $\deg(x) + nd$.

EXAMPLE 3.3. Let $R = \mathbf{k}[x]$. Define ∂^n to be the endomorphism of R mapping x^k to $\binom{k}{n} x^{k-n}$; here, as always, $\binom{k}{n} = 0$ for $k < n$. Then ∂ is a Hasse derivation. Indeed, it suffices to check the defining identity on monomials. We have

$$\partial^n(x^a x^b) = \binom{a+b}{n} x^{a+b-n},$$

$$\sum_{i+j=n} \partial^i(x^a) \partial^j(x^b) = \sum_{i+j=n} \binom{a}{i} \binom{b}{j} x^{a+b-n},$$

which are equal by a standard identity on binomial coefficients (think about choosing a subset of size n from $\{1, \dots, a\} \amalg \{a+1, \dots, a+b\}$). We call ∂ the **Hasse derivative**.

More generally, suppose $R = \mathbf{k}[x_i]_{i \in I}$ is a multivariate polynomial ring and pick $j \in I$. Then the Hasse derivative on $\mathbf{k}[x_j]$ can be extended to R by making it linear over $\mathbf{k}[x_i]_{i \in I \setminus \{j\}}$. We call this Hasse derivation on R the Hasse derivative

with respect to x_j. If R is graded and x_j is homogeneous of degree d, then the Hasse derivative with respect to x_j is homogeneous of degree $-d$.

PROPOSITION 3.4. *Let ∂ be a Hasse derivation on the ring R, let $x \in R$, and let $k > 0$. Then $\partial^k(x^n)$ can be expressed as a polynomial in x of degree $\leq n-1$ with coefficients in the subalgebra $\mathbf{Z}[\partial^i(x)]_{1\leq i\leq k}$.*

Proof. If $n = 1$, then there is nothing to prove. Otherwise, we write

$$\partial^k(x^n) = \sum_{i+j=k} \partial^i(x^{n-1})\partial^j(x),$$

and the result follows by induction on n and k. □

PROPOSITION 3.5. *Let R be a ring of characteristic p. Let ∂ be a Hasse derivation on R, and let $x \in R$. Then*

$$\partial^{[r]}(F^s x) = \begin{cases} F^s(\partial^{[r-s]}x) & \text{if } r \geq s, \\ 0 & \text{if } r \leq s. \end{cases}$$

Proof. See [ESS1, Lemma 2.9]. □

The following corollary of the proposition will be used constantly without reference.

COROLLARY 3.6. *Let R have characteristic p, and let $\varepsilon_1, \ldots, \varepsilon_s \in R_0$. Then for any R_0-linear Hasse derivation ∂, the space $\sum_{j=1}^s \varepsilon_j R^p$ is killed by $\partial^{[0]}$ and stable under $\partial^{[r]}$ for all $r \geq 0$.*

4. Admissible Sets

Throughout this section we fix a graded ring R, where R_0 is a field of characteristic p, and we fix an F-factorization (ϕ, σ) on R.

DEFINITION 4.1. Let $\mathcal{D}$ be a set of Hasse derivations on R. We say that $\mathcal{D}$ is **admissible** (with respect to (ϕ, σ)) if the following conditions are satisfied:

(D1) Each $\partial \in \mathcal{D}$ is homogeneous of negative degree.
(D2) Each $\partial \in \mathcal{D}$ commutes with ϕ.
(D3) Let $x \in R$ be homogeneous, and let $\varepsilon_1, \ldots, \varepsilon_s \in R_0$ (we allow $s = 0$). Suppose that $\partial^{[0]}(x) \in \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi)$ for all $\partial \in \mathcal{D}$. Then $x \in \operatorname{im}(\sigma) + \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi)$.

REMARK 4.2. Suppose that $\mathbf{k}$ is a perfect field of characteristic p, that R has the form $\mathbf{k} \otimes_{\mathbf{F}_p} S$ for some graded ring S with $S_0 = \mathbf{F}_p$, and that R is equipped with the F-factorization constructed in Proposition 2.4. Then ϕ is surjective, and $\operatorname{im}(\sigma) = R^p$. Thus condition (D3) is vacuous if some ε_i is nonzero. If all ε_i vanish (or if $s = 0$), then it simply states that $\bigcap_{\partial\in\mathcal{D}} \ker(\partial^1) = R^p$. Furthermore, a Hasse derivation of R commutes with ϕ if and only if it comes from a Hasse derivation of

S by extension of scalars. Thus R admits an admissible set of Hasse derivations if and only if S has enough Hasse derivations in the sense of [ESS1, Definition 2.10]. (In fact, using [ESS1, Theorem 2.11], we can show that S has enough Hasse derivations if and only if R has.)

EXAMPLE 4.3. Suppose $R = \mathbf{k}[x_i]_{i \in I}$ and (ϕ, σ) is the standard F-factorization. Let $\mathcal{D}$ be the collection of Hasse derivatives with respect to the variables. We claim that this is admissible. Conditions (D1) and (D2) are immediate, so we check (D3). Pick $\varepsilon_1, \dots, \varepsilon_s \in R_0$ and suppose that $\partial^{[0]}(f) \in \sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$ for all Hasse derivatives ∂. Write $f = \sum c_e x^e$, where the sum is over multi-indices e, and let $V \subset \mathbf{k}$ be the $\mathbf{k}^p$-span of $\varepsilon_1, \dots, \varepsilon_s$. Then $\sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$ consists of those elements of R for which all coefficients belong to V, whereas $\operatorname{im}(\sigma)$ consists of those elements of R for which all exponents are divisible by p. Thus to show that f belongs to $\operatorname{im}(\sigma) + \sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$, we must show that if e is not divisible by p, then c_e belongs to V. Let such e be given, and pick $i \in I$ such that e_i is not divisible by p. Let ∂ be the Hasse derivative with respect to x_i. Then $\partial^{[0]}(x^e) = e_i x^{e'}$, where e' is obtained from e by decrementing the ith entry by one. By assumption, $\partial^{[0]}(f)$ belongs to $\sum_{j=1}^{s} \varepsilon_j \operatorname{im}(\phi)$, and so all coefficients of $\partial^{[0]}(f)$ belong to V. The coefficient of $x^{e'}$ is exactly $e_i c_e$. Since e_i is a nonzero element of $\mathbf{k}^p$, as it is an integer not divisible by p, it follows that $c_e \in V$, and so the result follows.

For the remainder of this section, we fix an admissible set $\mathcal{D}$ and deduce some simple consequences of the definitions.

PROPOSITION 4.4. *Each $\partial \in \mathcal{D}$ is R_0-linear.*

Proof. Let $a \in R_0$ and $x \in R$. We have $\partial^n(ax) = \sum_{i+j=n} \partial^i(a)\partial^j(x)$. We have $\deg(\partial^i(a)) = i \deg(\partial)$, which is negative for $i > 0$ and thus vanishes. Hence $\partial^n(ax) = a\partial^n(x)$. □

PROPOSITION 4.5. *Let $\partial \in \mathcal{D}$. Then*

$$\partial^{[s]}(\sigma^r(x)) = \begin{cases} \sigma^r(\partial^{[s-r]}(x)) & \text{if } r \le s, \\ 0 & \text{if } r > s. \end{cases}$$

Proof. We can check after applying ϕ^r to each side, since ϕ is injective. The result now follows from Proposition 3.5. □

COROLLARY 4.6. *Let $x \in R$ be an element of level $\ge t$. Then*

$$\partial^{[t]}(x^n) = nx^{n-1}\partial^{[t]}(x).$$

Proof. Write $x = \sigma^t(y)$ for some $y \in R$. By Proposition 4.5 we have

$$\partial^{[t]}(\sigma^t(y^n)) = \sigma^t(\partial^{[0]}(y^n)) = \sigma^t(ny^{n-1}\partial^{[0]}(y)) = nx^{n-1}\partial^{[t]}(\sigma^t(y)). \qquad \square$$

PROPOSITION 4.7. *We have $\bigcap_{\partial \in \mathcal{D}} \ker(\partial^{[0]}) = \operatorname{im}(\sigma)$.*

Proof. We have $\operatorname{im}(\sigma) \subset \ker(\partial^{[0]})$ for any $\partial \in \mathcal{D}$ by Proposition 4.5. Conversely, suppose that $\partial^{[0]}(x) = 0$ for all $\partial \in \mathcal{D}$. By (D3) with $s = 0$ we find $x \in \operatorname{im}(\sigma)$. □

PROPOSITION 4.8. *The ring R is reduced.*

Proof. We must show that σ is injective (Proposition 2.6). Suppose not, and let $x \in R$ be a nonzero homogeneous element of minimal degree with $\sigma^k(x) = 0$ for some k. Then $x \notin \operatorname{im}(\sigma)$; indeed, if $x = \sigma(y)$, then y would have lower degree and $\sigma^{k+1}(y) = 0$, contradicting the choice of x. Since $x \notin \operatorname{im}(\sigma)$, there exists $\partial \in \mathcal{D}$ with $\partial^{[0]}(x) \neq 0$ by Proposition 4.7. But then $0 = \partial^{[k]}(\sigma^k(x)) = \sigma^k(\partial^{[0]}x)$ (Proposition 4.5), and $\partial^{[0]}(x)$ has lower degree than x, again contradicting the choice of x. It follows that σ is injective. □

