Canad. J. Math. Vol. **67** (2), 2015 pp. 286–314
http://dx.doi.org/10.4153/CJM-2013-048-3

A Skolem–Mahler–Lech Theorem for Iterated Automorphisms of K-algebras

Jason P. Bell and Jeffrey C. Lagarias

Abstract. In this paper we prove a commutative algebraic extension of a generalized Skolem–Mahler–Lech theorem. Let A be a finitely generated commutative K-algebra over a field of characteristic 0, and let σ be a K-algebra automorphism of A. Given ideals I and J of A, we show that the set S of integers m such that $\sigma^m(I) \supseteq J$ is a finite union of complete doubly infinite arithmetic progressions in m, up to the addition of a finite set. Alternatively, this result states that for an affine scheme X of finite type over K, an automorphism $\sigma \in \mathrm{Aut}_K(X)$, and Y and Z any two closed subschemes of X, the set of integers m with $\sigma^m(Z) \subseteq Y$ is as above. We present examples showing that this result may fail to hold if the affine scheme X is not of finite type, or if X is of finite type but the field K has positive characteristic.

1 Introduction

The Skolem–Mahler–Lech theorem is a fundamental result that characterizes the structure of the set of zeros of a linear recurrence. We term the resulting structure the SML property. The paper is motivated by the question: "What is the maximal level of generality for which the conclusion of the Skolem–Mahler–Lech theorem holds?" We view this question in the general framework of orbits of dynamical systems of algebraic type.

In 2006 the first author ([4, 5]) gave an algebro-geometric generalization of the Skolem–Mahler–Lech theorem that applied to orbits of an automorphism of an affine variety acting on geometric points. The object of this paper is to show there is a further algebro-geometric generalization of the Skolem–Mahler–Lech theorem that applies to automorphisms of the coordinate ring of the variety acting at the level of ideals. The new result can be interpreted as a result about automorphisms of affine schemes. To state it, we first review the successive generalizations of the Skolem–Mahler–Lech theorem.

1.1 The Skolem–Mahler–Lech Theorem

The Skolem–Mahler–Lech theorem (SML Theorem) is a fundamental result that can be stated in several apparently different forms. The original formulation of the SML

Received by the editors October 8, 2013; revised December 2, 2013.
Published electronically February 10, 2014.
The research of the first-named author was supported by NSERC grant 611456. The research of the second author was supported by NSF grants DMS-0801029 and DMS-1101373.
AMS subject classification: **11D45**, 14R10, 11Y55, 11D88.
Keywords: automorphisms, endomorphisms, affine space, commutative algebras, Skolem–Mahler–Lech theorem.

Theorem concerned the zeros of power series coefficients of rational functions.

Theorem 1.1 (SML Theorem: rational function form) *Let K be a field of characteristic zero, and let $G(x) \in K(x)$ be a rational function that is finite at $x = 0$. If the Taylor expansion $G(x) \in K[[x]]$ at $x = 0$ is given as*

$$G(x) = \sum_{k=0}^{\infty} a_k x^k,$$

then the set of its zero coefficients $S := \{k \in \mathbb{N} : a_k = 0\}$ is a union of a finite number of arithmetic progressions $\{an + b : n \geq 0\}$ with $a, b > 0$, together with a (possibly empty) finite set.

This result was established by Skolem [28] in 1934 for the case of rational coefficients using a p-adic method he introduced in [27]. It was extended by Mahler [21, Sect. 6] in 1935 to series with coefficients in algebraic number fields, and much later in 1956 ([22]) to coefficients in the complex field $\mathbb{C}$. In this last extension Mahler was unaware of the 1953 work of Lech [20] discussed below; see [23].

There are now many different proofs and extensions of the SML Theorem in the literature [8, 18, 31, 32], some described in the book of Everest et al. [14, Chap. 2.1]. The result is valid in any field of characteristic zero; however, all known proofs use p-adic methods.

The property of the set S formulated in the conclusion of all versions of the SML Theorem can be stated as follows.

Definition 1.2 A set of natural numbers $S \subset \mathbb{N}$ has the (one-sided) *SML property* if it is a finite union of one-sided arithmetic progressions $\{an + b : n \geq 0\}$ with $a, b > 0$ (possibly empty), augmented by a finite set, possibly empty. (We allow the possibility $b > a$ in the one-sided arithmetic progressions, *i.e.,* some initial terms of the complete progression in $\mathbb{N}$ can be omitted.)

A second form of the SML Theorem concerns zeros of linear recurrence sequences. This version was first formulated by Lech [20] in 1953.

Theorem 1.3 (SML Theorem: recurrence form) *Let K be a field of characteristic zero and let $f\colon \mathbb{N} \to K$ be a K-valued sequence that satisfies a linear recurrence*

$$f(n) = a_1 f(n-1) + a_2 f(n-2) + \cdots + a_r f(n-r), \quad a_i \in K,$$

for all $n \geq r$. Then the set $S := \{n \geq 0 : f(n) = 0\}$ of zeros of the recurrence has the SML property.

We can view the recurrence version of the SML Theorem as asserting a property of a forward orbit of a discrete dynamical system given by the linear recurrence. Note that the set S can also be interpreted as the intersection of the forward orbits of two different dynamical systems, the first being the recurrence $f(n)$ and the second being the constant linear recurrence $g(n) = 0$.

The recurrence form of the SML Theorem can be recast in a third equivalent form, which concerns iteration of linear maps, and encodes containment relations in a subspace of orbits of invertible linear maps under iteration ([4, Theorem 1.2 and Section 2]).

Theorem 1.4 (SML Theorem: linear map form) *Let K be a field of characteristic 0, and let $\sigma\colon K^n \to K^n$ be an invertible linear map. If $\mathbf{v} \in K^n$ and W is a vector subspace of K^n of codimension 1, then the set $S := \{n \in \mathbb{N} : \sigma^n(\mathbf{v}) \in W\}$ has the SML property.*

In 2006 the first author [4, 5] found a generalization of the SML Theorem to algebraic dynamics, which applies at the geometric level to iteration of automorphisms on affine algebraic varieties. It concerns two-sided infinite sequences of iterates, and to state it we extend the notion of SML property to this case.

Definition 1.5 A set of integers $S \subset \mathbb{Z}$ is said to have the *two-sided SML property* if it is a finite union of complete arithmetic progressions $\{an + b : n \in \mathbb{Z}\}$ on $\mathbb{Z}$ augmented by a finite set. (That is, we allow arithmetic progressions with $a = 0$, which give one element sets.)

The generalization of the SML Theorem to automorphisms on affine varieties is as follows.

Theorem 1.6 (Generalized SML Theorem for affine varieties) *Let K be a field of characteristic zero, and let X be an affine K-variety and let σ be an automorphism of X. If x is a K-point of X and Y is a subvariety of X (Zariski closed subset of X), then the set*

$$S := \{n \in \mathbb{Z} : \sigma^n(x) \in Y\}$$

has the two-sided SML property.

Despite its restriction to two-sided infinite sequences, Theorem 1.6 recovers the original (one-sided) recurrence form of the SML Theorem above via its implication of the linear map form (Theorem 1.4). The proof of Theorem 1.6 in [4, 5] again relies on a p-adic result, the *p-adic analytic arc theorem*, first established in [4, 5] and strengthened in [6]. This latter result was recently further strengthened by Poonen [25].

We also note that since the conclusion of Theorem 1.6 is purely set-theoretic and is preserved under extension of scalars, the result for a general characteristic 0 field K follows easily from the special case where K is an algebraically closed field of characteristic zero.

Subsequent work of the first author with Ghioca and Tucker [6, Theorem 1.3], established an analogous theorem for forward orbits of étale endomorphisms of quasiprojective varieties defined over $\mathbb{C}$. We also point out that Denis [11] had earlier proved a special case of this result for étale self maps of $\mathbb{P}^n_{\mathbb{C}}$. Recently Sierra [26, Conjecture 5.15] suggested a possible extension of these results that would have interesting consequences for the algebras studied in noncommutative projective geometry.

1.2 Main Result

Our starting point is the observation that Theorem 1.6 can be recast in purely algebraic terms. To do this, suppose that K is an algebraically closed field of characteristic zero. In classical affine algebraic geometry, we then have a contravariant equivalence of categories

$$\{\text{Affine } K\text{-Varieties}\} \longleftrightarrow \{\text{Reduced finitely generated } K\text{-algebras}\}$$

induced by the functor that takes an affine variety X to its coordinate ring $K[X]$ and takes a morphism $\phi\colon X \to Y$ of affine varieties to the homomorphism $\phi^*\colon K[Y] \to K[X]$ of K-algebras given by $\phi^*(f) = f \circ \phi$ ([19, Corollaries 1.4 and 3.8]). The Nullstellensatz gives further information, showing that there is an inclusion reversing bijection between the subvarieties of an affine variety X and the radical ideals of its coordinate ring $K[X]$. In particular, for a morphism $\phi\colon X \to X$ the inclusion $\phi(V(I)) \subseteq V(J)$ of zero sets of radical ideals I, J corresponds to the reversed algebraic inclusion $\phi^\star(I) \supseteq J$. It follows that Theorem 1.6 restricted to algebraically closed fields K can be recast in algebraic terms as follows:

If A is a finitely generated, reduced, commutative K-algebra with a K-algebra automorphism σ and M and J are ideals of A with M a maximal ideal and J a radical ideal, then the set of integers n for which $\sigma^n(M) \supseteq J$ has the two-sided SML property.

From this algebraic perspective, it is natural to ask whether a similar result holds for more general ideal inclusions in finitely generated commutative K-algebras. Our main result gives an affirmative answer to this question.

Theorem 1.7 (Generalized SML Theorem for ideal inclusions) *Let K be any field of characteristic zero and let A be a finitely generated commutative K-algebra. If $\sigma\colon A \to A$ is a K-algebra automorphism and I and J are ideals of A, then*

$$S = S(I, J) := \{n \in \mathbb{Z} : \sigma^n(I) \supset J\}$$

has the two-sided SML property. Here, $\sigma(I) := \{\sigma(a) : a \in I\}$.

The two-sided SML property of this result also holds for the set of integers n for which $\sigma^n(J) \subseteq I$, because this condition holds if and only if $\sigma^{-n}(I) \supseteq J$, where $\sigma^{-1}(I) = \{b : \sigma(b) \in I\}$; apply Theorem 1.7 to the automorphism σ^{-1}.

Theorem 1.7 implies Theorem 1.6 and hence all the earlier forms of the SML Theorem stated above. In the special case where I is a maximal ideal, Theorem 1.7 is itself deducible from the algebraic form of Theorem 1.6. The main content of Theorem 1.7, and also the source of the difficulty in proving it, revolves around relaxing the maximality condition on I. For example, if $A = \mathbb{C}[x, y]$, then a polynomial $p(x, y) \in A$ is in the maximal ideal (x, y) if and only if $p(0, 0) = 0$. On the other hand, $p(x, y)$ is in the ideal (x, y^2) if and only if $p(0, 0) = 0$ and $\partial p(x, y)/\partial y$ vanishes at $(0, 0)$. In this sense, the ideal $I = (x, y^2)$ encodes additional "infinitesimal" information. It seems easier to understand the behavior of the iterates of an element $p(x, y)$ of A under an automorphism σ with respect to evaluation at a given point than to understand how the iterates behave with respect to more complicated conditions involving the vanishing of partial derivatives at a point. This difficulty, and more generally the possible occurrence of nil ideals and non-radical ideals in A, adds an extra level of complication to the problem (see Examples 6.2 and 6.3).

In Section 6 we give examples showing that this result is strictly more general than Theorem 1.6. In particular, there exist two ideals I_1, I_2 having the same radical ideal $I = \sqrt{I_1} = \sqrt{I_2}$ and J such that the sets $S(I_1, J) \neq S(I_2, J)$; see Example 6.1.

As with previous work, our method to prove Theorem 1.7 makes use of a p-adic result. We present a p-adic interpolation result that strengthens the p-adic analytic arc theorem established in [5], which we call the *generalized p-adic analytic arc theorem* (Theorem 3.1). This result concerns polynomial automorphisms

$$\sigma \colon \mathbb{Z}_p[x_1, \dots, x_d] \to \mathbb{Z}_p[x_1, \dots, x_d]$$

and applies for $p \geq 5$. It asserts that for a $\mathbb{Z}_p$-algebra S that is finitely generated and is a torsion-free $\mathbb{Z}_p$-module, the induced (nonlinear) map $f_\sigma \colon S^d \to S^d$ has the property that iterates of a suitable initial point $\mathbf{s} = (s_1, \dots, s_d) \in S^d$ under σ can be embedded in a p-adic analytic arc. Note that S is a free $\mathbb{Z}_p$-module of finite rank $r > 0$, and one might think that this extension can be obtained by fixing a $\mathbb{Z}_p$-module isomorphism between S and $(\mathbb{Z}_p)^r$ and then applying the analytic arc theorem of [4] separately to each coordinate. This is not the case, however, as application of the map σ involves expressions that include combinations of elements from different coordinates. Our innovation to get around this obstacle consists of working with a larger ring of functions than usual, namely, the subset $\mathcal{R}(S)$ of $S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p[z]$ that consists of all polynomials which map $\mathbb{Z}_p$ into S, and obtaining analytic maps via successive approximations via functions in this ring. The commutative ring $\mathcal{R}(S)$ is rather pathological; it is not Noetherian and is not of finite type over $\mathbb{Z}_p$. Our proof requires establishing a nice property of certain subalgebras of $\mathcal{R}(S)$, given in Lemma 3.7. As in the case of the p-adic analytic arc theorem treated in [4], the generalized p-adic analytic arc theorem fails to hold for $p = 2$. Its truth for $p = 3$ remains open.