PROPOSITION 4.9. *Let $x \in R$. The following are equivalent*:

(a) *x has level $\geq t$.*
(b) *$\partial^{[r]}(x) = 0$ for all $0 \leq r < t$ and $\partial \in \mathcal{D}$.*

Proof. Proposition 4.5 shows that (a) implies (b). Conversely, suppose that (b) holds, and say that x has level $s < t$. Write $x = \sigma^s(y)$. Then $0 = \partial^{[s]}(x) = \sigma^s(\partial^{[0]}(y))$ for all $\partial \in \mathcal{D}$. Since σ is injective (Propositions 2.6 and 4.8), we have $\partial^{[0]}(y) = 0$. Since this holds for all ∂, we have $y = \sigma(z)$ for some z by Proposition 4.7, and so $x = \sigma^{s+1}(z)$, contradicting the assumption that x has level s. Thus x has level $\geq t$. □

COROLLARY 4.10. *If $x \in R$ is homogeneous of positive degree and $\partial^{[r]}(x) = 0$ for all $r \geq 0$ and $\partial \in \mathcal{D}$, then $x = 0$.*

Proof. By Proposition 4.9, x has level $\geq t$ for all t, and so $x = 0$. (Recall that $\mathcal{F}^t R_d = 0$ for $t \gg 0$ and $d > 0$.) □

PROPOSITION 4.11. *Let $\varepsilon_1, \ldots, \varepsilon_s \in R_0$. Suppose that $x \in R$ has level $\geq r \geq 1$, and $\partial^{[r]}(x) \in \sum_{j=1}^s \varepsilon_j R^p$ for all $\partial \in \mathcal{D}$. Then $x \in \operatorname{im}(\sigma^{r+1}) + \sum_{j=1}^s \varepsilon_j \operatorname{im}(\sigma^r \phi)$. In particular, $x \in \operatorname{im}(\sigma^{r+1}) + \sum_{j=1}^s \varepsilon_j R^p$.*

Proof. Write $x = \sigma^r(y)$. Let $\partial \in \mathcal{D}$ and write $\partial^{[r]}(x) = \sum_{j=1}^s \varepsilon_j z_i^p$. Then

$$\sigma^r(\partial^{[0]}(y)) = \partial^{[r]}(x) = \sum_{j=1}^{s} \varepsilon_j \sigma(\phi(z_i)).$$

Since σ is injective (Propositions 2.6 and 4.8), we find $\sigma^{r-1}(\partial^{[0]}(y)) \in \sum_{j=1}^s \varepsilon_j \times \operatorname{im}(\phi)$, from which it follows (by Proposition 2.7) that $\partial^{[0]}(y) \in \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi)$. Since this holds for all $\partial \in \mathcal{D}$, we see from (D3) that $y \in \operatorname{im}(\sigma) + \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi)$. Applying σ^r yields the stated result. □

5. The Polynomiality Theorem

5.1. Main Theorem and Initial Reductions

The following is the main theorem of this section.

THEOREM 5.1. *Let R be a graded ring such that R_0 is a field of characteristic p. The R is a polynomial ring if and only if it admits an F-factorization with an admissible set of Hasse derivations.*

The rest of this section is devoted to the proof of the theorem. From Examples 2.5 and 4.3 we see that a polynomial ring admits an F-factorization with an admissible set of Hasse derivations. We must prove the converse. We will do this via a series of reductions and induction arguments. We further give two statements $\mathscr{A}_{\mathcal{E}}$ and $\mathscr{I}$; their connections to the main theorem are as follows:

$$\mathscr{I} \overset{\text{Lemma 5.3}}{\Longrightarrow} \mathscr{A}_{\mathcal{E}} \overset{\text{Lemma 5.2}}{\Longrightarrow} \text{Theorem 5.1}.$$

The proof of $\mathscr{I}$ is handled in Section 5.2.

For the rest of this section, we fix the ring R, an F-factorization (ϕ, σ) on R, and an admissible set $\mathcal{D}$ of Hasse derivations on R. We put $\mathbf{k} = R_0$ and write R_+ for the homogeneous maximal ideal of R.

Recall the level filtration $\mathcal{F}^\bullet R$ on R (Definition 2.8). We define $\mathcal{F}^r(R_+/R_+^2)$ to be the image of $\mathcal{F}^r R_+$. By definition every level r element of R_+/R_+^2 admits a level r lift to R_+. Let $\overline{\mathcal{E}}$ be a basis of R_+/R_+^2 consisting of homogeneous elements that is compatible with the level filtration. We write $\overline{\mathcal{E}}_{d,r}$ for the set of degree d level r elements in $\overline{\mathcal{E}}$. The compatibility with the filtration means that $\bigcup_{s \geq r} \overline{\mathcal{E}}_{d,s}$ forms a basis of $\mathcal{F}^r(R_+/R_+^2)_d$ for all r and d. We let $\mathcal{E}_{d,r}$ be a set of degree d level r elements of R mapping bijectively to $\overline{\mathcal{E}}_{d,r}$ under the reduction map, and we let $\mathcal{E}$ be the union of these sets. Since $\mathcal{E}$ lifts a basis of R_+/R_+^2, it generates R as a $\mathbf{k}$-algebra. Our goal is to show that $\mathcal{E}$ is algebraically independent.

For a subset E of $\mathcal{E}$, consider the following statement:

$\mathscr{A}_E$: Let $x_1, \dots, x_n \in E$ be distinct elements, and let $\varepsilon_1, \dots, \varepsilon_s \in \mathbf{k}$ (we allow $s = 0$). Suppose that $f(x_1, \dots, x_n) \in \sum_{j=1}^s \varepsilon_j R^p$ for some polynomial $f \in \mathbf{k}[X_1, \dots, X_n]$. Then $f \in \sum_{j=1}^s \varepsilon_j \mathbf{k}[X_1, \dots, X_n]^p$.

It suffices to prove this statement for $E = \mathcal{E}$:

LEMMA 5.2. *If $\mathscr{A}_{\mathcal{E}}$ holds, then $\mathcal{E}$ is algebraically independent.*

Proof. Suppose that $f(x_1, \dots, x_n) = 0$ is an algebraic relation between distinct elements of $\mathcal{E}$. By $\mathscr{A}_{\mathcal{E}}$ with $s = 0$ we find $f = 0$. Thus $\mathcal{E}$ is algebraically independent. □

We will prove $\mathscr{A}_E$ for all E by induction on E. We have to proceed somewhat carefully in this induction. The precise inductive statement is the following:

$\mathscr{I}$: Fix d and t and let E be a subset of $\mathcal{E}$ satisfying the following:

$$\mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,>t} \subset E \subset \mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,\geq t}.$$

Let $x \in \mathcal{E}_{d,t} \setminus E$, and let $E' = E \cup \{x\}$. Then $\mathscr{A}_E$ implies $\mathscr{A}_{E'}$.

LEMMA 5.3. *If $\mathscr{I}$ holds, then $\mathscr{A}_{\mathcal{E}}$ holds.*

Proof. In this proof, we write $\mathscr{A}(E)$ in place of $\mathscr{A}_E$ for readability. Note that if E is a directed union of some family of subsets $\{E_i\}_{i\in I}$, then $\mathscr{A}(E)$ holds if and only if $\mathscr{A}(E_i)$ holds for all $i \in I$. We use this several times.

We prove that $\mathscr{A}(\mathcal{E}_{\leq d,\bullet})$ holds for all d by induction on d. Thus suppose that $\mathscr{A}(\mathcal{E}_{<d,\bullet})$ holds and let us show that $\mathscr{A}(\mathcal{E}_{\leq d,\bullet})$ holds. To do this, we show that $\mathscr{A}(\mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,\geq t})$ holds for all t, by descending induction on t. For $t \gg 0$, the statement is vacuous since $\mathcal{E}_{d,\geq t}$ is empty. Thus assume that $\mathscr{A}(\mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,>t})$ holds, and let us show that $\mathscr{A}(\mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,\geq t})$ holds. To do this, it suffices to show that $\mathscr{A}(\mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,>t} \cup \{e_1, \ldots, e_r\})$ holds for all finite subsets $\{e_1, \ldots, e_r\}$ of $\mathcal{E}_{d,t}$. This follows inductively by applying $\mathscr{I}$ with $x = e_i$ and $E = \mathcal{E}_{<d,\bullet} \cup \mathcal{E}_{d,>t} \cup \{e_1, \ldots, e_{i-1}\}$ for $i = 1, \ldots, r$. □

5.2. *Proof of $\mathscr{I}$*

We now prove statement $\mathscr{I}$. Fix d, t, E, x, and E' as in $\mathscr{I}$, and suppose $\mathscr{A}_E$ holds. We will prove $\mathscr{A}_{E'}$. For this, we will further introduce auxiliary statements $\mathscr{B}_{n,m}$, $\mathscr{C}$, and $\mathscr{C}'$. The logical implications between these statements are as follows:

$$\mathscr{A}_E \text{ and } \mathscr{B}_{n,m} \text{ for all } n \text{ and } m \overset{\text{Lemma } 5.6}{\Longrightarrow} \mathscr{A}_{E'},$$

$$(\mathscr{B}_{k,\ell} \text{ for all } k < n \text{ and all } \ell) \text{ and } (\mathscr{B}_{n,k} \text{ for all } k < m) \text{ and } \mathscr{C} \Longrightarrow \mathscr{B}_{n,m},$$

$$\text{Lemma } 5.10 \Longrightarrow \mathscr{C}', \qquad \mathscr{C}' \overset{\text{Lemma } 5.8}{\Longrightarrow} \mathscr{C}.$$

In words, the first statement shows that we can deduce $\mathscr{A}_{E'}$ from $\mathscr{B}_{n,m}$ for all n and m, since we have assumed that $\mathscr{A}_E$ holds. The second statement shows that we can prove $\mathscr{B}_{n,m}$ using induction on (n, m), once we have $\mathscr{C}$. And the final statement shows that $\mathscr{C}$ is implied by $\mathscr{C}'$, which, in turn, is established by Lemma 5.10.

We now start on the details. We let $A \subset R$ be the $\mathbf{k}$-subalgebra generated by E.

LEMMA 5.4. *The element x does not belong to A.*

Proof. Suppose x could be expressed as a polynomial in the elements in E. Reducing this expression modulo R_+^2, we would find that x belongs to the $\mathbf{k}$-span of E. But this contradicts the linear independence of the set $\mathcal{E}$. □

LEMMA 5.5. *Let $y \in R$ be homogeneous. Suppose y has degree $< d$, or degree d and level $> t$. Then $y \in A$.*

Proof. First suppose y has degree $e < d$. Then the image of y in R_+/R_+^2 is a linear combination of elements of $\overline{\mathcal{E}}_{e,\bullet}$. Thus if y' is the corresponding linear

combination of elements of $\mathcal{E}_{e,\bullet}$, then $y - y' \in R_+^2$, that is, we can write $y - y' = \sum_{i=1}^n a_i b_i$ with a_i and b_i of degree $< e$. By induction on e the elements a_i and b_i belong to A, whereas y' belongs to A by definition. Thus $y \in A$, as required.

Now suppose that $\deg(y) = d$ and y has level $> t$. Then the image of y in R_+/R_+^2 is a linear combination of elements of $\overline{\mathcal{E}}_{d,>t}$. Again, taking y' to be the corresponding linear combination of elements of $\mathcal{E}_{d,>t}$, we see that $y - y' \in R_+^2$. Thus the same reasoning shows that $y \in A$. □

By Lemma 5.5 we see that $\partial^k(x) \in A$ for any $\partial \in \mathcal{D}$ and $k > 0$, as $\partial^k(x)$ has degree $< d$. It follows from Proposition 3.4 that for $k \geq 1$, $n \geq 1$, and $\partial \in \mathcal{D}$, the element $\partial^k(x^n)$ can be expressed as a polynomial in x of degree $\leq n - 1$ with coefficients in A. We further use this constantly and without reference.

Consider the following statement:

$\mathscr{B}_{n,m}$: Let $a_0, \dots, a_n \in A$ with $\deg(a_n) \leq m$, and let $\varepsilon_1, \dots, \varepsilon_s \in \mathbf{k}$. Suppose that $\sum_{i=0}^n a_i x^i \in \sum_{j=1}^s \varepsilon_j R^p$. Then $a_i \in \sum_{j=1}^s \varepsilon_j R^p$ for all i, and $a_i = 0$ if $p \nmid i$.

We note that in the conclusion it would be equivalent to state that $a_i \in \sum_{j=1}^s \varepsilon_j A^p$, since $\mathscr{A}_E$ holds.

LEMMA 5.6. *Suppose $\mathscr{B}_{n,m}$ holds for all n and m. Then $\mathscr{A}_{E'}$ holds.*

Proof. Let $x_1, \dots, x_k$ be distinct elements of E' and suppose $f(x_1, \dots, x_k) \in \sum_{j=1}^s \varepsilon_j R^p$. Without loss of generality, we may assume that $x_k = x$ and $x_1, \dots, x_{k-1} \in E$. Write $f(X_1, \dots, X_k) = \sum_{i=0}^n g_i(X_1, \dots, X_{k-1}) X_k^i$ for polynomials g_i. Then $\sum_{i=0}^n g_i(x_1, \dots, x_{k-1}) x^i \in \sum_{j=1}^s \varepsilon_j R^p$. By $\mathscr{B}_{n,\bullet}$ we see that $g_i(x_1, \dots, x_{k-1}) \in \sum_{j=1}^s \varepsilon_j R^p$ for all i and $g_i(x_1, \dots, x_{k-1}) = 0$ for $p \nmid i$. By $\mathscr{A}_E$ we see that $g_i \in \sum_{j=1}^s \varepsilon_j \mathbf{k}[X_1, \dots, X_{k-1}]^p$ for all i and (by taking $s = 0$) $g_i = 0$ for $p \nmid i$. It follows that $f \in \sum_{j=1}^s \varepsilon_j \mathbf{k}[X_1, \dots, X_k]^p$, and so $\mathscr{A}_{E'}$ holds. □

We now prove the statement $\mathscr{B}_{n,m}$ for all n and m. We do this by induction on n and m. It is clear that $\mathscr{B}_{0,m}$ holds for all m. We now fix $n > 0$ and $m \geq 0$ and assume that $\mathscr{B}_{<n,\bullet}$ and $\mathscr{B}_{n,<m}$ hold, and we will prove that $\mathscr{B}_{n,m}$ holds. To this end, fix $a_0, \dots, a_n \in A$ with $\deg(a_n) \leq m$ and $\varepsilon_1, \dots, \varepsilon_s \in \mathbf{k}$ such that

$$\sum_{i=0}^n a_i x^i \in \sum_{j=1}^s \varepsilon_j R^p. \tag{5.7}$$

We must prove:

($\mathscr{C}$) We have $a_i \in \sum_{j=1}^s \varepsilon_j R^p$ for all i and $a_i = 0$ for $p \nmid i$.

Clearly, if we do this, then we will have established $\mathscr{B}_{n,m}$, and the theorem will follow. Without loss of generality, we assume $\varepsilon_1, \dots, \varepsilon_s$ to be linearly independent over $\mathbf{k}^p$. Before tackling $\mathscr{C}$, we make one simple reduction. Consider the following statement:

($\mathscr{C}'$) We have $a_n \in \sum_{j=1}^s \varepsilon_j R^p$ and $a_n = 0$ if $p \nmid n$.

The following lemma shows that it suffices to prove this statement.

LEMMA 5.8. *If $\mathscr{C}'$ holds, then $\mathscr{C}$ holds.*

Proof. Suppose $\mathscr{C}'$ holds. Combining this with (5.7), we see that $\sum_{i=0}^{n-1} a_i x^i$ belongs to $\sum_{j=1}^{s} \varepsilon_j R^p$. Thus by $\mathscr{B}_{<n,\bullet}$ we see that a_i belongs to $\sum_{j=1}^{s} \varepsilon_j R^p$ and $a_i = 0$ for $p \nmid i$, at least for $0 \leq i \leq n-1$. Of course, by $\mathscr{C}'$ we know this for $i = n$ as well. Thus $\mathscr{C}$ holds. □

Before establishing $\mathscr{C}'$, we need one auxiliary lemma:

LEMMA 5.9. *Suppose that we have the equation $\sum_{j=1}^{N} \delta_j y_j = 0$ where δ_j belong to $\mathbf{k}$, y_j belong to R^p, and not all y_j vanish. Then δ_j are linearly dependent over $\mathbf{k}^p$.*

Proof. We can assume that all y_j have the same degree, and we proceed by induction on the degree. If y_j have degree 0, then the statement is clear. Otherwise, we can find $\partial \in \mathcal{D}$ such that $\partial^{[r]}(y_j) \neq 0$ for some $r \geq 1$ and j (Corollary 4.10). Applying this to the given equation yields $\sum_{j=1}^{N} \delta_j \partial^{[r]}(y_j) = 0$. Each $\partial^{[r]}(y_j)$ is a pth power (Proposition 3.5), and not all vanish. Since the degree has dropped, the result follows by induction. □

We now come to the heart of the argument.

LEMMA 5.10. *Statement $\mathscr{C}'$ holds.*

Proof. We proceed in five cases. In what follows, in expressions such as $ax^{n-1} + \cdots$, the $\cdots$ will always refer to an A-linear combination of lower powers of x.

Case 1: *p does not divide n or $n-1$, and $m = 0$.* Since $m = 0$, the leading coefficient a_n is constant. We must show that it vanishes. Recall that t is the level of x. We first claim that a_{n-1} has level $\geq t$. Let $0 \leq r < t$. Applying $\partial^{[r]}$ to (5.7) for some $\partial \in \mathcal{D}$ and using the fact that $\partial^{[r]}(x) = 0$ (Proposition 4.9) and thus that $\partial^{[r]}(x^n) = 0$ (Corollary 4.6), we see that $\partial^{[r]}(a_{n-1})x^{n-1} + \cdots \in \sum_{j=1}^{s} \varepsilon_j R^p$. By $\mathscr{B}_{n-1,\bullet}$ we see that $\partial^{[r]}(a_{n-1}) = 0$ (here we are using $p \nmid n-1$). Since this holds for all $\partial \in \mathcal{D}$, we conclude that a_{n-1} has level $\geq t$ (Proposition 4.9).