The proof of Theorem 1.7 is commutative algebraic, aside from the p-adic interpolation result. A key idea is to first establish a result for the ring $A = \mathbb{Z}_p[x_1, \dots, x_d]$, treating only the special case where I, J are p-reduced ideals (Definition 4.2) for $p \geq 5$ (Theorem 4.5). The p-reduced condition is needed in order to apply the generalized p-adic analytic arc theorem. Here we also use an idea of Amitsur (Lemma 4.4), to handle the case of p-reduced ideals I where $(A/I) \otimes \mathbb{Q}_p$ is an infinite-dimensional $\mathbb{Q}_p$-vector space. We next deduce the result for arbitrary ideals I, J in a polynomial ring $A = K[x_1, \dots, x_d]$ over a field of characteristic 0 (Theorem 4.1), as follows. We first show that K can be taken to be finitely generated over $\mathbb{Q}$; next, we use the fact that such a field embeds into infinitely many p-adic fields $\mathbb{Q}_p$ via the Chebotarev density theorem. Finally, passing from $\mathbb{Q}_p$ to $\mathbb{Z}_p$-coefficients, we show that one can pass from ideals to suitable p-reduced ideals. We then treat the general case that A is a finitely-generated commutative K-algebra by using a theorem of Srinivas [29, Theorem 2] to reduce this case to that of a polynomial ring $K[x_1, \dots, x_d]$.

An interesting feature of this proof is that while Theorem 1.7 concerns finitely-generated commutative K-algebras A that are Noetherian rings, the proof itself currently requires a detour using the non-Noetherian ring $\mathcal{R}(S)$.

1.3 Affine Scheme Version of Main Result

Using the standard correspondence of categories

$$\{\text{Affine Schemes}\} \longleftrightarrow \{\text{Commutative rings with identity}\},$$

we can restate Theorem 1.7 as follows.

Theorem 1.8 (Generalized SML Theorem for affine schemes of finite type) *Let K be a field of characteristic zero and let X be an affine scheme of finite type over K. If $\sigma \in \mathrm{Aut}_K(X)$ and Y and Z are closed subschemes of X, then*

$$S = S(Z, Y) := \{n \in \mathbb{Z} : \sigma^n(Z) \subseteq Y\}$$

has the two-sided SML property.

From the scheme-theoretic viewpoint, Theorem 1.6 corresponds to the special case that Y and Z are reduced closed subschemes and $Z = \{x\}$ is a point. The main difficulty in establishing Theorem 1.8 is omitting the requirement that the source Z and target Y be reduced. Allowing a source Z of arbitrary dimension is less of a difficulty.

We show via examples in Section 6 that for automorphisms one cannot generalize this result to arbitrary affine schemes without altering the conclusion that the set is a two-sided SML set. Example 6.4 shows the need for the scheme to be of finite type over K, while Example 6.5 shows the need to work over a field K of characteristic zero. There remains a possibility of generalizing the result to arbitrary schemes of finite type over characteristic zero fields.

1.4 Generalizations

The ultimate level of generalization possible for mappings having the SML property is not clear.

A natural question is: "Is there an SML Theorem for endomorphisms of algebraic varieties?" For endomorphisms that are not automorphisms, the maps τ^m with $m < 0$ are not defined, and extensions of Theorem 1.7 to endomorphisms must be formulated in terms of one-sided infinite arithmetic progressions. Recent work described below shows that the SML property does hold for some classes of endomorphisms at the geometric level, while endomorphisms at the algebraic level have not yet been studied. At present in the characteristic 0 case, no counterexamples to the (one-sided) SML property are known for any endomorphism at either the geometric or algebraic level.

The dynamics of endomorphisms in the geometric setting is currently a very active area of study. In 2009 Ghioca and Tucker [16] conjectured that the forward iterates of a point P under an endomorphism $\tau\colon X \to X$ of a quasiprojective variety over $\mathbb{C}$ should satisfy the SML property for intersecting a closed subvariety V. They term this assertion the *dynamical Mordell–Lang conjecture*; see Ghioca, Tucker, and Zieve [17]. This conjecture fits in the general framework of dynamical conjectures of S. Zhang [33, Sect. 4]. It is now known that one-sided versions of the SML Theorem are valid for some special classes of endomorphisms; see for example Benedetto, Ghioca, Kurlberg, and Tucker [7]. The dynamical Mordell–Lang conjecture currently appears to be difficult in the general case.

When endomorphisms are viewed at the ideal level, as in this paper, there are two different questions to consider: the first concerns upward inclusions, and the second downward inclusions, of ideals under preimages of endomorphisms of polynomial rings. Given an endomorphism $\tau\colon A \to A$ of a commutative K-algebra A, and a nonzero ideal I of A the preimages $\tau^{-1}(I)$ are ideals of A, but the image $\tau(I)$ is usually not an ideal of A but is an ideal of the image ring $A' := \tau(A)$. To formulate inclusions purely in terms of A-ideals, these concern the sets

$$S(I, J) := \{m \geq 0 \mid I \supseteq (\tau^m)^{-1}(J)\},$$
$$S'(I, J) := \{m \geq 0 \mid (\tau^m)^{-1}(I) \supseteq J\},$$

respectively.

Our methods in this paper do not give information about either of the sets $S(I, J)$ and $S'(I, J)$. However, a number of results in this paper partially extend to the endomorphism case; see Remarks 2.2 and 3.3. New ideas are certainly needed for general endomorphisms, because the generalized analytic arc theorem need not hold in the p-adic case in neighborhoods of superattracting fixed points.

2 p-Adic Preliminaries

Much of our study of automorphisms of algebras relies on reductions to simpler cases. We will eventually reduce the proof of Theorem 1.7 to the special case where one is working with a polynomial ring over a p-adic field.

For the analysis of this special case we establish preliminary results on Jacobian matrices of p-adic mappings and some results from p-adic analysis. Section 2.1 allows S-algebra endomorphisms, while all later sections specialize to the automorphism case.

2.1 Evaluation Maps and Jacobians for Polynomial Endomorphicms

Let $R = S[x_1, \dots, x_d]$ be a polynomial ring over an integral domain S. Any S-algebra endomorphism $\tau\colon R \to R$ is uniquely determined by its values $\{\tau(x_i) : 1 \leq i \leq d\}$ on the monomials x_i, and any assignment of values

$$\tau(x_i) := F_i(x_1, \dots, x_d) \in S[x_1, \dots, x_d], \quad 1 \leq i \leq d,$$

uniquely extends to an endomorphism $\tau\colon R \to R$ that acts as the identity on S, given by

$$\tau(P(x_1, \dots, x_d)) := P(\tau(x_1), \dots, \tau(x_d)) \in S[x_1, \dots, x_d]. \tag{2.1}$$

Composition of endomorphisms will be denoted $\tau_2 \circ \tau_1(P) := \tau_2(\tau_1(P))$. In what follows we use τ to denote a general S-algebra endomorphism, while symbols σ, ρ are reserved for S-algebra automorphisms.

The *Jacobian matrix* $J(\tau;\mathbf{x}) \in M_{d\times d}(S[x_1,\dots,x_d])$ of the map τ at $\mathbf{x}$ is given by

$$J(\tau;\mathbf{x}) := \begin{bmatrix} \frac{\partial}{\partial x_1}F_1 & \frac{\partial}{\partial x_2}F_1 & \cdots & \frac{\partial}{\partial x_d}F_1 \\ \frac{\partial}{\partial x_1}F_2 & \frac{\partial}{\partial x_2}F_2 & \cdots & \frac{\partial}{\partial x_d}F_2 \\ & \cdots & \cdots & \\ \frac{\partial}{\partial x_1}F_d & \frac{\partial}{\partial x_2}F_2 & \cdots & \frac{\partial}{\partial x_d}F_d \end{bmatrix}.$$

These matrices satisfy the polynomial identity under composition

$$J(\tau_2\circ\tau_1;\mathbf{x}) = J\big(\tau_2;\tau_1(\mathbf{x})\big)\,J(\tau_1;\mathbf{x}),$$

in the ring $M_{d\times d}(S[x_1,\dots,x_d])$.

For $\mathbf{s} = (s_1,s_2,\dots,s_d) \in S^d$, we define the *evaluation map* $\mathrm{ev}_{\mathbf{s}}\colon S[x_1,x_2,\dots,x_d] \to S$, which assigns $x_i \mapsto s_i$, *i.e.,*

$$\mathrm{ev}_{\mathbf{s}}(F)(x_1,\dots,x_d) := F(s_1,s_2,\dots,s_d).$$

(For constants $c \in S$ we have $\mathrm{ev}_{\mathbf{s}}(c)(x_1,\dots,x_d) = c$.) Using this map, we define the Jacobian matrix of a polynomial map τ with its entries evaluated at the point $\mathbf{s} \in S^d$ as

$$J(\tau;\mathbf{s}) := \mathrm{ev}_{\mathbf{s}}(J(\tau;\mathbf{x})) = \Big[\mathrm{ev}_{\mathbf{s}}\Big(\frac{\partial}{\partial x_j}F_i(x_1,\dots,x_d)\Big)\Big]_{1\le i,j\le d},$$

with $J(\tau;\mathbf{s}) \in M_{d\times d}(S)$.

In the same vein, given an endomorphism τ of $S[x_1,\dots,x_d]$ we define a map $f_\tau\colon S^d \to S^d$ for each $\mathbf{s} \in S^d$, acting coordinatewise, by

$$\begin{aligned} f_\tau(\mathbf{s}) &:= \mathrm{ev}_{\mathbf{s}}\big(\tau(x_1),\tau(x_2),\cdots,\tau(x_d)\big) \\ &= \big(F_1(s_1,\dots,s_d),F_2(s_1,\dots,s_d),\dots,F_d(s_1,\dots,s_d)\big). \end{aligned}$$

We call f_τ the *dynamical evaluation map* associated with τ. The important property it has is compatibility with composition of maps, given as

$$f_{\tau_2\circ\tau_1}(\mathbf{s}) = (f_{\tau_2}\circ f_{\tau_1})(\mathbf{s}).$$

In particular, for iteration of the map f_τ one has $f_{\tau^m} = (f_\tau)^m$. A consequence of this compatibility is that if the endomorphism is an automorphism σ, then the dynamical evaluation map $f_\sigma\colon S^d \to S^d$ is a bijection, because $f_\sigma \circ f_{\sigma^{-1}} = f_{id}$, the identity map. A second consequence is the identity

$$J(\tau_2\circ\tau_1;\mathbf{s}) = J(\tau_2;f_{\tau_1}(\mathbf{s}))\,J(\tau_1;\mathbf{s}), \quad \mathbf{s}\in S$$

in the ring $M_{d\times d}(S)$.

The dynamical evaluation map f_τ is analogous to a map acting on an affine variety as in Theorem 1.6. In general it is a nonlinear map, and it usually does not respect either addition or coordinatewise multiplication on S^d; *i.e.,* one can have $f_\tau(\mathbf{s}_1+\mathbf{s}_2) \neq f_\tau(\mathbf{s}_1)+f_\tau(\mathbf{s}_2)$ and $f_\tau(\mathbf{s}_1\mathbf{s}_2) \neq f_\tau(\mathbf{s}_1)f_\tau(\mathbf{s}_2)$. Furthermore, one can have $f_\tau(\mathbf{0}) \neq \mathbf{0}$, where $\mathbf{0} := (0,0,\dots,0) \in S^d$. In an Appendix to this paper we prove a result (Proposition A.1) that clarifies the differences between the algebraic dynamic action of an endomorphism τ acting on ideals I and the geometric action of the dynamic evaluation map f_τ acting on varieties $V(I)$.

The above definitions are stated for endomorphisms τ, but in the remainder of the paper we will restrict to the case of automorphisms σ, unless specified otherwise.

2.2 p-adic Approximate Fixed Points for Automorphisms

Now we specialize to the case where the integral domain S is a $\mathbb{Z}_p$-algebra. We consider an automorphism σ of $R = S[x_1, \dots, x_d]$ and study the dynamical evaluation map f_σ. The following lemma asserts the existence of approximate fixed points $(\bmod\, p)$ with invertible Jacobian matrices for dynamical evaluation maps of polynomial automorphisms.

Lemma 2.1 *Let p be a prime, let S be a $\mathbb{Z}_p$-algebra that is finitely generated as a $\mathbb{Z}_p$-module, and let $\sigma = (F_1, \dots, F_d)\colon \mathbb{Z}_p[x_1, \dots, x_d] \to \mathbb{Z}_p[x_1, \dots, x_d]$ be an $\mathbb{Z}_p$-algebra automorphism. Then there is an integer m such that for every point $\mathbf{s}_0 = (s_1, \dots, s_d) \in S^d$ with the property that the dynamical evaluation map $f_\sigma\colon S^d \to S^d$ at $\mathbf{s}_0$ satisfies*

$$f_\sigma(s_1, \dots, s_d) \equiv (s_1, \dots, s_d) \pmod{pS},$$

and the Jacobian $J(\sigma^m; \mathbf{x})$ evaluated at $(x_1, x_2, \dots, x_d) = (s_1, \dots, s_d)$ is the identity matrix $(\bmod\, pS)$, that is, $\mathrm{ev}_{\mathbf{s}_0}(J(\sigma^m; \mathbf{x})) \equiv I (\bmod\, pS)$.