Now apply $\partial^{[t]}$ to (5.7) for some $\partial \in \mathcal{D}$. Using the identity $\partial^{[t]}(x^n) = nx^{n-1}\partial^{[t]}(x)$ (Corollary 4.6), we see that the coefficient of x^{n-1} in the result is $\partial^{[t]}(na_n x + a_{n-1})$. We thus have

$$\partial^{[t]}(na_n x + a_{n-1})x^{n-1} + \cdots \in \sum_{j=1}^{s} \varepsilon_j R^p.$$

Applying $\mathscr{B}_{n-1,m}$ and using $p \nmid n-1$, we see that $\partial^{[t]}(na_n x + a_{n-1}) = 0$. Since we already saw that $na_n x + a_{n-1}$ has level $\geq t$, this shows that $na_n x + a_{n-1}$ has level $\geq t+1$ (Proposition 4.9). Since $na_n x + a_{n-1}$ has the same degree d as x but greater level, it belongs to A (Lemma 5.5). Since a_{n-1} also belongs to A and $n \neq 0$ in $\mathbf{k}$, we see that $a_n x$ belongs to A. Since x does not belong to A (Lemma 5.4), we see that $a_n = 0$, which completes the proof.

Case 2: *p does not divide n, p does divide $n-1$, and $m=0$.* The argument is similar to the previous case. We first treat the case $t=0$. Applying $\partial^{[0]}$ to (5.7), for some $\partial \in \mathcal{D}$, we find

$$\partial^{[0]}(na_nx + a_{n-1})x^{n-1} + \cdots = 0.$$

By $\mathscr{B}_{n-1,\bullet}$ with $s=0$, we see that $\partial^{[0]}(na_nx + a_{n-1}) = 0$. Since this holds for all $\partial \in \mathcal{D}$, we see that $na_nx + a_{n-1}$ has level ≥ 1. As in Case 1, this implies $na_nx + a_{n-1} \in A$, from which we conclude $a_n = 0$.

Now suppose $t > 0$. We first claim that there is some $b \in \sum_{j=1}^{s} \varepsilon_j R^p$ such that $a_{n-1} + b$ is homogeneous and has level $\geq t$. To begin, applying $\partial^{[0]}$ to (5.7) for some $\partial \in \mathcal{D}$, we find $\partial^{[0]}(a_{n-1})x^{n-1} + \cdots = 0$, whence $\partial^{[0]}(a_{n-1}) = 0$ by $\mathscr{B}_{n-1,\bullet}$ (with $s=0$). Since this holds for all $\partial \in \mathcal{D}$, we see that a_{n-1} has level ≥ 1. Now suppose $1 \leq k < t$ and we can find $b \in \sum_{j=1}^{s} \varepsilon_j R^p$ so that $a_{n-1} + b$ is homogeneous and has level $\geq k$. We have just shown this to be the case for $k=1$, by taking $b=0$. Applying $\partial^{[k]}$ to (5.7) for some $\partial \in \mathcal{D}$, we find $\partial^{[k]}(a_{n-1})x^{n-1} + \cdots \in \sum_{j=1}^{s} \varepsilon_j R^p$. By $\mathscr{B}_{n-1,\bullet}$ we see that $\partial^{[k]}(a_{n-1}) \in \sum_{j=1}^{s} \varepsilon_j R^p$. Thus we have $\partial^{[k]}(a_{n-1} + b) \in \sum_{j=1}^{s} \varepsilon_j R^p$ as well. Since $a_{n-1} + b$ has level $\geq k$ and this holds for all $\partial \in \mathcal{D}$, Proposition 4.11 implies $a_{n-1} + b = \sigma^{k+1}(c) + b'$ for some $b' \in \sum_{j=1}^{s} \varepsilon_j R^p$. Thus $a_{n-1} + (b - b')$ has level $\geq k+1$. Replacing b with $b - b'$ and continuing, the claim follows.

Fix $b \in \sum_{j=1}^{s} \varepsilon_j R^p$ so that $a_{n-1} + b$ has level $\geq t$. Apply $\partial^{[t]}$ to (5.7) for some $\partial \in \mathcal{D}$. We find

$$\partial^{[t]}(na_nx + a_{n-1})x^{n-1} + \cdots \in \sum_{j=1}^{s} \varepsilon_j R^p.$$

By $\mathscr{B}_{n-1,\bullet}$ we find $\partial^{[t]}(na_nx + a_{n-1}) \in \sum_{j=1}^{s} \varepsilon_j R^p$. Of course, we also have $\partial^{[t]}(na_nx + a_{n-1} + b) \in \sum_{j=1}^{s} \varepsilon_j R^p$ by Corollary 3.6 because $b \in \sum_{j=1}^{s} \varepsilon_j R^p$. Since this holds for all $\partial \in \mathcal{D}$ and $na_nx + a_{n-1} + b$ has level $\geq t$ with $t > 0$, Proposition 4.11 implies $na_nx + a_{n-1} + b = \sigma^{t+1}(y) + b'$ for some $b' \in \sum_{j=1}^{s} \varepsilon_j R^p$, and we may further assume that $\sigma^{t+1}(y)$ and b' are homogeneous of the same degree. Since $\sigma^{t+1}(y)$ has the same degree as x but higher level, it belongs to A. Since b and b' have the same degree as x and belong to R_+^2, they also belong to A. Thus we find $a_nx \in A$, and so $a_n = 0$.

Case 3: *p does not divide n and $m > 0$.* If $\deg(a_n) = 0$, then the result follows from $\mathscr{B}_{n,<m}$, so we assume that $\deg(a_n) > 0$. Applying $\partial^{[r]}$ to (5.7) for some $\partial \in \mathcal{D}$ and $r \geq 0$, we find

$$\partial^{[r]}(a_n)x^n + \cdots \in \sum_{j=1}^{s} \varepsilon_j R^p.$$

By $\mathscr{B}_{n,m-1}$ and the fact that $p \nmid n$ we conclude that $\partial^{[r]}(a_n) = 0$. Since this holds for all $\partial \in \mathcal{D}$ and $r \geq 0$, we conclude that $a_n = 0$ by Corollary 4.10.

Case 4: *p divides n and $m = 0$.* Let $\varepsilon_{s+1} = a_n$, which belongs to $\mathbf{k}$ since $m = 0$. Moving the term a_nx^n in (5.7) to the other side and noting that $x^n \in R^p$ as $p \mid n$,

we find

$$\sum_{i=0}^{n-1} a_i x^i \in \sum_{j=1}^{s+1} \varepsilon_j R^p.$$

Applying $\mathscr{B}_{<n,\bullet}$, it follows that $a_i \in \sum_{j=1}^{s+1} \varepsilon_j R^p$ for each $0 \le i \le n$ and $a_i = 0$ for $p \nmid i$. By $\mathscr{A}_E$ we in fact have $a_i \in \sum_{j=1}^{s+1} \varepsilon_j A^p$. Let $b_i \in A$ be such that $a_i \in \varepsilon_{s+1} b_i^p + \sum_{j=1}^{s} \varepsilon_j R^p$. Take $b_i = 0$ for $p \nmid i$ and also put $b_n = 1$. Putting this into (5.7), we find $\varepsilon_{s+1} \sum_{i=0}^{n} b_i^p x^i \in \sum_{j=1}^{s} \varepsilon_j R^p$. The summation on the left is $(\sum_{i=0}^{n} b_{i/p} x^{i/p})^p$, where the sum is over indices divisible by p. This sum is nonzero by $\mathscr{B}_{n/p,\bullet}$ since $b_n = 1$. Thus by Lemma 5.9 and our assumption that $\{\varepsilon_1, \dots, \varepsilon_s\}$ is linearly independent over $\mathbf{k}^p$ we see that $a_n = \varepsilon_{s+1}$ is in the $\mathbf{k}^p$-span of $\varepsilon_1, \dots, \varepsilon_s$, and this establishes $\mathscr{C}'$.

Case 5: *p divides n and $m > 0$.* If $\deg(a_n) = 0$, then the result follows from $\mathscr{B}_{n,<m}$, so assume that $\deg(a_n) > 0$. We claim that for any r, we can find $b \in \sum_{j=1}^{s} \varepsilon_j R^p$ such that $a_n + b$ has level $\ge r$.

To start, apply $\partial^{[0]}$ to (5.7) for some $\partial \in \mathcal{D}$. We find $\partial^{[0]}(a_n) x^n + \cdots = 0$. From $\mathscr{B}_{n,<m}$ it follows that $\partial^{[0]}(a_n) = 0$. Since this holds for all $\partial \in \mathcal{D}$, we conclude that a_n has level ≥ 1. This proves the claim for $r = 1$ (take $b = 0$).

Suppose now that we have found b such that $a_n + b$ has level $\ge r \ge 1$. Applying $\partial^{[r]}$ to (5.7) for some $\partial \in \mathcal{D}$, we find $\partial^{[r]}(a_n) x^n + \cdots \in \sum_{j=1}^{s} \varepsilon_j R^p$. By $\mathscr{B}_{n,<m}$ we have $\partial^{[r]}(a_n) \in \sum_{j=1}^{s} \varepsilon_j R^p$. Of course, we also have $\partial^{[r]}(a_n + b) \in \sum_{j=1}^{s} \varepsilon_j R^p$. As this holds for all ∂ and $a_n + b$ has level $\ge r$, Proposition 4.11 implies that $a_n + b = \sigma^{r+1}(c) + b'$ for some $b' \in \sum_{j=1}^{s} \varepsilon_j R^p$. Thus $a_n + b - b'$ has level $\ge r + 1$. The claim follows.