Proof The ring S/pS is a finite ring, since S is a finitely generated $\mathbb{Z}_p$-module. Furthermore, $J(\sigma; \mathbf{s})$ has inverse mod p given by $J(\sigma^{-1}; \mathbf{s})$, and hence it is invertible mod p. Take m to be the order of $\mathrm{GL}_d(S/pS)$. We let

$$J(\sigma; \mathbf{s}) := \mathrm{ev}_{\mathbf{s}}\big(J(\sigma; \mathbf{x})\big) \in M_{d\times d}(S)$$

denote the Jacobian matrix of a polynomial map σ with its entries evaluated at the point $\mathbf{s} \in S^d$. Since σ is a $\mathbb{Z}_p$-algebra automorphism, we have for $\mathbf{s}_1, \mathbf{s}_2 \in S^d$ that

$$\mathbf{s}_1 \equiv \mathbf{s}_2 \pmod{pS} \Rightarrow f_\sigma(\mathbf{s}_1) \equiv f_\sigma(\mathbf{s}_2) \pmod{pS}.$$

It follows that the quotient map $\bar{f}_\sigma\colon (S/pS)^d \to (S/pS)^d$ is well-defined. Similarly, since $J(\sigma; \mathbf{x})$ has entries given by polynomials with coefficients in $\mathbb{Z}_p$,

$$\mathbf{s}_1 \equiv \mathbf{s}_2 \pmod{pS} \Longrightarrow J(\sigma; \mathbf{s}_1) \equiv J(\sigma; \mathbf{s}_2) \pmod{pS},$$

where $\equiv$ is taken entry-wise.

Then for any point $\mathbf{s} = (s_1, \dots, s_d) \in S^d$ we have

$$\begin{aligned} J(\sigma^m; \mathbf{s}) &= J\big(\sigma; f_{\sigma^{m-1}}(\mathbf{s})\big)\, J\big(\sigma; f_{\sigma^{m-2}}(\mathbf{s})\big) \cdots J(\sigma; \mathbf{s}) \\ &= J\big(\sigma; (f_\sigma)^{m-1}(\mathbf{s})\big)\, J\big(\sigma; (f_\sigma)^{m-2}(\mathbf{s})\big) \cdots J(\sigma; \mathbf{s}). \end{aligned}$$

Hence if $\mathbf{s}_0$ is a fixed point of the quotient map $\bar{f}_\sigma$, then $(f_\sigma)^j(\mathbf{s}_0) \equiv \mathbf{s}_0 \pmod{pS}$, for all $j \geq 1$, so that

$$J\big(\sigma; (f_\sigma)^j(\mathbf{s}_0)\big) \equiv J(\sigma; \mathbf{s}_0) \pmod{pS}.$$

Substituting these in the formula above yields

$$J(\sigma^m; \mathbf{s}_0) \equiv J(\sigma; \mathbf{s}_0)^m \pmod{pS}.$$

By our choice of m, $M := J(\sigma^m; \mathbf{s}_0)$ is congruent to the identity mod pS, as required. ■

Remark 2.2 The argument of Lemma 2.1 extends to $\mathbb{Z}_p$-algebra endomorphisms τ, but yields only the weaker conclusion: there exists an integer m such that for each

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

$\mathbf{s}_0$ such that $f_\tau(\mathbf{s}_0) \equiv \mathbf{s}_0 \pmod{pS}$, the Jacobian $\mathrm{ev}_{\mathbf{s}_0}(J(\tau^m;\mathbf{x})) \equiv M \pmod{pS}$, where $M^2 = M$ is an idempotent in $M_{d\times d}(S/pS)$ and M depends on $\mathbf{s}_0$.

2.3 p-adic Reduction Lemmas

We start with an embedding theorem due to Lech [20, §4–5]. His result can be regarded as a p-adic analogue of the Lefschetz principle.

Lemma 2.3 *Let K be a finitely generated extension of $\mathbb{Q}$ and let $\mathcal{S}$ be a finite subset of K. Then there exist infinitely many primes p such that K embeds in $\mathbb{Q}_p$; moreover, for all but finitely many of these primes every nonzero element of $\mathcal{S}$ is sent to a unit in $\mathbb{Z}_p$.*

Proof This is shown in [4, Lemma 3.1]. The Chebotarev density theorem is used to show that there exists a positive density set of primes p having the required property. ■

Strassman's theorem [30] asserts that if a power series $f \in \mathbb{Q}_p[[z]]$ converges in the closed p-adic unit disc

$$B_{\mathbb{Q}_p}(0;1) := \{z \in \mathbb{Q}_p : |z|_p \le 1\} = \mathbb{Z}_p$$

and has infinitely many zeros in this disc, then it is identically zero. We will use the following variant of Strassman's theorem.

Theorem 2.4 (Extended Strassman's Theorem) *Let p be a prime and let R be a finite-dimensional $\mathbb{Q}_p$-algebra. Suppose that the formal power series $f(z) \in R[[z]]$ is absolutely convergent for all $z \in \mathbb{Z}_p$ and has infinitely many zeros in $\mathbb{Z}_p$. Then $f(z)$ is identically zero.*

Proof Let n denote the dimension of R as a $\mathbb{Q}_p$-vector space. We write

$$R = \mathbb{Q}_p v_1 + \mathbb{Q}_p v_2 + \cdots + \mathbb{Q}_p v_n,$$

with $v_1 = 1$. Then $f(z) = v_1 f_1(z) + \cdots + v_n f_n(z)$ with each

$$f_i(z) = \sum_{k=0}^{\infty} c_k z^k \in \mathbb{Q}_p[[z]],$$

converging for all $z \in \mathbb{Z}_p$. Linear independence of the v_i over $\mathbb{Q}_p$ implies that $f(z) = 0$ requires that each $f_i(z) = 0$ separately. Since $f(z)$ has infinitely many zeros on $z \in \mathbb{Z}_p$, by Strassman's theorem ([30], *cf.* Cassels [10, Theorem 4.1]) applied to $f_i(z)$, each $f_i(z)$ is identically zero. Thus $f(z)$ is identically zero. ■

Finally, we will need a finiteness result for reduction (mod p) in a $\mathbb{Z}_p$-module.

Lemma 2.5 *Let p be prime and let $\mathcal{M}$ be a $\mathbb{Z}_p$-module that is isomorphic to a submodule of $\mathbb{Q}_p^d$ for some natural number d. Then $\mathcal{M}/p\mathcal{M}$ is a finite-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space.*

Proof Note that $\mathcal{M}/p\mathcal{M}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space. We claim that its dimension is at most d. To see this, let $\theta_1, \ldots, \theta_{d+1}$ be elements of $\mathcal{M}$. If we regard $\mathcal{M}$ as a submodule of $\mathbb{Q}_p^d$, then we see that 0 is a nontrivial $\mathbb{Q}_p$-linear combination of the images of $\theta_1, \dots, \theta_{d+1}$ in $\mathbb{Q}_p^d$. Clearing denominators, we see that there exist $a_1, \dots, a_{d+1} \in \mathbb{Z}_p$, not all of which are in $p\mathbb{Z}_p$, such that $\sum_{i=1}^{d+1} a_i\theta_i = 0$. Reducing mod $p\mathcal{M}$, we see that the images of $\theta_1, \dots, \theta_{d+1}$ in $\mathcal{M}/p\mathcal{M}$ are linearly dependent over $\mathbb{Z}/p\mathbb{Z}$ and thus any set of size $d+1$ in $\mathcal{M}/p\mathcal{M}$ is linearly dependent. Hence $\mathcal{M}/p\mathcal{M}$ is at most d-dimensional, and, in particular, it is a finite-dimensional $\mathbb{Z}/p\mathbb{Z}$-vector space. ■

3 Generalized p-adic Analytic Arc Theorem

In this section we prove a generalization of the p-adic analytic arc theorem given in [5, Theorem 1.1] that applies to a larger class of rings. The generalization applies to any $\mathbb{Z}_p$-algebra S that is finitely generated and torsion-free as a $\mathbb{Z}_p$-module with the added hypothesis that $p \geq 5$. Examples given in [4] show that this theorem does not hold for $p = 2$; the case $p = 3$ is currently open.

Theorem 3.1 (Generalized p-adic analytic arc theorem) *Let $p \geq 5$ be prime, and suppose $\sigma = (H_1, H_2, \dots, H_d)$ is a polynomial automorphism of $\mathbb{Z}_p[x_1, \dots, x_d]$. Let S be a $\mathbb{Z}_p$-algebra that is finitely generated and torsion-free as a $\mathbb{Z}_p$-module, and let $f_\sigma\colon S^d \to S^d$ denote the induced dynamical evaluation map. Suppose that an initial value $\mathbf{s}_0 = (s_1, \dots, s_d) \in S^d$ satisfies the following two conditions:*

(i) *$H_i(s_1, \dots, s_d) \equiv s_i \pmod{pS}$ for $0 \leq i \leq d$;*
(ii) *the Jacobian matrix $M = J(\sigma; \mathbf{x})|_{\mathbf{x}=\mathbf{s}_0}$ evaluated at $\mathbf{x} = \mathbf{s}_0$ is the identity matrix $\pmod{pS}$.*

Then there exist power series $f_1(z), \dots, f_d(z) \in (S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)[[z]]$ that converge for all $z \in \mathbb{Z}_p$ and that satisfy

(a) *$f_i(z+1) = H_i(f_1(z), \dots, f_d(z))$, for $1 \leq i \leq d$;*
(b) *$f_i(0) = s_i$, for $1 \leq i \leq d$.*

Remark 3.2 The associated *analytic arc* in S^d constructed in Theorem 3.1 is

$$\mathcal{C} = \mathcal{C}(\sigma, \mathbf{s}_0) := \{(f_1(z), \dots, f_d(z)) : z \in \mathbb{Z}_p\} \subset S^d.$$

The result implies that the arc $\mathcal{C}$ contains all the iterates $\{f_\sigma^{(m)}(\mathbf{s}_0) : m \geq 0\}$ of the initial value $\mathbf{s}_0$, since (a) shows that $f_\sigma^{(m)}(\mathbf{s}_0) = (f_1(m), \dots, f_d(m))$ holds. It covers cases such as $S = \mathbb{Z}_5$ with $\sigma(x) = x + 5$ on $\mathbb{Z}_5[x]$, where one can take $\mathbf{s}_0 = 0$, and nevertheless the induced dynamical evaluation map f_σ has no fixed points. The proof follows the basic plan of the result in [4] but involves more complications. It shows that conditions (i) and (ii) imply that $f_\sigma^{(p^m)}(\mathbf{s}_0)$ converges rapidly to s_0 as $m \to \infty$, and uses this to show analyticity of the constructed maps $f_1(z), \dots, f_d(z)$.

Remark 3.3 Theorem 3.1 cannot be extended to cover all general algebra endomorphisms of $\mathbb{Z}_p[x_1, \dots, x_d]$. For general endomorphisms there may be no iterate where conditions (i) and (ii) both hold, and Remark 2.2 asserts one can only guarantee there exists a point where the Jacobian, when evaluated $\pmod{pS}$, is an idempotent matrix. The worst case is where the Jacobian vanishes identically $\pmod{pS}$. Consider $d = 1$ with $H_1(x) = x^{10}$, where we take $p = 5$ and $s_0 = 5$, a case where the

Jacobian vanishes identically. In this case, we have that $\sigma^n(s_0) = 5^{10^n}$ for $n \geq 0$. Suppose that it were possible to find an arithmetic progression $\{an+b\}_{n\in\mathbb{Z}}$ and a 5-adic analytic map $f\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ with the property that $f(n) = \sigma^{an+b}(s_0)$ for all integers n. Then we would necessarily have $f(5^k) \to 0$ as $k \to \infty$. But $f(0) = \sigma^b(5) \neq 0$, and so it is impossible to find even a continuous map $f\colon \mathbb{Z}_5 \to \mathbb{Z}_5$ that has the property (a).

To begin the proof, we first introduce a ring of polynomials that take "integral" values when evaluated at values in $\mathbb{Z}_p$.

Definition 3.4 Given a prime p and a $\mathbb{Z}_p$-algebra S that is finitely generated and torsion-free as a $\mathbb{Z}_p$-module, let $\mathcal{R}(S)$ denote the subring of the polynomial ring $(S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)[z]$ consisting of those polynomials that belong to S under evaluation at each $z \in \mathbb{Z}_p$.

The $\mathbb{Z}_p$-algebra $\mathcal{R}(S)$ offers a crucial advantage over the polynomial ring $S \otimes_{\mathbb{Z}_p} \mathbb{Q}[z]$, which is that the following closure property holds: if $Q(z) \in \mathcal{R}(S)$, then the equation

$$F(z+1) - F(z) = Q(z)$$

has a solution with $F(z) \in \mathcal{R}(S)$. We use this in proving our general analytic arc theorem (Theorem 3.1). We note however that the ring $\mathcal{R}(S)$ has some pathological properties. It is a non-Noetherian ring, by a general criterion of Cahen and Chabert [9, Prop. VI.2.4]. (In fact, for $S = \mathbb{Z}_p$, the ring

$$\mathcal{R}(S) = \mathbb{Z}_p\Big[\, f_n(z) = \frac{z(z-1)\cdot(z-(n-1))}{n!} : n \geq 0\Big]$$

as a linear space over $\mathbb{Z}_p$; see Lemma 3.5. An example of an infinite ascending chain of ideals in $\mathcal{R}(S)$ that does not stabilize is $(z), (z, f_p(z)), (z, f_p(z), f_{p^2}(z)), \dots$.) Secondly, it can be shown that $\mathcal{R}(S)$ is not of finite type over $\mathbb{Z}_p$; *i.e.*, , it is not finitely generated as a $\mathbb{Z}_p$-algebra. Finally, $\mathcal{R}(S)$ is not a UFD in general: for $S = \mathbb{Z}_2$, $u := z(z-1)/2$, $v := (z-2)(z-3)/2$, $u' := z(z-3)/2$, $v' := (z-1)(z-2)/2$ are irreducible elements of $\mathcal{R}(S)$ and $uv = u'v'$; there are similar examples for $S = \mathbb{Z}_p$, $p \geq 3$.

Lemma 3.5 *Given a prime p and a $\mathbb{Z}_p$-algebra S that is finitely generated and torsion-free as a $\mathbb{Z}_p$-module, the ring $\mathcal{R}(S)$ is given by*

$$\mathcal{R}(S) = \Big\{\, f(z) = \sum_{i=0}^{m} b_i \binom{z}{i} : m \geq 0 \text{ and } b_i \in S \Big\}.$$

Proof In the special case $S = \mathbb{Z}_p$ the lemma asserts that the polynomials

$$\binom{z}{k} = \frac{z(z-1)\cdots(z-k+1)}{k!}$$

for $k \geq 0$ are a basis of the polynomials in $\mathbb{Q}_p[z]$ that map $\mathbb{Z}_p$ into itself. This is a theorem of Mahler [24, pp. 49–50]. For the general case, since S is finitely generated

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

and torsion-free, $S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p[z]$ is a finite direct sum of copies of $\mathbb{Q}_p[z]$. The result then follows from the special case applied to each copy separately. ∎

Lemma 3.6 *Let p be prime and let S be a $\mathbb{Z}_p$-algebra that is finitely generated and torsion-free as a $\mathbb{Z}_p$-module. Suppose $Q_1(z), \dots, Q_d(z) \in \mathcal{R}(S)$ are given polynomials of degree at most N. Then there exists a solution $[h_1(x), \dots, h_d(x)]^{\mathrm{T}} \in \mathcal{R}(S)^n$ to the equation*

$$\begin{bmatrix} h_1(z+1) \\ \vdots \\ h_n(z+1) \end{bmatrix} \equiv \begin{bmatrix} h_1(z) \\ \vdots \\ h_d(z) \end{bmatrix} - \begin{bmatrix} Q_1(z) \\ \vdots \\ Q_d(z) \end{bmatrix} \pmod{p\mathcal{R}(S)} \tag{3.1}$$

such that $h_1(0) = \cdots = h_d(0) = 0$ and $h_1, \dots, h_d$ have degree at most $N+1$.

Proof By assumption, each $Q_i(z) \in \mathcal{R}(S)$ is of degree at most N, and so

$$Q_i(z) = \sum_{k=0}^{N} c_{i,k} \binom{z}{k}$$

with each $c_{i,k} \in S$. We define

$$h_i(z) := -\sum_{k=0}^{N} c_{i,k} \binom{z}{k+1},$$

which implies that h_i is in $\mathcal{R}(S)$ and is of degree at most $N+1$. Using the identity

$$\binom{z+1}{k+1} - \binom{z}{k+1} = \binom{z}{k}$$

it is easy to check that this gives a solution to equation (3.1). Furthermore, $h_i(0) = 0$ for $1 \le i \le d$. ∎

To create analytic maps in the modified version of the p-adic analytic arc lemma, we will use the following lemma about subalgebras of $\mathcal{R}(S)$.

Lemma 3.7 *Let p be a prime and let S be a $\mathbb{Z}_p$-algebra that is finitely generated and torsion-free as a $\mathbb{Z}_p$-module. Let N be a natural number, and let*

$$S_N = \Big\{ c + \sum_{i=1}^{N} p^i h_i(z) \mid c \in S, h_i(z) \in \mathcal{R}(S), \deg(h_i) \le 2i-1 \Big\},$$

$$T_N = S_N + \Big\{ c + \sum_{i=1}^{M} p^i h_i(z) \mid M \ge 1, c \in S, h_i(z) \in \mathcal{R}(S), \deg(h_i) \le 2i-2 \Big\}.$$

Then the $\mathbb{Z}_p$-subalgebra of $\mathcal{R}(S)$ generated by S_N is contained in T_N.

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

Proof Since S_N and T_N are both closed under addition and $S_N \subseteq T_N$, it is sufficient to show that $S_N T_N \subseteq T_N$. To do this, suppose

$$H(z) = c + \sum_{i=1}^{N} p^i h_i(z) \in S_N,$$

$$G(z) = d + \sum_{i=1}^{M} p^i g_i(z) \in T_N,$$

where $c, d \in S$ and $h_i(z), g_i(z) \in \mathcal{R}(S)$ with $\deg(g_i) \leq 2i - 2$ for $i > N$ and $\deg(g_i), \deg(h_i) \leq 2i - 1$ for $i \leq N$. We must show that $H(z)G(z) \in T_N$. Notice that

$$H(z)G(z) = cG(z) + dH(z) - cd + \sum_{i=1}^{N} p^i h_i(z) \sum_{j=1}^{M} p^j g_j(z).$$

Then $cG(z), dH(z)$, and cd are all in T_N, and since T_N is closed under addition, it is sufficient to show that

$$\sum_{i=1}^{N} p^i h_i(z) \sum_{j=1}^{M} p^j g_j(z) = \sum_{k=2}^{N+M} p^k \sum_{i=1}^{k-1} g_i(z) h_{k-i}(z)$$

is in T_N. But since $g_i(z)$ has degree at most $2i - 1$ and $h_{k-i}(z)$ has degree at most $2(k - i) - 1$, we see that

$$\sum_{i=1}^{k-1} g_i(z) h_{k-i}(z)$$

has degree at most $2k - 2$. It follows that

$$\sum_{i=1}^{N} p^i h_i(z) \sum_{j=1}^{M} p^j g_j(z) \in T_N.$$

The result follows. ∎

Proof of Theorem 3.1 We construct $(f_1(z), \ldots, f_d(z))$ by successive approximation $(\mathrm{mod}\ p^j \mathcal{R}(S))$. The approximations will be denoted $g_{i,j}(z)$ for $1 \leq i \leq d$. We initialize with

$$g_{i,0}(z) := s_i \text{ for } 1 \leq i \leq d.$$

We prove by induction on j that one can recursively pick

$$g_{i,j}(z) := s_i + \sum_{k=1}^{j} p^k h_{i,k}(z),$$

such polynomials $h_{i,j}(z) \in \mathcal{R}(S)$ $(1 \leq i \leq d)$ satisfy the three conditions:

(a) $h_{i,j}(0) = 0$ for $1 \leq i \leq d$;
(b) $h_{i,j}(z)$ has degree at most $2j - 1$ for $1 \leq i \leq d$;
(c) there holds

$$g_{i,j}(z+1) \equiv H_i\big(g_{1,j}(z), \ldots, g_{d,j}(z)\big) \ \big(\mathrm{mod}\ \ p^{j+1}\mathcal{R}(S)\big).$$

The base case of the induction is $j = 0$. Conditions (a) and (b) are vacuous, and (c) holds using hypothesis (i), observing that $\mathcal{R}(S) \cap S = S$.

Let $j \geq 1$ and assume that we have defined $h_{i,k}$ for $0 \leq i \leq d$ and $k < j$ so that conditions (a)–(c) hold for $j - 1$. Our object is now to construct

$$g_{i,j}(z) := g_{i,j-1}(z) + p^j h_{i,j}(z),$$

in which polynomials $h_{i,j}(z) \in \mathcal{R}(S)$ are to be determined, so that conditions (a)–(c) hold. By assumption

$$g_{i,j-1}(z+1) - H_i(g_{1,j-1}(z), \dots, g_{d,j-1}(z)) = p^j Q_{i,j}(z),$$

with $Q_{i,j} \in \mathcal{R}(S)$ for $1 \le i \le d$. Using the notation of the statement of Lemma 3.7, we see that conditions (b) and (c) show that $g_{1,j-1}(z), \dots, g_{d,j-1}(z)$ are in S_{j-1}. Thus by Lemma 3.7 we see that

$$p^j Q_{i,j}(z) = g_{i,j-1}(z+1) - H_i\big(g_{1,j-1}(z), \dots, g_{d,j-1}(z)\big)$$

is in the algebra generated by S_{j-1} and hence is in T_{j-1}. It follows that we can write

$$p^j Q_{i,j}(z) = c_{i,j} + \sum_{k=1}^{M} p^k q_{i,j,k}(z)$$

for some $c_{i,j} \in S$ and polynomials $q_{i,j,k}(z) \in \mathcal{R}(S)$ such that $\deg(q_{i,j,k}) \le 2k-1$ for $k \le j-1$ and $\deg(q_{i,j,k}) \le 2k-2$ for $k \ge j$. Consequently, $p^j Q_{i,j}(z)$ is equivalent modulo $p^{j+1}R$ to the polynomial

$$c_{i,j} + \sum_{k=1}^{j} p^k q_{i,j,k}(z),$$

a polynomial of degree at most $2j-2$. Hence $Q_{i,j}(z)$ is congruent to a polynomial in $\mathcal{R}(S)$ of degree at most $2j-2$ mod $p\mathcal{R}(S)$. To satisfy property (c) for j it is sufficient to find $\{h_{i,j}(z) \in \mathcal{R}(S) : 1 \le i \le d\}$ such that

$$g_{i,j-1}(z+1) + p^j h_{i,j}(z+1) - H_i\big(g_{1,j-1}(z) + p^j h_{1,j}(z), \dots, g_{d,j-1}(z) + p^j h_{d,j}(z)\big)$$

is in $p^{j+1}\mathcal{R}(S)$ for $1 \le i \le d$. This expression becomes

$$p^j Q_{i,j}(z) + p^j h_{i,j}(z+1) - p^j \sum_{\ell=1}^{d} h_{\ell,j}(z) \frac{\partial H_i}{\partial x_\ell}(x_1, \dots, x_d)\Big|_{x_1=g_{i,j-1}(z),\dots,x_d=g_{d,j-1}(z)}$$

modulo $p^{j+1}\mathcal{R}(S)$. It therefore suffices to solve the system

$$Q_{i,j}(z) + h_{i,j}(z+1) - \sum_{\ell=1}^{d} h_{\ell,j}(z) \frac{\partial H_i}{\partial x_\ell}(x_1, \dots, x_d)\Big|_{x_1=g_{i,j-1}(z),\dots,x_d=g_{d,j-1}(z)} \tag{3.2}$$

$(\bmod\ p\mathcal{R}(S))$, for $1 \le i \le d$, where we can assume that $Q_{i,j}$ is of degree at most $2j-2$. Now consider the Jacobian matrix $M^{(j)}(z) \in M_{d\times d}(\mathcal{R}(S))$ with polynomial entries

$$M^{(j)}(z)_{i\ell} := \frac{\partial H_i}{\partial x_\ell}(x_1, \dots, x_d)\Big|_{x_1=g_{i,j-1}(z),\dots,x_d=g_{d,j-1}(z)}.$$

Property (a) for j yields that

$$g_{i,j}(z) \equiv s_i \,(\bmod\ p\mathcal{R}(S)) \quad \text{for } 1 \le i \le d.$$

It follows that $M^{(j)}(z) \equiv J(\sigma; \mathbf{s}_0)(\bmod\ p\mathcal{R}(S))$. By hypothesis (ii) the matrix $M = J(\sigma; \mathbf{s}_0) \in M_{d\times d}(S)$ is congruent to the identity $(\bmod\ pS)$, and we have $M^{(j)}(z) \equiv M(\bmod\ p\mathcal{R}(S))$. Now equation (3.2) can be rewritten in the form

$$\begin{bmatrix} h_{1,j}(z+1) \\ \vdots \\ h_{d,j}(z+1) \end{bmatrix} \equiv M \begin{bmatrix} h_{1,j}(z) \\ \vdots \\ h_{d,j}(z) \end{bmatrix} - \begin{bmatrix} Q_{1,j}(z) \\ \vdots \\ Q_{d,j}(z) \end{bmatrix} \big(\bmod\ p\mathcal{R}(S)\big).$$

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

The hypotheses of Lemma 3.6 are satisfied, so we conclude that there exists a solution $[h_{1,j}(z), \dots, h_{d,j}(z)]^T \in \mathcal{R}(S)^d$ with $h_{i,j}(0) = 0$ for $1 \le i \le d$ and $h_i(z)$ of degree at most $2j - 1$. Thus conditions (a)–(c) are satisfied for j, completing the induction step.