Take $r \gg m$ and pick $b \in \sum_{j=1}^{s} \varepsilon_j R^p$ so that $a_n + b$ has level $\ge r$. Then $a_n + b = 0$, since the level of a nonzero element of positive degree is bounded in terms of its degree. Thus $a_n \in \sum_{j=1}^{s} \varepsilon_j R^p$, which establishes $\mathscr{C}'$. □

6. Applications

6.1. Inverse Limit Rings

For a (nongraded) ring A and an infinite set $\mathcal{U}$, we put

$$A[\![x_i]\!]_{i \in \mathcal{U}} = \varprojlim A[x_i]_{i \in \mathcal{V}},$$

where the inverse limit is taken in the category of graded rings over all finite subsets $\mathcal{V}$ of $\mathcal{U}$, and $A[x_i]_{i \in \mathcal{V}}$ denotes the standard-graded polynomial ring in the indicated variables. Thus $A[\![x_i]\!]_{i \in \mathcal{U}}$ is a graded ring, and a degree d element can be written uniquely in the form $\sum c_e x^e$, where the sum is over multi-indices e of degree d, and c_e are arbitrary elements of A. (A multi-index is a function $e \colon \mathcal{U} \to \mathbf{N}$ of finite support; its degree is the sum of its values.) Fix a field K and an infinite set $\mathcal{U}$, and let $\mathbf{R} = K[\![x_i]\!]_{i \in \mathcal{U}}$. The following theorem is a slight generalization of Theorem 1.1.

THEOREM 6.1. *The ring* $\mathbf{R}$ *is a polynomial K-algebra.*

Proof. If K has characteristic 0, then this follows from [ESS1, Theorem 5.3] (which also covers some cases in positive characteristic). We note that the statement of [ESS1, Theorem 5.3] takes $\mathcal{U}$ to be countable, but the argument applies generally. Suppose now that K has positive characteristic p. Define the endomorphisms ϕ and σ of $\mathbf{R}$ by

$$\phi\left(\sum c_e x^e\right) = \sum c_e^p x^e, \qquad \sigma\left(\sum c_e x^e\right) = \sum c_e x^{pe}.$$

Then (ϕ, σ) defines an F-factorization on $\mathbf{R}$: the argument in Proposition 2.4 applies with essentially no changes.

Let $\overline{\partial}_i$ be the Hasse derivative with respect to x_i on the polynomial ring $K[x_i]_{i\in\mathcal{U}}$. Let ∂_i^n be the unique continuous extension of $\overline{\partial}_i^n$ to $\mathbf{R}$; concretely,

$$\partial_i^n\left(\sum c_e x^e\right) = \sum c_i \overline{\partial}_i^n(x^e).$$

We easily see that $\{\partial_i^n\}_{n\geq 0}$ is a Hasse derivation ∂_i on $\mathbf{R}$ that is homogeneous of degree -1. Let $\mathcal{D}$ be the set of these Hasse derivations over all i. An argument as in Example 4.3 shows that the set $\mathcal{D}$ is admissible, and the result then follows from Theorem 5.1. □

6.2. *Bounded Inverse Limit Rings*

We now prove a generalization of Theorem 6.1. Let K, $\mathcal{U}$, and $\mathbf{R}$ be as in the previous section. Fix a subring A of K with $\mathrm{Frac}(A) = K$. We say that a subset S of K is **bounded** if there exists a nonzero element $b \in A$ such that $S \subset b^{-1}A$. We let $\mathbf{R}^\flat \subset \mathbf{R}$ be the subring consisting of elements with bounded coefficients (i.e., the set of coefficients forms a bounded subset of K). We note that $\mathbf{R}^\flat$ is naturally identified with $K \otimes_A A[\![x_i]\!]_{i\in\mathcal{U}}$, which is typically *not* isomorphic to $K[\![x_i]\!]_{i\in\mathcal{U}}$. The interest in this ring comes from [ESS1, Section 5], where it plays a key role in our second proof of Stillman's conjecture: it arises when localizing the ring $A[\![x_i]\!]_{i\in\mathcal{U}}$ over the generic point of $\mathrm{Spec}(A)$.

Suppose for the moment that K has characteristic p. For a cardinal κ, we consider the following condition on A:

(C_κ) Given $\varepsilon_1, \dots, \varepsilon_s \in K$ and a subset S of $A \cap \sum_{j=1}^s \varepsilon_j K^p$ of cardinality at most κ, there exists a nonzero element $b \in A$ such that $S \subset b^{-p}\sum_{j=1}^s \varepsilon_j A^p$.

We also consider the following simpler condition:

(C) Given $\varepsilon_1, \dots, \varepsilon_s \in K$, there exists a nonzero element $b \in A$ such that $A \cap \sum_{j=1}^s \varepsilon_j K^p \subset b^{-p}\sum_{j=1}^s \varepsilon_j A^p$.

We note that (C) holds if and only if (C_κ) holds for all κ.

THEOREM 6.2. *Suppose that either K has characteristic 0, or K has characteristic p and condition (C_κ) holds for $\kappa = \#\mathcal{U}$. Then $\mathbf{R}^\flat$ is a polynomial K-algebra.*

If K has characteristic 0, then the result follows from [ESS1, Theorem 5.3]. We assume for the rest of the proof that K has characteristic p. We aim to show

that the F-factorization and admissible set $\mathcal{D}$ on $\mathbf{R}$ constructed in the proof of Theorem 6.1 restrict to such a structure on $\mathbf{R}$. It is clear that ϕ and σ map $\mathbf{R}^\flat$ into itself; we let $\phi^\flat$ and $\sigma^\flat$ denote their restrictions to $\mathbf{R}^\flat$. Similarly, it is clear that each Hasse derivative ∂_i maps $\mathbf{R}^\flat$ into itself; we let $\mathcal{D}^\flat = \{\partial_i|_{\mathbf{R}^\flat}\}_{i\in\mathcal{U}}$.

LEMMA 6.3. *The pair $(\phi^\flat, \sigma^\flat)$ is an F-factorization on $\mathbf{R}^\flat$.*

Proof. It is clear that (F1), (F2), and (F3) hold. We now verify (F4). Thus let $\varepsilon_1, \dots, \varepsilon_s \in K$ be given, and suppose f belongs to $\operatorname{im}(\sigma^\flat) \cap \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi^\flat)$. Write $f = \sum_{j=1}^s \varepsilon_j \phi(g_j)$ for some $g_j \in \mathbf{R}^\flat$. Decompose g_j as $g_j^1 + g_j^2$, where g_j^1 contains all monomials x^e where $p \mid e$, and g_j^2 contains the other monomials. Every monomial occurring in f with nonzero coefficient has the form x^e with $p \mid e$, since $f \in \operatorname{im}(\sigma)$, and so we see that $f = \sum_{j=1}^s \varepsilon_j \phi(g_j^1)$. Since all exponents appearing in g_j^1 are divisible by p, we can write $g_j^1 = \sigma(h_j)$ for some $h_j \in \mathbf{R}$. The set of coefficients appearing in h_j is the same as the set of coefficients appearing in g_j^1 and thus is bounded, and so $h_j \in \mathbf{R}^\flat$. Thus $\phi(g_j^1) = \phi(\sigma(h_j)) \in (\mathbf{R}^\flat)^p$, and the claim follows. □

LEMMA 6.4. *The set $\mathcal{D}^\flat$ is admissible if and only if condition (C_κ) holds, where $\kappa = \#\mathcal{U}$.*

Proof. It is clear that $\mathcal{D}^\flat$ satisfies (D1) and (D2). We show that (D3) holds if and only if (C_κ) holds.

First, suppose that (D3) holds. Let $\varepsilon_1, \dots, \varepsilon_s \in K$, and let S be a subset of $A \cap \sum_{j=1}^s \varepsilon_j K^p$ of cardinality at most κ. Enumerate S as $\{a_i\}_{i\in\mathcal{U}}$; if the cardinality of S is smaller than κ, then simply let the values of a_i repeat. Consider the element $f = \sum_{i\in\mathcal{U}} a_i x_i$ of $\mathbf{R}^\flat$. We have $\partial_i^{[0]}(f) = a_i$, which belongs to $\sum_{j=1}^s \varepsilon_j K^p \subset \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi^\flat)$. Since this holds for all i, we conclude that $f \in \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi^\flat)$ by (D3); we note that the summand $\operatorname{im}(\sigma^\flat)$ in (D3) is irrelevant here since f is linear. Write $f = \sum_{j=1}^s \varepsilon_j \phi(g_j)$ with $g_j \in \mathbf{R}^\flat$. Letting $b \in A$ be a nonzero element such that $bg_j \in A[\![x_i]\!]_{i\in\mathcal{U}}$ for all j, we see that $a_i \in b^{-p} \sum_{j=1}^s \varepsilon_j A^p$ for all j, and so (C_κ) holds.