We now set

$$f_i(z) := s_i + \sum_{j=1}^{\infty} p^j h_{i,j}(z).$$

Each $h_{i,j}(z) \in \mathcal{R}(S)$ is of degree at most $2j - 1$ and hence

$$h_{i,j}(z) = \sum_{k=0}^{2j-1} c_{i,j,k} \binom{z}{k},$$

with $c_{i,j,k} \in S$. We find that

$$f_i(z) = s_i + \sum_{j=1}^{\infty} p^j \Big(\sum_{k=0}^{N_j} c_{i,j,k} \binom{z}{k} \Big) = s_0 + \sum_{k=0}^{\infty} b_{i,k} \binom{z}{k} \tag{3.3}$$

in which

$$b_{i,k} := \sum_{j=1}^{\infty} p^j c_{i,j,k}$$

is absolutely convergent p-adically, since each $c_{i,j,k} \in S$. To show that the series (3.3) converges to an analytic map on $z \in \mathbb{Z}_p$, we must establish that $|b_{i,k}|_p / |k!|_p \to 0$ as $k \to \infty$, *i.e.*, that for any $j > 0$ one has $b_{i,k}/k! \in p^j \mathbb{Z}_p$ for all sufficiently large k. To do this, we note that $c_{i,j,k} = 0$ if $k > 2j - 1$, which is $j < (k+1)/2$. Hence

$$b_{i,k} := \sum_{j \ge (k+1)/2} p^j c_{i,j,k}.$$

It follows that $|b_{i,k}|_p < p^{-(k+1)/2}$. Since $1/|k!|_p < p^{k/(p-1)}$, we see that $b_{i,k}/k! \to 0$, since $p > 3$. Hence $f_1, \dots, f_d$ are analytic maps on $\mathbb{Z}_p$.

The argument above also showed that

$$f_i(z) \equiv g_{i,j}(z) \pmod{p^j \mathcal{R}(S)}.$$

It then follows from property (c) that

$$f_i(z+1) \equiv H_i\big(f_1(z), \dots, f_d(z)\big) \pmod{p^j \mathcal{R}(S)}.$$

Since this holds for all $j \ge 1$, we conclude that

$$f_i(z+1) = H_i\big(f_1(z), \dots, f_d(z)\big).$$

This establishes (a). Finally, we have

$$f_i(0) = s_i + \sum_{j=1}^{\infty} p^j h_{i,j}(0) = s_i,$$

which establishes (b). ∎

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

4 Polynomial Ring Case

In this section, we consider automorphisms of a polynomial ring over a field. We prove the following theorem.

Theorem 4.1 *Let K be a field of characteristic zero and let $A = K[x_1,\dots,x_d]$. If $\sigma\colon A \to A$ is a K-algebra automorphism and I and J are ideals of A, then*

$$\{n \in \mathbb{Z} : \sigma^n(I) \supseteq J\}$$

has the two-sided SML property.

In Section 5 we will deduce the main Theorem 1.7 from this result. We establish Theorem 4.1 using a reduction to the ring $\mathbb{Z}_p[x_1,\dots,x_d]$, given below (Theorem 4.5). A key ingredient in the proof of Theorem 4.5 will be the p-adic analytic arc theorem proved earlier; see Proposition 4.3.

In restricting ideals from a ring with $\mathbb{Q}_p$-coefficients to one with $\mathbb{Z}_p$-coefficients, we only need to consider a special subclass of ideals in $\mathbb{Z}_p[x_1,x_2,\dots,x_d]$, defined as follows.

Definition 4.2 Let p be a prime and let A be a $\mathbb{Z}_p$-algebra. We say that a proper ideal I of A is *p-reduced* if, whenever $x \in A$ has the property that $px \in I$, we necessarily have $x \in I$.

The condition that an ideal I of a $\mathbb{Z}_p$-algebra A be p-reduced is imposed to ensure that the quotient ring A/I is torsion-free as a $\mathbb{Z}_p$-module.

Proposition 4.3 *Let p be prime, and let I and J be two p-reduced ideals in $\mathbb{Z}_p[x_1,\dots,x_d]$. Suppose that $(\mathbb{Z}_p[x_1,\dots,x_d]/I) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is finite dimensional as a $\mathbb{Q}_p$-vector space. If σ is a $\mathbb{Z}_p$-algebra automorphism of $\mathbb{Z}_p[x_1,\dots,x_d]$, then the set $\{n \in \mathbb{Z} \mid \sigma^n(I) \supseteq J\}$ has the two-sided SML property.*

Proof For a polynomial automorphism, $\sigma^n(I) \supseteq J$ if and only if $\sigma^{-n}(J) \subseteq I$. Thus, replacing σ with σ^{-1}, it is sufficient to show that $\{n \in \mathbb{Z} : \sigma^n(J) \subseteq I\}$ is a finite union of complete arithmetic progressions and a finite set. Let $S := \mathbb{Z}_p[x_1,\dots,x_d]/I$. The ring S is a finitely generated and torsion-free $\mathbb{Z}$-algebra, since I is p-reduced. Write $\sigma = (F_1,\dots,F_d) \in \mathbb{Z}_p[x_1,\dots,x_d]^d$. The automorphism σ induces the dynamical evaluation map $f_\sigma\colon S^d \to S^d$ given by

$$(s_1,\dots,s_d) \mapsto \big(F_1(s_1,\dots,s_d),\dots,F_d(s_1,\dots,s_d)\big),$$

for $s_i \in S$, which is a (nonlinear) bijection on S^d. Since S is a torsion-free $\mathbb{Z}_p$-algebra and since, by hypothesis, $S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is finite-dimensional, we have that S^d/pS^d is a finite ring. Although f_σ is nonlinear, we have

$$f_\sigma(s + pS^d) \subseteq f_\sigma(s) + pS^d,$$

hence f_σ induces a well-defined bijective map of S^d/pS^d. Since S/pS is finite, there exists a positive integer a such that $f_\sigma^a(\mathbf{s}) \equiv \mathbf{s} \pmod{pS^d}$ for all $\mathbf{s} \in S^d$.

Now set $\rho = \sigma^{ma}$, where m is chosen as in the statement of Lemma 2.1 and write $\rho = (H_1,\dots,H_d)$. Then for any $\mathbf{s} \in S^d$, we have $f_\rho(\mathbf{s}) \equiv \mathbf{s} \pmod{pS^d}$, and by

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

Lemma 2.1, the Jacobian matrix of ρ is the identity matrix $(\bmod\ pS)$ when evaluated at any point in S^d. For any polynomial $P(x_1,\dots,x_d) \in \mathbb{Z}_p[x_1,\dots,x_d]$ and for any k with $0 \le k \le ma-1$, the fact that σ and ρ are endomorphisms gives (via (2.1))

$$\rho^n(\sigma^k(P(x_1,\dots,x_d))) \in I \text{ if and only if } P \circ f_{\rho^n} \circ f_{\sigma^k}(s_1,\dots,s_d) = 0,$$

where $s_i := x_i + I$. We now treat each k separately. By construction,

$$f_\rho \circ f_{\sigma^k}(s_1,\dots,s_d) \equiv f_{\sigma^k}(s_1,\dots,s_d) \ (\bmod\ pS),$$

and the Jacobian matrix $J(\rho, f_{\sigma^k}(s_1,\dots,s_d))$ is congruent to the identity $(\bmod\ pS)$. Now the generalized p-adic analytic arc theorem (Theorem 3.1) applies to show there exist power series

$$f_1(z),\dots,f_d(z) \in (S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)[[z]]$$

that are analytic on $\mathbb{Z}_p$ and satisfy $(f_1(0),\dots,f_d(0)) = f_{\sigma^k}(s_1,\dots,s_d)$ and

$$f_i(z+1) = H_i(f_1(z),\dots,f_d(z)) \qquad \text{for } 1 \le i \le d.$$

By construction, $f_{\rho^n} \circ f_{\sigma^k}(s_1,\dots,s_d)) = (f_1(n),\dots,f_d(n))$ for all $n \in \mathbb{N}$. Next, select a generating set for the ideal J,

$$J = \big\langle P_1(x_1,\dots,x_d),\dots,P_m(x_1,\dots,x_d) \big\rangle.$$

Then for $1 \le i \le m$, define

$$g_i(z) := P_i\big(f_1(z),\dots,f_d(z)\big) \in (S \otimes_{\mathbb{Z}_p} \mathbb{Q}_p)[[z]].$$

Since $f_1,\dots,f_d$ are analytic on $\mathbb{Z}_p$ and $P_1,\dots,P_m \in \mathbb{Z}_p[x_1,\dots,x_d]$, each $g_i(z)$ is a power series that converges on $\mathbb{Z}_p$, for $1 \le i \le d$. Moreover, $g_i(n) = 0$ if and only if $\rho^n \circ \sigma^k(P_i(x_1,\dots,x_d)) \in I$. Notice that if $g_i(n) = 0$ for infinitely many integers n, then it is identically zero by Theorem 2.4. Thus

$$\{n \in \mathbb{Z} \mid \rho^n(\sigma^k)(J) \subseteq I\}$$

is either a finite set or is all of $\mathbb{Z}$. Since this holds for $0 \le k \le ma_1$, the result now follows. ∎

We must also treat the case where $(\mathbb{Z}_p[x_1,\dots,x_d]/I) \otimes \mathbb{Q}_p$ is an infinite-dimensional $\mathbb{Q}_p$-vector space. This is handled by a reduction to the preceding proposition. To perform this reduction, we use the following lemma, based on an idea of Amitsur [2, Lemma 4, p. 41].

Lemma 4.4 *Let K be an uncountable field and let A be a finitely generated commutative K-algebra. Suppose that there exists a countable set of ideals $\{I_i \mid i \ge 1\}$ of A such that each ideal L of A of finite codimension contains one of the I_i. Then there exists a finite set $j_1,\dots,j_d$ such that $I_{j_1} \cap \cdots \cap I_{j_d} = (0)$.*

Proof Let $J(A)$ denote the Jacobson radical of A. Since A is a finitely generated K-algebra, A is a Jacobson ring (that is, every prime ideal of A is the intersection of the maximal ideals containing it) [13, Theorem 4.19]. Thus $J(A)$ is the intersection of the prime ideals of A (that is, it is the nilradical of A). By the Hilbert basis theorem A is Noetherian and hence some power of the nilradical of A is zero [3, Corollary 7.15]. Hence there is some $m \ge 1$ such that $J(A)^m = (0)$. Given a maximal ideal M of A, note that there is some i such that $I_i \subseteq M^m$. Let Q_i denote the intersection of all ideals of the form M^m, where M is a maximal ideal of A with the property that $M^m \supseteq I_i$. Similarly, we let P_i denote the intersection of all maximal ideals M with the property that $M^m \supseteq I_i$. Then $P_i^m = Q_i \supseteq I_i$ for each $i \geq 1$.

Each maximal ideal M of A necessarily contains some P_i. A result of Amitsur (*cf.* [2, Corollary 4, p. 40]) shows that there exist $j_1, \dots, j_d$ such that $P_{j_1} \cap P_{j_2} \cap \cdots \cap P_{j_d}$ is contained in the Jacobson radical $J(A)$ of A. Hence

$$I_{j_1} \cap \cdots \cap I_{j_d} \subseteq Q_{j_1} \cap \cdots \cap Q_{j_d} = P_{j_1}^m \cap \cdots \cap P_{j_d}^m \subseteq J(A)^m = (0),$$

as required. ■

Theorem 4.5 *Let $p \geq 5$ be prime, let I and J be two p-reduced ideals in $\mathbb{Z}_p[x_1, \dots, x_d]$ with $I \cap \mathbb{Z}_p = J \cap \mathbb{Z}_p = (0)$. If σ is a $\mathbb{Z}_p$-algebra automorphism of $\mathbb{Z}_p[x_1, \dots, x_d]$, then the set $\{m \in \mathbb{Z} \mid \sigma^m(I) \supseteq J\}$ has the two-sided SML property.*

Proof Let $\mathcal{T}$ denote the collection of subsets of $\mathbb{Z}$ that are finite unions of complete doubly-infinite arithmetic progressions along with a finite set. Then $\mathcal{T}$ is countable. Suppose first that $I \subseteq \mathbb{Z}_p[x_1, \dots, x_d]$ is a p-reduced ideal with the property that $(\mathbb{Z}_p[x_1, \dots, x_d]/I) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is finite-dimensional as a $\mathbb{Q}_p$-vector space. Then by Proposition 4.3, we have

$$\{n \in \mathbb{Z} \mid \sigma^n(I) \supseteq J\} \in \mathcal{T}.$$

We now treat the general case. Given $T \in \mathcal{T}$, let I_T denote the intersection of all p-reduced ideals L that contain I and such that

(a) $L \cap \mathbb{Z}_p = (0)$;
(b) $(\mathbb{Z}_p[x_1, \dots, x_d]/L) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a finite-dimensional $\mathbb{Q}_p$-vector space;
(c) $T = \{n \in \mathbb{Z} \mid \sigma^n(L) \supseteq J\}$.

Suppose first that $T \in \mathcal{T}$ is such that I_T is a non-empty intersection. We first note that if $n \in T$, then $\sigma^n(I_T) \supseteq J$; moreover, I_T is an intersection of ideals that contain I and hence it contains I. If $n \notin T$, then $\sigma^n(I)$ cannot contain J, since by definition $\sigma^n(I_T) \not\supseteq J$ and $I \subseteq I_T$. Thus if I_T is a non-empty intersection, then $\{n \mid \sigma^n(I_T) \supseteq J\} = T$.

We next note that the collection of ideals

$$\{I_T \mid T \in \mathcal{T}, I_T \text{ is a nonempty intersection}\}$$

in $\mathbb{Z}_p[x_1, \dots, x_d]$ is countable. Consider the ideals $I'_T = I_T\mathbb{Q}_p[x_1, \dots, x_d]$. By Lemma 4.4, one of the following holds:

(i) there exist $T_1, \dots, T_d \in \mathcal{T}$ such that $I'_{T_1} \cap \cdots \cap I'_{T_d} \subseteq I\mathbb{Q}_p[x_1, \dots, x_d]$;
(ii) there is an ideal $L \supset I\mathbb{Q}_p[x_1, \dots, x_d]$ of $\mathbb{Q}_p[x_1, \dots, x_d]$ of finite codimension that does not contain any of the non-empty I'_T.

In the first case, note that $T_0 = T_1 \cap \cdots \cap T_d \in \mathcal{T}$ and by definition,

$$I'_{T_0} \subseteq I'_{T_1} \cap \cdots \cap I'_{T_d} \subseteq I\mathbb{Q}_p[x_1, \dots, x_d].$$

Since $I\mathbb{Q}_p[x_1, \dots, x_d] \subseteq I_{T_0}$, we see that $I\mathbb{Q}_p[x_1, \dots, x_d] = I_{T_0}$. It follows that the set of integers n for which $\sigma^n(I) \supseteq J$ is exactly T_0. If, on the other hand, (ii) holds, then there exists an ideal L of finite codimension that contains I but does not contain any of the non-empty I_T. Then $L_1 = L \cap \mathbb{Z}_p[x_1, \dots, x_d]$ is p-reduced and satisfies

$\mathbb{Z}_p[x_1,\ldots,x_d]/L_1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p[x_1,\ldots,x_d]/L$ is finite-dimensional. Hence $I_T \subseteq L_1$ for some $T \in \mathcal{T}$, and so $I'_T \subseteq L$, a contradiction. We thus obtain the result. ■

Now we can prove Theorem 4.1.

Proof of Theorem 4.1 Let K be a field of characteristic 0 and let $A = K[x_1,\ldots,x_d]$, with $\sigma\colon A \to A$ a K-algebra automorphism, and let I and J be two proper ideals of A. Then there exist polynomials $F_1,\ldots,F_d,G_1,\ldots,G_d$ in A such that $\sigma(x_i) = F_i(x_1,\ldots,x_d)$ and $\sigma^{-1}(x_i) = G_i(x_1,\ldots,x_d)$ for $i \in \{1,\ldots,d\}$. Next there exist polynomials $C_1,\ldots,C_s$ in A that generate I as an ideal and polynomials $D_1,\ldots,D_t$ in A that generate J.

We let $\mathcal{S}$ denote the set of all nonzero elements of K that occur as a coefficient of one of $F_1,\ldots,F_d,G_1,\ldots,G_d$ and $C_1,\ldots,C_s,D_1,\ldots,D_s$. Then we let R_0 denote the finitely generated $\mathbb{Z}$-algebra generated by the elements of $\mathcal{S}$ inside K, and let K_0 denote the field of fractions of R_0. By construction, $\sigma(R_0[x_1,\ldots,x_d]) \subseteq R_0[x_1,\ldots,x_d]$ and $\sigma^{-1}(R_0[x_1,\ldots,x_d]) \subseteq R_0[x_1,\ldots,x_d]$, and so σ restricts to an R_0-algebra automorphism of $R_0[x_1,\ldots,x_d]$ and to a K_0-algebra automorphism of $K_0[x_1,\ldots,x_d]$.

We let $I_0 := I \cap K_0[x_1,\ldots,x_d])$ and $J_0 = J \cap K_0[x_1,\ldots,x_d])$, which are both $K_0[x_1,x_2,\ldots,x_d]$- ideals. We claim that $\sigma^n(I) \supseteq J$ if and only if $\sigma^n(I_0) \supseteq J_0$. To see this, first observe that if $\sigma^n(I) \supseteq J$, then we have $\sigma^n(I_0) \supseteq J_0$, since

$$\sigma^n(K_0[x_1,\ldots,x_d]) = K_0[x_1,\ldots,x_d].$$

Next suppose that n is an integer for which $\sigma^n(I_0) \supseteq J_0$. Note that $\sigma^n(I)$ is generated by $\sigma^n(C_1),\ldots,\sigma^n(C_s)$, and each of these generators is in $K_0[x_1,\ldots,x_d]$. Since $K[x_1,\ldots,x_d]$ is a free $K_0[x_1,\ldots,x_d]$-module, we have that $\sigma^n(I_0)$ is generated by $\sigma^n(C_1),\ldots,\sigma^n(C_s)$ as an ideal in $K_0[x_1,x_2,\ldots,x_d]$. By construction of K_0, the generators D_i of J lie in J_0 for $i \in \{1,\ldots,t\}$, and so by assumption

$$D_i \in \sum_{i=1}^{t} K_0[x_1,\ldots,x_d]\sigma^n(C_i) \subseteq \sigma^n(I)$$

for $i = 1,\ldots,t$. It follows that $J \subseteq \sigma^n(I)$, proving the claim.

By Lemma 2.3, there exists a prime $p \geq 5$ such that R_0 embeds in $\mathbb{Z}_p$ as a $\mathbb{Z}$-algebra. We identify R_0 with its image in $\mathbb{Z}_p$, and we similarly identify K_0 with its image in $\mathbb{Q}_p$. We then see that the restriction of σ to $K_0[x_1,\ldots,x_d]$ lifts to a $\mathbb{Q}_p$-algebra automorphism ρ of $\mathbb{Q}_p[x_1,\ldots,x_d]$, by identifying $\mathbb{Q}_p[x_1,\ldots,x_d]$ with $(K_0[x_1,\ldots,x_d] \otimes_{K_0} \mathbb{Q}_p)$ and then taking ρ to be the map $\sigma \otimes \mathrm{id}$. In addition, the restriction of σ to $R_0[x_1,\ldots,x_d]$ lifts to a $\mathbb{Z}_p$-algebra automorphism ρ_0 of

$$\mathbb{Z}_p[x_1,\ldots,x_d] \cong (R_0 \otimes_{R_0} \mathbb{Z}_p)[x_1,\ldots,x_d].$$

Note that $\mathbb{Q}_p[x_1,\ldots,x_d]$ is a free $K_0[x_1,\ldots,x_d]$-module, and hence the ideals I_0 and J_0 lift to ideals I' and J' of $\mathbb{Q}_p[x_1,\ldots,x_d]$ respectively. Moreover, since any basis for $\mathbb{Q}_p$ over K_0 is fixed by ρ, by freeness we have

$$\{m \in \mathbb{Z} : \sigma^m(I_0) \supseteq J_0\} \equiv \{m \in \mathbb{Z} : \rho^m(I') \subset J'\}.$$

Next, we let

$$\widetilde{I} = I' \cap \mathbb{Z}_p[x_1,\ldots,x_d] \quad \text{and} \quad \widetilde{J} = J' \cap \mathbb{Z}_p[x_1,\ldots,x_d].$$

Since I', J' are $\mathbb{Q}_p[x_1,\dots,x_d]$-ideals, the ideals $\widetilde{I}$, $\widetilde{J}$ are necessarily p-reduced. Since ρ restricts to the automorphism ρ_0 of $\mathbb{Z}_p[x_1,\dots,x_d]$, a similar argument to the one employed earlier in the proof gives

$$\{m\in\mathbb{Z}:\rho^m(I')\subset J'\}\equiv\{m\in\mathbb{Z}:\rho_0^m(\widetilde{I})\subset\widetilde{J}\}.$$

Theorem 4.5 now applies to show that the set on the right is the union of a finite number of complete, doubly infinite, arithmetic progressions plus a finite set; this equals the set of n with $\sigma^n(I_0)\supseteq J_0$. Finally, using the claim above, this set is identical to the set of integers n for which $\sigma^n(I)\supseteq J$, giving the result. ■

5 Proof of Main Result

In this section we prove Theorem 1.7. This is established by reduction of the general case to the polynomial ring case using the following result of Srinivas, and then using Theorem 4.1.

Theorem 5.1 (Srinivas) *Let A be a finitely generated algebra over an infinite field K. Then there exists a natural number $n=n(A)$ such that for all $N>n$, if*

$$f\colon K[x_1,\dots,x_N]\longrightarrow A\quad\text{and}\quad g\colon K[x_1,\dots,x_N]\longrightarrow A$$

are two surjective K-algebra homomorphisms, then there is an elementary K-algebra automorphism $\phi\colon K[x_1,\dots,x_N]\to K[x_1,\dots,x_N]$ such that $f=g\circ\phi$.

Remark Here *elementary K-algebra automorphism* means one that is a finite composition of automorphisms of the types:

(i) (Translations) $x_i\mapsto x_i+c_i$, with $c_i\in K$;
(ii) (Linear transformations) $x_i\mapsto\sum_j c_{i,j}x_j$ where $(c_{i,j})\in\mathrm{GL}_N(K)$;
(iii) (Triangular automorphisms) $x_i\mapsto x_i$ for $1\le i\le N-1$ and $x_N\mapsto x_N+F(x_1,x_2,\dots,x_{N-1})$.

For our application we only need the fact that ϕ is a K-algebra automorphism.

Proof See Srinivas [29, Theorem 2, p. 126]. ■

We obtain the following result as an immediate corollary.

Proposition 5.2 *Let A be a finitely generated algebra over a field K and let $\phi\colon A\to A$ be a K-algebra automorphism. Then there exists a natural number N, a surjective K-algebra homomorphism $\nu\colon K[x_1,\dots,x_N]\to A$, and a K-algebra automorphism $\tilde{\phi}$ of $K[x_1,\dots,x_N]$ such that:*

(i) *$\nu\circ\tilde{\phi}^n=\phi^n\circ\nu$ for all integers n;*
(ii) *if I and J are ideals in A, then $\phi^n(I)\supseteq J$ if and only if $\tilde{\phi}^n(\nu^{-1}(I))\supseteq\nu^{-1}(J)$.*

Proof We pick $n(A)$ as in the statement of Theorem 5.1. Since A is finitely generated, by $f_1,\dots,f_r$, say, we can take $N=\max(r,\,n(A)+1)$ and construct a surjective map $\nu\colon K[x_1,\dots,x_N]\to A$ sending $x_i\mapsto f_i$ for $1\le i\le r$ and, if $r<n(A)+1$, sending any extra x_j to 0. Now, since ν and $\phi\circ\nu$ are surjective, by Theorem 5.1 there

exists an automorphism $\tilde{\phi}$ of $K[x_1, \ldots, x_N]$ satisfying $\nu \circ \tilde{\phi} = \phi \circ \nu$. Note that by composing on the left by ϕ^{-1} and on the right by $\tilde{\phi}^{-1}$, we see

$$\nu \circ \tilde{\phi}^{-1} = \phi^{-1} \circ \nu.$$

We now prove property (i) by induction on $|n|$, noting the base case $|n| = 1$ is established (for both $n = 1, -1$). Assume that it is true for all integers n with $0 < |n| < m$. Then

$$\phi^m \circ \nu = \phi \circ (\phi^{m-1} \circ \nu) = \phi \circ (\nu \circ \tilde{\phi}^{m-1}) = (\phi \circ \nu) \circ \tilde{\phi}^{m-1} = \nu \circ \tilde{\phi}^m.$$

A similar argument shows that $\phi^{-m} \circ \nu = \nu \circ \tilde{\phi}^{-m}$, and so (i) follows by induction.

To verify (ii), suppose that I and J are ideals of A. Since ν is surjective, we have $\nu(\nu^{-1}(L)) = L$ for every ideal L of A. If $\phi^n(I) \supseteq J$, then $\phi^n \circ \nu(\nu^{-1}(I)) \supseteq J$. Consequently, $\nu \circ \tilde{\phi}^n(\nu^{-1}(I)) \supseteq J$. Thus

$$\tilde{\phi}^n(\nu^{-1}(I)) \supseteq \nu^{-1}(\nu \circ \tilde{\phi}^n(\nu^{-1}(I))) \supseteq \nu^{-1}(J).$$

Also, if $\tilde{\phi}^n(\nu^{-1}(I)) \supseteq \nu^{-1}(J)$, then $\nu(\tilde{\phi}^n(\nu^{-1}(I))) \supseteq \nu(\nu^{-1}(J)) = J$. Since $\nu \circ \tilde{\phi}^n = \phi^n \circ \nu$, we see that $\phi^n(I) = \phi^n(\nu(\nu^{-1}(I)) \supseteq J$. Thus (ii) is established. ■

Proof of Theorem 1.7. We are given a field K of characteristic 0 and a finitely generated commutative K-algebra A with a K-algebra automorphism σ. We wish to show that the set of integers n such that $\sigma^n(I) \supseteq J$ is a finite union of complete doubly-infinite arithmetic progressions along with a finite set.

By Proposition 5.2 there exists a polynomial algebra $K[x_1, \ldots, x_N]$ with an automorphism ϕ and ideals I' and J' such that

$$\phi^n(I') \supseteq J' \iff \sigma^n(I) \supseteq J.$$

The result now follows from Theorem 4.1. ■

6 Examples

We give several examples showing that the results for general ideals I, J can change the answers compared to their associated radical ideals $\sqrt{I}, \sqrt{J}$. Allowing non-radical ideals can change the structure of infinite arithmetic progressions, or eliminate them entirely. We recall that in a commutative ring R, the *radical* is the ideal I consisting of all nilpotent elements of R. In particular, R/I is reduced.

Example 6.1 Let K be an algebraically closed field of characteristic 0 and let $A = K[x, y, z, t, u]$. We define a K-algebra automorphism σ by

$$x \mapsto y - (x - y + yz)t + (x - y + yz), \qquad y \mapsto x - y + yz, \qquad z \mapsto -z,$$
$$t \mapsto -t, \qquad u \mapsto u.$$

Then σ is an automorphism. Let

$$J = (x^2, xy, y^2, y - x, zt - 1, x - u),$$
$$I = (x^2, xy, y^2, y - x, zt - 1, x(z - 1), x - u).$$

Then $\sigma^n(\sqrt{I}) \supseteq \sqrt{J}$ for all $n \in \mathbb{Z}$. However we have

$$\sigma^n(I) \supseteq J \text{ if and only if } n \equiv 0, 3 \pmod{4}.$$

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

Also, $\sigma^n(I) \supseteq \sqrt{J}$ never holds.