Conversely, suppose (C_κ) holds. Let $\varepsilon_1, \dots, \varepsilon_s \in K$ and $f \in \mathbf{R}^\flat$ be given, and suppose $\partial^{[0]}(f) \in \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi^\flat)$ for all $\partial \in \mathcal{D}$. We aim to show that f belongs to $\operatorname{im}(\sigma^\flat) + \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi^\flat)$. By scaling f appropriately we may assume f belongs to $A[\![x_i]\!]_{i\in\mathcal{U}}$. Write $f = \sum c_e x^e$ as usual. Since $\mathcal{D}$ satisfies (D3), we can write $f = \sigma(h) + \sum_{j=1}^s \varepsilon_j \phi(g_j)$ for $h, g_1, \dots, g_s \in \mathbf{R}$. We thus see that if $p \nmid e$, then c_e belongs to $A \cap \sum_{j=1}^s \varepsilon_j K^p$. By (C_κ) we thus see that there is some nonzero $b \in A$ such that each such c_e is contained in $b^{-p} \sum_{j=1}^s \varepsilon_j A^p$; we note that the collection of c_e has cardinality at most κ. For $p \nmid e$, write $c_e = \sum_{j=1}^s \varepsilon_j (d_{j,e}/b)^p$, where $d_{j,e} \in A$. Then $f = \sigma(h') + \sum_{j=1}^s \varepsilon_j \varphi(g_j')$, where $h' = \sum_{p\mid e} c_e x^{e/p}$ and $g_j' = b^{-1} \sum_{p\nmid e} d_{j,e} x^e$. Clearly, h' has coefficients in A and thus belongs to $\mathbf{R}^\flat$. It is clear from the definition that g_j' belong to $\mathbf{R}^\flat$. We have thus verified (D3). □

Theorem 6.2 follows from the previous two lemmas: indeed, if (C_κ) holds, then these lemmas show that $\mathbf{R}^\flat$ admits an F-factorization and an admissible set of Hasse derivations and is thus a polynomial ring by Theorem 5.1.

6.3. *More on Condition* (C)

To apply Theorem 6.2, we need some understanding of condition (C). We therefore turn our attention to it in this section. Throughout this section, $\mathbf{k}$ denotes a field of characteristic p, and $\otimes$ denotes the tensor product over $\mathbf{k}$.

PROPOSITION 6.5. *Suppose that A is a Noetherian domain that is finite over A^p. Then A satisfies condition (C).*

Proof. Let $\varepsilon_1, \dots, \varepsilon_s \in K = \mathrm{Frac}(A)$ be given. Let $M = A \cap \sum_{j=1}^s \varepsilon_j K^p$ and $N = \sum_{j=1}^s \varepsilon_j A^p$. Since $K^p N = \sum_{j=1}^s \varepsilon_j K^p$, we have $M \subset K^p N$. On the other hand, M is an A^p-submodule of A and thus is finitely generated as an A^p-module (since A is finite over A^p and $A^p \cong A$ is Noetherian). Let $x_1, \dots, x_n$ be generators for M as an A^p-module, and let $b \in A$ be a nonzero element such that $b^p x_i \in N$ for each $1 \le i \le n$. Then $M \subset b^{-p} N$, as required. □

LEMMA 6.6. *Let $\mathbf{k} \subset K_1$, $K_2 \subset L$ be fields of characteristic p such that K_1 and K_2 are linearly disjoint over $\mathbf{k}$ and L is the compositum of K_1 and K_2. Let $\{\varepsilon_i\}_{i \in I}$ and $\{\delta_j\}_{j \in J}$ be subsets of K_1 and K_2. Then*

$$(K_1 \otimes K_2) \cap \Big(\sum_{i \in I, j \in J} \varepsilon_i \delta_j L^p \Big) = \Big(\sum_{i \in I} \varepsilon_i K_1^p \Big) \otimes \Big(\sum_{j \in J} \delta_j K_2^p \Big),$$

where both sides are regarded as subsets of L.

Proof. Let X denote the left side and Y the right side. Clearly, $Y \subset X$, so we must prove the reverse inclusion. We may as well assume that $\{\varepsilon_i\}_{i \in I}$ is linearly independent over K_1^p; extend it to a basis $\{\varepsilon_i\}_{i \in I_+}$, where $I \subset I_+$. Similarly, let $\{\delta_j\}_{j \in J_+}$ be a basis for K_2 over K_2^p. We claim that $\{\varepsilon_i \delta_j\}_{i \in I_+, j \in J_+}$ is linearly independent over L^p. To see this, suppose that $\sum_{i \in I_+, j \in J_+} c_{i,j} \varepsilon_i \delta_j = 0$ is a linear relation with $c_{i,j} \in L^p$. Since $L = \mathrm{Frac}(K_1 \otimes K_2)$, we can clear denominators and assume that $c_{i,j} \in K_1^p \otimes K_2^p$. But $K_1 \otimes K_2$ is a free module over $K_1^p \otimes K_2^p$ with basis $\{\varepsilon_i \delta_j\}_{i \in I_+, j \in J_+}$, and so $c_{i,j} = 0$ for all i and j.

Now let $x \in X$ be given. Since x belongs to $K_1 \otimes K_2$, we can express it as $x = \sum_{i \in I_+, j \in J_+} c_{i,j} \varepsilon_i \delta_j$ with $c_{i,j} \in K_1^p \otimes K_2^p$. On the other hand, since x belongs to $\sum_{i \in I, j \in J} \varepsilon_i \delta_j L^p$, we can express it as $x = \sum_{i \in I, j \in J} c'_{i,j} \varepsilon_i \delta_j$ with $c'_{i,j} \in L^p$. By the previous paragraph we must have $c'_{i,j} = c_{i,j} \in K_1^p \otimes K_2^p$, which shows that x belongs to Y. □

LEMMA 6.7. *Let $\mathbf{k}$ be a field of characteristic p, and let B_1 and B_2 be integral domains containing $\mathbf{k}$ such that $C = B_1 \otimes_{\mathbf{k}} B_2$ is a domain. Let $K_i = \mathrm{Frac}(B_i)$*

and $L = \mathrm{Frac}(C)$. *Let* $\varepsilon_1, \ldots, \varepsilon_s \in K_1$. *Then*

$$C \cap \left(\sum_{j=1}^{s} \varepsilon_j L^p \right) = \left(B_1 \cap \sum_{j=1}^{s} \varepsilon_j K_1^p \right) \otimes (B_2 \cap K_2^p),$$

where each side is regarded as a subset of C.

Proof. Applying the previous lemma with $\{\delta_j\}_{j \in J}$ the singleton set $\{1\}$, we find

$$(K_1 \otimes K_2) \cap \sum_{j=1}^{s} \varepsilon_j L^p = \left(\sum_{j=1}^{s} \varepsilon_j K_1^p \right) \otimes K_2^p.$$

Now intersect each side with C. Note that C is contained in $K_1 \otimes K_2$, so the left side is just $C \cap \sum_{j=1}^{s} \varepsilon_j L^p$. Since $C = B_1 \otimes B_2$, the right side factors as required. □

Recall that if $\{A_i\}_{i \in \mathcal{I}}$ is a family of $\mathbf{k}$-algebras, then $\bigotimes_{i \in \mathcal{I}} A_i$ is defined as the direct limit of the algebras $\bigotimes_{i \in \mathcal{J}} A_i$ taken over all finite subsets $\mathcal{J}$ of $\mathcal{I}$.

Proposition 6.8. *Let* $\mathbf{k}$ *be a field of characteristic* p, *let* $\{A_i\}_{i \in \mathcal{I}}$ *be a family of* $\mathbf{k}$*-algebras, and let* $A = \bigotimes_{i \in \mathcal{I}} A_i$, *which we assume to be a domain. Assume*:

(a) *For each finite subset* $\mathcal{J}$ *of* $\mathcal{I}$, *the ring* $A_{\mathcal{J}} = \bigotimes_{i \in \mathcal{J}} A_i$ *satisfies condition* (C).
(b) *For each* i, *we have* $A_i \cap \mathrm{Frac}(A_i)^p = A_i^p$.

Then A *satisfies condition* (C).

Proof. Let $K = \mathrm{Frac}(A)$, $K_i = \mathrm{Frac}(A_i)$, and $K_{\mathcal{J}} = \mathrm{Frac}(A_{\mathcal{J}})$. Note that A_i and $A_{\mathcal{J}}$ are subrings of A and thus domains. Now, let $\varepsilon_1, \ldots, \varepsilon_s \in K$ be given. Let $\mathcal{J}_0 \subset \mathcal{I}$ be a sufficiently large finite set such that $\varepsilon_1, \ldots, \varepsilon_s$ belong to $K_{\mathcal{J}_0}$. Since $A_{\mathcal{J}_0}$ satisfies condition (C) by assumption (a), there exists a nonzero element $b \in A_{\mathcal{J}_0}$ such that

$$A_{\mathcal{J}_0} \cap \sum_{j=1}^{s} \varepsilon_j K_{\mathcal{J}_0}^p \subset b^{-p} \sum_{j=1}^{s} \varepsilon_j A_{\mathcal{J}_0}^p.$$

We claim that

$$A \cap \sum_{j=1}^{s} \varepsilon_j K^p \subset b^{-p} \sum_{j=1}^{s} \varepsilon_j A^p,$$

which will verify condition (C) for A. To see this, it suffices to prove that

$$A_{\mathcal{J}} \cap \sum_{j=1}^{s} \varepsilon_j K_{\mathcal{J}}^p \subset b^{-p} \sum_{j=1}^{s} \varepsilon_j A_{\mathcal{J}}^p$$

for all finite subsets $\mathcal{J}$ of $\mathcal{I}$ containing $\mathcal{J}_0$. Let $I(\mathcal{J})$ be the true value of this containment. We prove $I(\mathcal{J})$ by induction on $\mathcal{J}$, the base case being $\mathcal{J} = \mathcal{J}_0$.