Proof We note that σ is an automorphism, since it is a composition of automorphisms $\sigma_3 \circ \sigma_2 \circ \sigma_1$, where

$$\begin{array}{lll}
\sigma_1(x) = x + yt + y, & \sigma_2(x) = y, & \sigma_3(x) = x - y + yz \\
\sigma_1(y) = y, & \sigma_2(y) = x, & \sigma_3(y) = y \\
\sigma_1(z) = z, & \sigma_2(z) = z, & \sigma_3(z) = -z \\
\sigma_1(t) = t, & \sigma_2(t) = t, & \sigma_3(t) = -t \\
\sigma_1(u) = u, & \sigma_2(u) = u, & \sigma_3(u) = u.
\end{array}$$

We note that $\sqrt{J} \supseteq (x, y, zt - 1, u)$, as $x^2, y^2 \in I$ and $zt - 1, x - u \in J$. We claim that $\sqrt{J} = (x, y, zt-1, u)$. To see this, observe that $J \subseteq (x, y, zt-1, u)$ and so A/J surjects onto $A/(x, y, zt - 1, u) \cong K[z, z^{-1}]$. Since $K[z, z^{-1}]$ is reduced, we see that $\sqrt{J}$ must have zero image under this homomorphism and so $\sqrt{J} \subseteq (x, y, zt - 1, u)$. Thus $\sqrt{J} = (x, y, zt-1, u)$, which is a σ-invariant ideal. Also $J \subset (x, y, zt-1, xz, u) \subset \sqrt{I}$ hence $\sigma^n(\sqrt{J}) \subseteq \sqrt{I}$ for all $n \in \mathbb{Z}$. Let $L = (x^2, xy, y^2, y - x, zt - 1)$. We note that $L \subseteq J$ is σ-invariant. An easy induction shows that

$$\sigma^n(x) \equiv (-1)^{\binom{n-1}{2}} xz^n \pmod{L}$$

for $n \in \mathbb{Z}$, where we interpret z^{-i} as being $t^i \pmod{L}$. Thus $\sigma^n(J) \subseteq I$ if and only if

$$(-1)^{\binom{n-1}{2}} xz^n - u \in L + A\big(x(z - 1)\big) + A(x - u) =: I.$$

Since $x(z - 1) \in I$, this occurs if and only if

$$(-1)^{\binom{n-1}{2}} x - u \in L + A\big(x(z - 1)\big) + A(x - u).$$

Since $x - u \in I$, this occurs when $n \equiv 0, 1 \pmod{4}$. Note that

$$I = L + A\big(x(z - 1)\big) + A(x - u) \subseteq (z - 1, t - 1, x^2, y, x - u)$$

and

$$A/(z - 1, t - 1, x^2, y, x - u) \cong K[x]/(x^2).$$

The image of $(-1)^{\binom{n-1}{2}} x - u$ under this homomorphism is $(-1)^{\binom{n-1}{2}} x - x + (x^2)$, which has nonzero image for $n \equiv 2, 3 \pmod{4}$. Hence we have two arithmetic progressions $n \equiv 0 \pmod{4}$ and $n \equiv 1 \pmod{4}$ for which $\sigma^n(J) \subseteq I$. Equivalently, $\sigma^n(I) \supseteq J$ if and only if $n \equiv 0, 3 \pmod{4}$. We already saw that $\sigma^n(\sqrt{I}) \supseteq \sqrt{J}$ for all n. Finally, note that we always have $\sigma^n(\sqrt{J}) \not\subseteq I$, since $\sqrt{J}$ is σ-stable and $x \notin I$. ∎

We next consider finitely generated commutative K-algebras A having a nontrivial radical. We give two examples of automorphisms of algebras with nonzero radicals for which the radical affects the dynamics nontrivially. We begin with a simple example that shows that an automorphism of a ring whose action is trivial on the reduced ring can still produce nontrivial dynamics.

Example 6.2 Let K be a field of characteristic 0 and let $A = K[x, y, z]/(x, y)^3$. Let $\sigma\colon A \to A$ be the automorphism given by $\sigma(x) = y$, $\sigma(y) = x$, $\sigma(z) = z$. Let $I = (x)$

and $J = (y)$. Then
$$\sigma^n(I) \supseteq J \text{ if and only if } n \equiv 1 \pmod{2}.$$

Proof This holds by inspection. The point of this example is that σ induces the trivial automorphism on $K[z] \cong A/J(A)$, where $J(A)$ denotes the radical of the zero ideal. ∎

We next give an example of an automorphism of a non-reduced ring A with suitable ideals exhibiting nontrivial dynamics, consisting of infinite arithmetic progressions, on both A and its reduction $A/J(A)$, but the dynamics differ.

Example 6.3 Let K be a field of characteristic 0, and let
$$A = K[u, v, y, y^{-1}, z, z^{-1}]/(u, v)^3.$$
We let $\sigma\colon A \to A$ be the automorphism given by $\sigma(u) = uy$, $\sigma(v) = vz$, $\sigma(y) = -y$, $\sigma(z) = z$. Let
$$J = (u + v), \qquad I = (y - 1, z - 1, u + v).$$
Then
$$\sigma^n(I) \supseteq J \text{ if and only if } n \equiv 0, 3 \pmod{4}.$$

Proof We have
$$\sigma^n(J) = \left((-1)^{\binom{n-1}{2}} uy^n + vz^n\right),$$
which is contained in I if and only if $\binom{n-1}{2} \equiv 0 \pmod{2}$. This occurs exactly when $n \equiv 0, 1 \pmod{4}$. The result follows. ∎

In Example 6.3 the ring A is non-reduced and the arithmetic progressions that occur each have "gaps" of length 4. However, when one studies the action of the automorphism σ on the reduced ring $A/J(A) \simeq K[y, y^{-1}, z, z^{-1}]$ one sees that it has order 2, so that its action on the reduced ring for any ideals I, J will have orbits that decompose into arithmetic progressions whose gaps have length 1 or 2 along with a finite set; in Example 6.3 it is all integers n, since $J \subseteq J(A)$. An interesting question is whether the "gaps" between the two cases can be bounded in terms of the size of the gaps that occur from the induced action on the reduced ring and the degree of nilpotency of the radical ideal.

We conclude with examples showing that the hypotheses that the commutative K-algebra A must be finitely generated over K and that K must have characteristic zero, are both needed for the truth of the theorems above.

Example 6.4 Let K be a field and let S be an arbitrary subset of the integers. Then there exists a commutative K-algebra $A = A_S$ that is not Noetherian and is infinitely generated over K, having the property that it has an automorphism σ and ideals I and J such that $\sigma^i(I) \supseteq J$ holds if and only if $i \in S$.

Proof Let $A = K[x_n : n \in \mathbb{Z}]$ be a polynomial ring in infinitely many variables and let σ be the two-sided shift automorphism defined by $\sigma(x_i) = x_{i+1}$ for $i \in \mathbb{Z}$. Given a subset S of integers, we let $P_S = (x_i \mid -i \in S)$. Then $\sigma^i((x_0)) \subseteq P_S$ if and only if $-i \in S$, and so $\sigma^n(P_S) \supseteq (x_0)$ precisely when $n \in S$. ∎

If we impose the extra requirement that A be Noetherian, but allow it to be infinitely generated, there are nontrivial restrictions on the allowable sets $S \subset \mathbb{Z}$ giving ideal inclusions. A result of Farkas [15, Theorem 8] (applied with $G = \mathbb{Z}$) shows that if A is Noetherian and ϕ is an endomorphism of A, then the set of natural numbers i such that $\phi^i(I) \subseteq J$ must either be the entire set of natural numbers, or else must have a *syndetic* complement; that is, there exists a natural number d such that if m is in the complement then there exists j with $1 \leq j \leq d$ such that $m + j$ is also in the complement. For K a field of characteristic 0, we do not know any example of an infinitely generated Noetherian commutative K-algebra A with ideals such that the set S is not a finite union of arithmetic progressions, possibly augmented by a finite set.

Our final example shows that the hypothesis that the ground field K have characteristic zero is necessary for Theorem 1.7 to hold. In 1953, Lech [20] gave a counterexample in positive characteristic p, and we observe that it applies at the level of ideals.

Example 6.5 (Lech) Let p be a prime, let $K = \mathbb{F}_p(t)$ for the finite field $\mathbb{F}_p$, and let $A = K[x, y]$. Define $\sigma\colon A \to A$ by $\sigma(x) = tx$ and $\sigma(y) = (1 + t)y$. Take

$$J = (x + y - 1), \qquad I = (x - 1, y - 1).$$

Then $\sigma^n(I) \supseteq J$ if and only if $n \in \{-1, -p, -p^2, \dots\}$.

Proof We show the equivalent assertion $\sigma^n((x-y+1)) \subseteq (x-1, y-1)$ if and only if $n \in \{1, p, p^2, \dots\}$. Note that $\sigma^n(x - y + 1) = t^n x - (1+t)^n y + 1$, whence we have the ideal inclusion $\sigma^n((x-y+1)) \subseteq (x-1, y-1)$ if and only if $t^n - (1+t)^n + 1 = 0$. This equation holds if and only if n is a power of p. ∎

In the case K has characteristic $p > 0$, Derksen [12] has further shown that if σ is a linearizable endomorphism of $A = K[x_1, \dots, x_d]$, then for ideals I and J of A, the set of m such that $\sigma^m(I) \subseteq J$ can be classified; in particular this set is always a p-*automatic set*, as defined in Allouche and Shallit [1].

Appendix A Dynamics of Endomorphisms—Geometric versus Algebraic

This appendix presents a result addressing the difference between the geometric and algebraic formulations of dynamics of endomorphisms. This result relates the geometric action of endomorphisms acting as dynamical evaluation maps f_τ on S^d by forward iteration versus the algebraic action of endomorphisms τ acting on ideals in $R = S[x_1, \dots, x_d]$ by backward iteration. It shows that the two actions differ in some circumstances.

To state the result, suppose that S is an integral domain, take $R = S[x_1, \dots, x_d]$ and let U be a subset of R. The set of S-points cut out by U in S^d is

$$V(U) := V_S(U) = \{\mathbf{s} = (s_1, \dots, s_d) \in S^d : \mathrm{ev}_{\mathbf{s}}(p(x)) = 0 \text{ for all } p(x) \in U\}.$$

Of course $V(U) = V(I(U))$, where $I(U)$ is the smallest ideal containing U. Note that for endomorphisms τ and ideals I that $\tau^{-1}(I)$ is an R-ideal, while

$$\tau(I) := \{\tau(p(x)) : p(x) \in I\}$$

need not be an R-ideal.

Proposition A.1 *Let S be an integral domain of any characteristic, and consider the polynomial ring $R = S[x_1, \dots, x_d]$. Let $\tau\colon R \to R$ be a S-algebra endomorphism of R. Consider the following possible relations between ideals I and J of R, the S-algebra endomorphism τ, and the dynamical evaluation map f_τ:*

(i) $\tau^{-1}(I) \supseteq J$, *in the ring R;*
(ii) $I \supseteq \tau(J)$, *in the ring R;*
(iii) $V(I) \subseteq V(\tau(J))$ *in S^d;*
(iv) $f_\tau(V(I)) \subseteq V(J)$ *in S^d;*
(v) $V(I) \subseteq (f_\tau)^{-1}(V(J))$ *in S^d.*

Then the following hold:

(a) *We have* (i) $\Leftrightarrow$ (ii) *and* (iii) $\Leftrightarrow$ (iv) $\Leftrightarrow$ (v). *In addition* (ii) $\Rightarrow$ (iii)*, however, in general* (iii) $\not\Rightarrow$ (ii).
(b) *If $S = K$ is an algebraically closed field of any characteristic and I is a radical ideal, then* (iii) $\Leftrightarrow$ (ii). *In this case all five relations* (i)–(v) *are equivalent.*

This proposition shows that for endomorphisms τ the obstruction to the equivalence of all five of these properties is (iii) $\not\Rightarrow$ (ii), which concerns *non-radical ideals* I. This difference matters at the level of the generalized SML Theorem for ideal inclusion (Theorem 1.7) in that it can change the allowed arithmetic progressions for inclusion relations of ideals I, I' having the same radical ideal $\sqrt{I} = \sqrt{I'}$ with a fixed J; *cf.* Example 6.1.

Proof Let τ be an S-algebra endomorphism of $R = S[x_1, \dots, x_d]$.