Thus suppose that $I(\mathcal{J})$ holds, and let us prove $I(\mathcal{J}')$ where $\mathcal{J}' = \mathcal{J} \cup \{i\}$ for some $i \in \mathcal{I} \setminus \mathcal{J}$. As $A_{\mathcal{J}'} = A_{\mathcal{J}} \otimes A_i$, the previous lemma yields

$$A_{\mathcal{J}'} \cap \left(\sum_{j=1}^{s} \varepsilon_j K_{\mathcal{J}'}^p \right) = \left(A_{\mathcal{J}} \cap \sum_{j=1}^{s} \varepsilon_j K_{\mathcal{J}}^p \right) \otimes (A_i \cap K_i^p).$$

The first factor on the right is contained in $b^{-p} \sum_{j=1}^{s} \varepsilon_j A_{\mathcal{J}}^p$ by $I(\mathcal{J})$, whereas the second factor on the right is A_i^p by assumption (b); thus the right side is contained in $b^{-p} \sum_{j=1}^{s} \varepsilon_j A_{\mathcal{J}'}^p$, and so $I(\mathcal{J}')$ holds. □

COROLLARY 6.9. *Let* $\mathbf{k}$ *be a semiperfect field, let* $\{A_i\}_{i \in \mathcal{I}}$ *be a family of normal finitely generated* $\mathbf{k}$*-algebras, and let* $A = \bigotimes_{i \in \mathcal{I}} A_i$*, which we assume to be a domain. Then* A *satisfies condition* (C).

Proof. We apply Proposition 6.8. Since $A_{\mathcal{J}}$ is finitely generated over a semiperfect field, it satisfies (C) by Proposition 6.5, and so condition (a) holds. Since each A_i is normal, condition (b) holds. □

COROLLARY 6.10. *Any polynomial ring over a semiperfect field satisfies condition* (C).

Proof. Suppose $A = \mathbf{k}[x_i]_{i \in \mathcal{I}}$ is a polynomial ring. Then $A = \bigotimes_{i \in \mathcal{I}} A_i$, where A_i is the univariate polynomial ring $\mathbf{k}[x_i]$. The result now follows from Corollary 6.9. □

COROLLARY 6.11. *Let* A *be a polynomial ring over a semiperfect field, let* $K = \operatorname{Frac}(A)$*, and let* $\mathcal{U}$ *be an infinite set. Then* $\mathbf{R}^\flat = K \otimes_A A[\![x_i]\!]_{i \in \mathcal{U}}$ *is a polynomial* K*-algebra.*

Proof. This follows from Corollary 6.10 and Theorem 6.2. □

Having given some examples where (C) holds, we now give an example where it does not.

EXAMPLE 6.12. Let $A = \mathbf{F}_p[t_i^2, t_i^3]_{i \geq 1}$, a subring of the polynomial ring $\mathbf{F}_p[t_i]_{i \geq 1}$. We claim that A does not satisfy condition (C). Take $s = 1$ and $\varepsilon_1 = 1$, and let $S \subset A \cap K^p$ be the set $S = \{t_i^p\}_{i \geq 1}$. We note that $K = \operatorname{Frac}(A)$ is the rational function field $\mathbf{F}_p(t_i)_{i \geq 1}$, so t_i^p does indeed belong to K^p. We claim that S is not contained in $b^{-p} A^p$ for any nonzero $b \in A$. Indeed, b can only use finitely many variables, say $t_1, \dots, t_n$, and then $b^{-p} A^p$ cannot contain t_{n+1}^p, as $b^{-1} A$ does not contain t_{n+1}. We do not know if $\mathbf{R}^\flat$ is a polynomial ring in this case: this is an interesting open problem.

REMARK 6.13. Broadly speaking, the main difficulty with the derivational criteria like Theorem 5.1 or those in [ESS1, Section 2] lies in dealing with elements that look like pth powers but actually are not. For example, if $K = \mathbf{F}_p(t_i)_{i \geq 1}$, then the element $f = \sum_{i \geq 1} t_i x_i^p$ of $K[\![x_1, x_2, \dots]\!]$ looks like a pth power in the sense that

it is annihilated by all continuous derivations, even though it is not. The criterion in [ESS1] is not powerful enough to handle such elements and thus cannot establish the polynomiality of $K[\![x_1, x_2, \ldots]\!]$. Our Theorem 5.1 can handle this kind of element and does prove that $K[\![x_1, x_2, \ldots]\!]$ is polynomial. However, Theorem 5.1 cannot handle certain more subtle elements. For example, if $A = \mathbf{F}_p[t_i^2, t_i^3]_{i\geq 1}$ is the ring from the previous example and $g \in \mathbf{R}^\flat$ is the element $g = \sum_{i\geq 1} t_i^p x_i^p$, then g *really* looks like a pth power—for example, it is a limit of pth powers and is a pth power in the overring $\mathbf{R}$—even though g actually is not a pth power in $\mathbf{R}^\flat$. Our Theorem 5.1 is not powerful enough to handle this kind of element and thus cannot determine whether or not $\mathbf{R}^\flat$ is a polynomial ring.

6.4. *A Curious Example*

We now give an example of a ring A for which (C_κ) holds for $\kappa = \aleph_0$ but fails for $\kappa = \aleph_1$. Thus the ring $\mathbf{R}^\flat$ is polynomial if $\mathcal{U}$ is countable, but our methods cannot determine whether or not it is so for uncountable $\mathcal{U}$.

Fix a well-ordered set I of type ω_1. Thus I is uncountable (of cardinality $\aleph_1$), but for any $i \in I$, the set $\{j \in I \mid j < i\}$ is countable. In particular, any countable subset of I is bounded from above (if not, I would be a countable union of countably many subsets). Let Γ be the group of all functions $I \to \mathbf{Z}$ with finite support. We totally order Γ using the lexicographic order, that is, $\gamma < \gamma'$ if $\gamma(i) < \gamma'(i)$, where i is maximal such that $\gamma(i) \neq \gamma'(i)$. Given a nonzero element $\gamma \in \Gamma$, the **top index** of γ is the maximal i for which $\gamma(i) \neq 0$, and the **top value** of γ is $\gamma(i)$, where i is the top index. We let Γ_+ (resp. Δ) be the submonoid of Γ consisting of 0 and all nonzero elements $\gamma \in \Gamma$ with top value at least 1 (resp., at least 2). We note that Γ_+ can also be described as the set of $\gamma \in \Gamma$ with $\gamma \geq 0$.

Let $L = \mathbf{F}_p((\Gamma))$ be the ring of Laurent series with coefficients in $\mathbf{F}_p$ and exponents in Γ. By definition an element of L is a formal series $\sum_{\gamma\in\Gamma} c_\gamma t^\gamma$, where t^γ are formal symbols, c_γ belong to $\mathbf{F}_p$, and the set $\{\gamma \in \Gamma \mid c_\gamma \neq 0\}$ is well ordered (under the order on Γ). Multiplication in L is performed in the usual manner; the condition on the support of the coefficients ensures that it is well defined. For a nonzero element $f = \sum c_\gamma t^\gamma$ of L, we let $v(f)$ be the minimal γ for which c_γ is nonzero. It is well known that L is a field and v is a valuation on L with value group Γ. In fact, this is the standard construction of a valuation field with value group Γ. The valuation ring $\mathcal{O}_L$ consists of those elements of L that have the form $\sum_{\gamma\in\Gamma_+} c_\gamma t^\gamma$. See [FS, Section II.3] for further background on these constructions.

Let $A \subset \mathcal{O}_L$ be the set of elements of the form $\sum_{\gamma\in\Delta} c_\gamma t^\gamma$. Since Δ is a submonoid of Γ, it follows that A is a subring of L. Let K be the fraction field of A. We note that the valuation of any nonzero element of A belongs to Δ.

LEMMA 6.14. *Given $f \in K$, there exists $i \in I$ such that $t^\delta f \in A$ for any $\delta \in \Delta$ with top index $> i$.*

Proof. It suffices to prove the result for $f = g^{-1}$ with nonzero $g \in A$. Let $\gamma = v(g)$; we may as well scale g so that t^γ has coefficient 1. Let i be the top index

of γ. Write $g = t^\gamma + g_1 + g_2$, where g_1 consists of all terms in g with top index i (other than the leading term), and g_2 consists of terms with top index $> i$. Then

$$g^{-1} = t^{-\gamma}(1 + t^{-\gamma}g_1 + t^{-\gamma}g_2)^{-1} = t^{-\gamma}\sum_{n,m\geq 0}\binom{n+m}{n}(t^{-\gamma}g_1)^n(t^{-\gamma}g_2)^m.$$

The terms in $t^{-\gamma}g_2$ have the same top values as the terms in g_2; in particular, they are all at least 2, and so $t^{-\gamma}g_2$ belongs to A. The terms in $t^{-\gamma}g_1$ have top index at most i, and so the same is true for terms in $t^{-\gamma}(t^{-\gamma}g_1)^n$ for any n. Thus if $\delta \in \Delta$ has top index $> i$, then all terms in $t^\delta \cdot t^{-\gamma}(t^{-\gamma}g_1)^n$ have the same top index and top value as δ, and so this element belongs to A. Thus $t^\delta g^{-1}$ belongs to A. □

LEMMA 6.15. *A satisfies (C_κ) with $\kappa = \aleph_0$.*

Proof. Let $\varepsilon_1, \dots, \varepsilon_s \in K$ be given, and let $S = \{f_n\}_{n\geq 1}$ be a countable subset of $A \cap \sum_{j=1}^s \varepsilon_j K^p$. By Lemma 6.14, for each $n \geq 1$, we can choose some $i_n \in I$ such that $t^{p\delta} f_n \in \sum_{j=1}^s \varepsilon_j A^p$ for any $\delta \in \Delta$ with top index $> i_n$. Since $\{i_n\}_{n\geq 1}$ is a countable subset of I, it is bounded from above; let $i^* \in I$ be an element such that $i_n < i^*$ for all n. Then if $\delta \in \Delta$ has top index i^*, then we have $t^{p\delta} f_n \in \sum_{j=1}^s \varepsilon_j A^p$ for all n, and so $S \subset b^{-p}\sum_{j=1}^s \varepsilon_j A^p$ with $b = t^\delta \in A$. Thus (C_κ) holds. □

LEMMA 6.16. *A does not satisfy (C_κ) with $\kappa = \aleph_1$.*

Proof. For $i \in I$, let $\delta_i \in \Gamma_+$ be the element that is 1 at i and 0 elsewhere. Then $t^{p\delta_i}$ belongs to $A \cap K^p$ for all i: indeed, $n\delta_i$ belongs to Δ for any $n \geq 2$, and so $t^{p\delta_i}$ belongs to A, whereas $t^{\delta_i} = t^{3\delta_i}/t^{2\delta_i}$ belongs to K, and so $t^{p\delta_i}$ belongs to K^p. Let $S = \{t^{p\delta_i}\}_{i\in I}$; this is a subset of $A \cap K^p$ of cardinality κ. To prove the lemma, it suffices to show that S is not contained in $b^{-p}A^p$ for any nonzero $b \in A$. Thus suppose a nonzero $b \in A$ is given. Let $\gamma = v(b)$, let i be the top index of γ, and let $j > i$. We claim that $t^{p\delta_j}$ does not belong to $b^{-p}A^p$, which will complete the proof. Indeed, suppose that it did, and write $b^p t^{p\delta_j} = a^p$ for some $a \in A$. Taking valuations, we find $\gamma + \delta_j = v(a) \in \Delta$. However, $\gamma + \delta_j$ has top value 1, a contradiction. □

6.5. *Ultraproducts*

We now treat an ultraproduct version of Theorem 1.1. We refer to [ESS1, Section 4] for the relevant background. Let $\mathcal{I}$ be a set equipped with a nonprincipal ultrafilter. We regard elements of the ultrafilter as neighborhoods of some hypothetical point $*$. Let $\{\mathbf{k}_i\}_{i\in\mathcal{I}}$ be a family of fields, let $R_i = \mathbf{k}_i[x_1, x_2, \dots]$ with the standard grading, and let $\mathbf{S}$ be the graded ultraproduct of the R_i.

THEOREM 6.17. *$\mathbf{S}$ is a polynomial ring.*

Proof. If the ultraproduct of the fields $\mathbf{k}_i$ has characteristic 0, then this follows from [ESS1, Theorem 4.7] (which also covers some cases in positive characteristic). Thus assume that this ultraproduct has positive characteristic p. Passing to

a neighborhood of $*$, we can thus assume that each $\mathbf{k}_i$ has characteristic p. Each R_i then comes with a standard F-factorization and an admissible set of Hasse derivations (the Hasse derivatives with respect to the variables). We claim that the ultraproduct of these structures endow $\mathbf{S}$ with an F-factorization and an admissible set $\mathcal{D}$.

First, we start with the F-factorization. Properties (F1), (F2), (F3) are clearly preserved under taking ultraproduct, so we need to check (F4). Pick $\varepsilon_1, \dots, \varepsilon_s \in \mathbf{S}_0$. Suppose we have $f \in \operatorname{im}(\sigma) \cap \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi)$. In particular, we can write $f = \sigma(x)$ and $f = \sum_{j=1}^s \varepsilon_j \phi(y_j)$ for some elements $x, y_1, \dots, y_s \in \mathbf{S}$. Each of f, x, y_j can be represented by a sequence of elements in R_i, say $f = (f_i)$, $x = (x_i)$, and $y = (y_{j,i})$, and the same equalities will hold in some neighborhood of $*$. Similarly, we can write $\varepsilon_j = (\varepsilon_{j,i})$. In particular, we can write $f_i = \sum_{j=1}^s \varepsilon_{j,i} z_{j,i}^p$ with $z_{j,i} \in R_i$. Then we have $f = \sum_{j=1}^s \varepsilon_j z_j$, where z_j is the ultraproduct of the elements $z_{j,i}$, and this shows that $\operatorname{im}(\sigma) \cap \sum_{j=1}^s \varepsilon_j \operatorname{im}(\phi) \subseteq \sum_{j=1}^s \varepsilon_j \mathbf{S}^p$. As in Remark 2.3, the other inclusion follows from the other axioms (or could be proven in a similar way). The proof that the ultraproduct of admissible sets of derivations is still admissible is similar, so we omit it.

The result now follows from Theorem 5.1. □

6.6. *Small Subalgebras*

We now explain the application of Theorem 6.17 to small subalgebras. We begin with some definitions.

DEFINITION 6.18. Let $\mathbf{k}$ be a field. We say that **small subalgebras exist** for $\mathbf{k}$ if for all integers r and d, there exists an integer $s = s(r, d, \mathbf{k})$ with the following property: given homogeneous polynomials $f_1, \dots, f_r$ of degrees $\le d$ in the polynomial ring $\mathbf{k}[x_1, \dots, x_n]$, with $n \ge s$, there exists a regular sequence $g_1, \dots, g_s$ in $\mathbf{k}[x_1, \dots, x_n]$ consisting of homogeneous elements such that $f_1, \dots, f_r \in \mathbf{k}[g_1, \dots, g_s]$.

DEFINITION 6.19. Let $\mathscr{K}$ be a class of fields. We say that **small subalgebras exist uniformly** for $\mathscr{K}$ if small subalgebras exist for all $\mathbf{k} \in \mathscr{K}$ and the quantity $s(r, d, \mathbf{k})$ can be taken to be independent of $\mathbf{k}$ for $\mathbf{k} \in \mathscr{K}$.

Ananyan and Hochster [AH, Theorem A] proved that small subalgebras exist uniformly for algebraically closed fields. In [ESS1], we proved the following:

THEOREM 6.20. *Let $\mathscr{K}$ be a class of fields. Suppose that for every countable sequence $\{\mathbf{k}_i\}_{i \in \mathcal{I}}$ of $\mathscr{K}$, the ultraproduct ring $\mathbf{S}$ (as defined in the previous section) is polynomial. Then small subalgebras exist uniformly for $\mathscr{K}$.*

Proof. The argument is exactly the same as in [ESS1, Section 4.3]: simply replace "perfect field" with "field in $\mathscr{K}$" everywhere. □

We used Theorem 6.20 and our polynomiality results to prove that small subalgebras exist uniformly for perfect fields. The results of [ESS1] can also prove the

existence of small subalgebras for semiperfect fields but not uniformity for this class. Using the superior polynomiality result of this paper (Theorem 6.17), we obtain the following improvement.

THEOREM 6.21. *Small subalgebras exist uniformly for all fields.*

References

[AH] T. Ananyan and M. Hochster, *Small subalgebras of polynomial rings and Stillman's conjecture,* J. Amer. Math. Soc. 33 (2020), 291–309, arXiv:1610.09268v3.

[BDE] A. Bik, J. Draisma, and R. H. Eggermont, *Polynomials and tensors of bounded strength,* Commun. Contemp. Math. 21 (2019), no. 7, 1850062, arXiv:1805.01816v2.

[Dr] J. Draisma, *Topological noetherianity for polynomial functors,* J. Amer. Math. Soc. 32 (2019), no. 3, 691–707, arXiv:1705.01419v4.

[DLL] J. Draisma, M. Lason, and A. Leykin, *Stillman's conjecture via generic initial ideals,* Comm. Algebra 47 (2019), 2384–2395, arXiv:1802.10139v2.

[ESS1] D. Erman, S. V. Sam, and A. Snowden, *Big polynomial rings and Stillman's conjecture,* Invent. Math. 218 (2019), no. 2, 413–439, arXiv:1801.09852v4.

[ESS2] ———, *Strength and Hartshorne's conjecture in high degree,* Math. Z. (to appear), arXiv:1804.09730v1.

[FS] L. Fuchs and L. Salce, *Modules over non-Noetherian domains,* Math. Surveys Monogr., 84, American Mathematical Society, Providence, RI, 2001.

D. Erman
Department of Mathematics
University of Wisconsin
Madison, WI 53706
USA

derman@math.wisc.edu
http://math.wisc.edu/~derman/

S. V. Sam
Department of Mathematics
University of Wisconsin
Madison, WI 53706
USA

Current address
Department of Mathematics
University of California, San Diego
La Jolla, CA 92093
USA

ssam@ucsd.edu
http://math.ucsd.edu/~ssam/

A. Snowden
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
USA

asnowden@umich.edu
http://www-personal.umich.edu/~asnowden/