(a). (i) $\Leftrightarrow$ (ii). For any $U \subseteq R$, set $\tau^{-1}(Y) := \{r(x) \in R : \tau(r(x)) \in U\}$. Then we have the inclusions

$$\tau \circ \tau^{-1}(U) \subseteq U \subseteq \tau^{-1} \circ \tau(U).$$

Furthermore, if $\tau := \sigma$ is an automorphism, then equality holds in both inclusions. Suppose $\tau^{-1}(I) \supseteq J$. We apply τ to both sides to obtain

$$I \supseteq \tau \circ \tau^{-1}(I) \supseteq \tau(J).$$

Conversely, given $I \supseteq \tau(J)$, applying τ^{-1} to both sides gives

$$\tau^{-1}(I) \supseteq \tau^{-1} \circ \tau(J) \supseteq J.$$

(ii) $\Rightarrow$ (iii). We are given $I \supset \tau(J)$. Now suppose that $\mathbf{s} \in V(I) = V_S(I)$, and we are to show that $\mathbf{s} \in V(\tau(J))$. The hypothesis asserts that $\mathrm{ev}_{\mathbf{s}}(q(\mathbf{x})) = 0$ for all $q(\mathbf{x}) \in I$. The conclusion asserts that

$$\tau(p)(\mathbf{s}) := \mathrm{ev}_{\mathbf{s}}(\tau(p)(\mathbf{x})) = 0 \quad \text{for all} \quad p(\mathbf{x}) \in J.$$

To verify this, the inclusion $\tau(J) \subseteq I$ gives

$$\tau(p)(x) = p\big(\tau(x_1), \dots, \tau(x_d)\big) =: q(\mathbf{x}),$$

https://doi.org/10.4153/CJM-2013-048-3 Published online by Cambridge University Press

for some $q(\mathbf{x}) \in I$. Now

$$\mathrm{ev}_{\mathbf{s}}\big(\tau(p)\big)(\mathbf{x}) = p\big(\mathrm{ev}_{\mathbf{s}}\big(\tau(x_1)\big), \dots, \mathrm{ev}_{\mathbf{s}}\big(\tau(x_d)\big)\big)$$

and by definition $\mathrm{ev}_{\mathbf{s}}\big(\tau(x_1), \dots, \tau(x_d)\big) = f_\tau(\mathbf{s})$. We conclude

$$\mathrm{ev}_{\mathbf{s}}\big(\tau(p)(\mathbf{x})\big) = \mathrm{ev}_{f_\tau(s)}\big(p(\mathbf{x})\big).$$

Now $\mathbf{s} \in V(I)$ gives $q(\mathbf{s}) = 0$, whence

$$\begin{aligned} 0 = q(\mathbf{s}) := \mathrm{ev}_{\mathbf{s}}\big(q(\mathbf{x})\big) &= \mathrm{ev}_{\mathbf{s}}\big(p\big(\tau(x_1), \dots, \tau(x_d)\big)\big) \\ &= p\big(\mathrm{ev}_{\mathbf{s}}\big(\tau(x_1), \dots, \tau(x_d)\big)\big) = \mathrm{ev}_{f_\tau(s)}\big(p(\mathbf{x})\big) \end{aligned}$$

Since this holds for all $p(\mathbf{x}) \in J$, we have $\mathbf{s} \in V(\tau(J))$.

(iii) $\Leftrightarrow$ (iv). Let $\mathbf{s} \in S^d$. The key property is the identity, valid for all $r(\mathbf{x}) = r(x_1, \dots, x_d) \in R$, that

$$\mathrm{ev}_{\mathbf{s}}\big(\tau\big(r(x_1, \dots, x_d)\big)\big) = \mathrm{ev}_{\mathbf{s}}\big(r(\tau(x_1)), \dots, r(\tau(x_d))\big) = \mathrm{ev}_{f_\tau(\mathbf{s})}(r(x)).$$

In what follows we abbreviate $r(\mathbf{s}) := \mathrm{ev}_{\mathbf{s}}(r(x_1, \dots, x_d))$.

Suppose $V(I) \subseteq V(\tau(J))$. If $\mathbf{s} \in V(I)$, then $q(\mathbf{s}) = 0$ for all $q(x) \in I$. We are to show that $f_\tau(V(I)) \subseteq V(J)$, which asserts that for all $p(x) \in J$ there holds $p(f_\tau(\mathbf{s})) := \mathrm{ev}_{f_\tau(\mathbf{s})}(p(x)) = 0$. Here, using the equality above,

$$\mathrm{ev}_{f_\tau(\mathbf{s})}\big(p(\mathbf{x})\big) = \mathrm{ev}_{\mathbf{s}}\big(\tau(p)(\mathbf{x})\big) =: \tau\big(p(\mathbf{s})\big).$$

Now $\tau(p(\mathbf{s})) = 0$, because $V(I) \subset V(\tau(J))$.

Conversely, suppose , $f_\tau(V(I)) \subseteq V(J)$ in S^d. We must show that $V(I) \subset V(\tau(J))$. Given $\mathbf{s} \in V(I)$, we must show that for each $p(x) \in J$,

$$\tau(p)(\mathbf{s}) := \mathrm{ev}_{\mathbf{s}}\big(\tau(p)(\mathbf{x})\big) = 0.$$

Using the identity above, $\mathrm{ev}_{\mathbf{s}}(\tau(p)(\mathbf{x})) = \mathrm{ev}_{f_\tau(\mathbf{s})}(p(\mathbf{x}))$. But by hypothesis, $f_\tau(\mathbf{s}) \in V(J)$, whence

$$p\big(f_\tau(\mathbf{s})\big) := \mathrm{ev}_{f_\tau(\mathbf{s})}\big(p(\mathbf{x})\big) = 0,$$

as required.

(iv) $\Leftrightarrow$ (v). For any subset $\mathcal{N} \subset S^d$, set $f_\tau^{-1}(\mathcal{N}) = \{\mathbf{s} \in S^d : f_\tau(\mathbf{s}) \in \mathcal{N}\}$. Then we have the inclusions

$$f_\tau \circ f_\tau^{-1}(\mathcal{N}) \subseteq \mathcal{N} \subseteq f_\tau^{-1} \circ f_\tau(\mathcal{N}).$$

Furthermore if $\tau := \sigma$ is an automorphism, we have equality in both inclusions, for in this case f_σ is a bijection with inverse $f_{\sigma^{-1}}$. The argument is similar to (i) $\Leftrightarrow$ (ii). Suppose $f_\tau(V(I)) \subset V(J)$. Applying f_τ^{-1} yields

$$V(I) \subseteq f_\tau^{-1} \circ f_\tau\big(V(I)\big) \subseteq f_\tau\big(V(J)\big).$$

Conversely, suppose $V(I) \subseteq f_\tau^{-1}(V(J))$. Applying f_τ^{-1} yields

$$f_\tau(V(I)) \subseteq f_\tau \circ f_\tau^{-1}(V(J)) \subseteq V(J).$$

(iii) $\not\Rightarrow$ (ii). This is well known. Take $R = K[x]$, for K a field and $\tau(x) = x^3$. Take $I = (x^4)$ and $J = (x)$. Then $x^3 \in \tau(J) \subset (x^3)$, so that $V(I) = V(\tau(J)) = \{0\}$, and $V(I) \subseteq V(\tau(J))$. But $x^3 \notin I$, so $I \not\supseteq \tau(J)$. (Note also that

$$\tau(J) = \{\tau(p)(x) : p(x) \in J\}$$

is not an R-ideal.)

(b). The assertion (iii) $\Rightarrow$ (ii) when $S = K$ is an algebraically closed field (of any characteristic) and I is a radical ideal is the Nullstellensatz. This gives all the equalities (i)–(v). No condition is imposed on the ideal J to get the equality. ∎

Remark A.2 The failure of the methods of this paper to handle general endomorphisms arises not from Proposition A.1, but rather from the failure of the generalized p-adic analytic arc theorem to apply to certain endomorphisms.

Acknowledgments We thank Harm Derksen for comments on the nonzero characteristic case and Brian Conrad for comments on the scheme theory viewpoint. We thank the reviewer for helpful comments.

References

[1] J.-P. Allouche and J. Shallit, *Automatic sequences. Theory, applications, generalizations.* Cambridge University Press, Cambridge, 2003

[2] A. S. Amitsur, *Algebras over infinite fields.* Proc. Amer. Math. Soc. **7**(1956), 35–48. http://dx.doi.org/10.1090/S0002-9939-1956-0075933-2

[3] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, ON, 1969.

[4] J. P. Bell, *A generalised Skolem–Mahler–Lech theorem for affine varieties.* J. London Math. Soc. **73**(2006), no. 2, 367–379. http://dx.doi.org/10.1112/S002461070602268X

[5] J. P. Bell, *Corrigendum to: "A generalised Skolem–Mahler–Lech theorem for affine varieties".* J. London Math. Soc. **78**(2008), 267–272. http://dx.doi.org/10.1112/jlms/jdn012

[6] J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell-Lang problem for étale maps.* Amer. J. Math. **132**(2010), no. 6, 1655–1675.

[7] R. L. Benedetto, D. Ghioca, P. Kurlberg, and T. J. Tucker, *A case of the dynamical Mordell-Lang conjecture.* Math. Ann. **352**(2012), no. 1, 1–26. http://dx.doi.org/10.1007/s00208-010-0621-4

[8] J.-P. Bézivin, *Une généralisation du théorème de Skolem-Mahler-Lech.* Quart. J. Math. Oxford Ser. (2) **40**(1989), no. 158, 133–138. http://dx.doi.org/10.1093/qmath/40.2.133

[9] P. J. Cahen and J.-L. Chabert, *Integer-valued polynomials.* Mathematical Surveys and Monographs, 48, American Mathematical Society, Providence, RI, 1997.

[10] J. W. S. Cassels, *Local fields*. London Mathematical Society Student Texts, 3, Cambridge University Press, Cambridge, 1986.

[11] L. Denis, *Géométrie et suites récurrentes.* Bull. Soc. Math. France **122**(1994), no. 1, 13–27.

[12] H. Derksen, *A Skolem-Mahler-Lech theorem in positive characteristic and finite automata.* Invent. Math. **168**(2007), no. 1, 175–224. http://dx.doi.org/10.1007/s00222-006-0031-0

[13] D. Eisenbud, *Commutative algebra. With a view towards algebraic geometry.* Graduate Texts in Mathematics, 150, Springer-Verlag, New York, 1995.

[14] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*. Mathematical Surveys and Monographs, 104, American Mathematical Society, Providence, RI, 2003.

[15] D. R. Farkas. *Recurrent behavior in rings.* J. Algebra **108**(1987), no. 1, 127–138. http://dx.doi.org/10.1016/0021-8693(87)90126-8

[16] D. Ghioca and T. J. Tucker, *Periodic points, linearizing maps, and the dynamical Mordell-Lang problem.* J. Number Theory **129**(2009), no. 6, 1392–1403. http://dx.doi.org/10.1016/j.jnt.2008.09.014

[17] D. Ghioca, T. J. Tucker, and M. E. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell-Lang conjecture.* Invent. Math. **171**(2008), no. 2, 463–483. http://dx.doi.org/10.1007/s00222-007-0087-5

[18] G. Hansel, *Une démonstration simple du théorème de Skolem-Mahler-Lech.* Theoret. Comput. Sci. **43**(1986), no. 1, 91–98. http://dx.doi.org/10.1016/0304-3975(86)90168-4

[19] R. Hartshorne, *Algebraic geometry*. Graduate Texts in Mathematics, 52, Springer-Verlag, New York, 1977.

[20] C. Lech, *A note on recurring series.* Ark. Mat. **2**(1953), 417–421. http://dx.doi.org/10.1007/BF02590997

[21] K. Mahler, *Eine arithmetische Eigenshaft der Taylor-Koeffizienten rationaler Funktionen,* Proc. Kon. Nederlandsche Akad. v. Wetenschappen, **38**(1935), 50–60.

[22] ———, *On the Taylor coefficients of rational functions.* Proc. Cambridge Philos. Soc. **52**(1956), 39–48. http://dx.doi.org/10.1017/S0305004100030966

[23] ———, *Addendum to the paper "On the Taylor coefficients of rational functions".* Proc. Cambridge Philos. Soc. **53**(1957), 544. http://dx.doi.org/10.1017/S0305004100032552

[24] ———, *p-adic numbers and their functions.* Second ed., Cambridge Tracts in Mathematics, 76, Cambridge University Press, Cambridge, New York, 1981.

[25] B. Poonen, *p-adic interpolation of iterates.* arxiv:1307.5887

[26] S. J. Sierra, *Geometric idealizer rings.* Trans. Amer. Math. Soc. **363**(2011), no. 1, 457–500. http://dx.doi.org/10.1090/S0002-9947-2010-05110-4

[27] T. Skolem, *Einige Sätze über gewisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf Diophantische Gleichungen.* Skrifter Norske Vidensk. Acad. Oslo, Mat. Naturv. Klasse (1933), no. 6.

[28] ———, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen.* C. r. 8 congr. scand. à Stockholm (1934), 163–188.

[29] V. Srinivas, *On the embedding dimension of an affine variety.* Math. Ann. **289**(1991), no. 1, 125–132. http://dx.doi.org/10.1007/BF01446563

[30] R. Strassman, *Über den Wertevorrat von Potenzreihen im Gebiet der p-adischen Zahlen.* J. Reine Angew. Math. **159**(1928), 13–28; 65–66.

[31] A. J. van der Poorten, *Some facts that should be better known; especially about rational functions.* In: Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 265, Kluwer Academic Publishers, Dordrecht, 1989, pp. 497–528.

[32] A. J. van der Poorten and R. Tijdeman, *On common zeros of exponential polynomials.* Enseignement Math. (2) **21**(1975), no. 1, 57–67.

[33] S.-W. Zhang, *Distributions in algebraic dynamics.* Surv. Differ. Geom. **10**(2006), 381–430.

Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2L 3G1
e-mail: jpbell@uwaterloo.ca

Department of Mathematics, University of Michigan,, Ann Arbor, MI 48109-1043, USA
e-mail: lagarias@umich.edu