Utrecht University
Faculty of Science
Department of Mathematics

Dynamics on Algebraic Groups

Master's Thesis

Author
Marc Houben

Supervisor
prof. dr. Gunther Cornelissen

Second Reader
dr. Damaris Schindler

July 2018

Abstract

Using the Artin-Mazur dynamical zeta function, we study the periodic behavior of discrete dynamical systems arising from algebraic groups over algebraically closed fields k of characteristic $p > 0$.

Of particular interest are maps arising as finite quotients of affine morphisms on algebraic groups; so-called dynamically affine maps. For a dynamically affine map f on an algebraic variety V over k, we present a set of hypotheses that imply that the corresponding dynamical zeta function ζ_f is either a root of a rational function, or has a natural boundary. By verifying the hypotheses in the special case where V is the projective line, this generalizes recent work by Bridy. Under slightly weaker assumptions, we show that the *tame* dynamical zeta function ζ_f^*, formed by ignoring orbits whose order is divisible by p, is always a root of a rational function.

We work towards a conjectural description of the orbit structure for a discrete dynamical system (G, σ), where σ is an endomorphism of a connected algebraic group G over k. This extends recent work by Byszewski and Cornelissen for the case that G is an abelian variety.

Acknowledgements

Most importantly, I would like to thank my supervisor prof. Gunther Cornelissen for his guidance during the past nine months. Our regular meetings were always a great source of inspiration and motivation. What especially struck me was his extremely open-minded attitude: he always listened to my progress with complete attention. Instead of quickly dismissing an incorrect idea, he often managed to guide it into a correct direction. He closely monitored my work, but also gave me complete freedom to pursue the path I felt was most interesting, keeping me productive and, most of all, enthusiastic during the entire project.

I would also like to thank dr. Jakub Byszewski for our fruitful conversations during the time he was in Utrecht, and for taking a suitably critical attitude towards my work. Working with him was a very inspiring and rewarding experience.

Furthermore, I would like to thank dr. Damaris Schindler for taking the time to be my second reader.

Finally, I would like to express my gratitude to my friends and family for their support and encouragement over the past year.

Contents

1 Introduction

A *discrete dynamical system* is, in its most general form, a set S together with a map $f : S \to S$. Usually, the set S has some structure (e.g. S could be a topological space, an abstract group or a smooth manifold), and f is a morphism preserving that structure (e.g. a continuous function, a group homomorphism or a smooth map). When studying discrete dynamics, one is often interested in *periodic points*, i.e. fixed points of some iterate of f. A natural way to begin a quantitative analysis of the structure of a discrete dynamical system is therefore to consider the *fixed point sequence* $(f_n)_{n\geq 1}$, defined by

$$f_n := \#\operatorname{Fix}(f^{\circ n}) = \#\{x \in S \mid \underbrace{f \circ \cdots \circ f}_{n \text{ times}}(x) = x\}.$$

Let us say that the map f is *confined* when f_n is finite for all $n \in \mathbf{Z}_{>0}$. If this is the case, we can encapsulate the fixed point sequence in the form of a formal power series, called the *dynamical zeta function* ζ_f [41, p. 764], given by

$$\zeta_f(z) := \exp\left(\sum_{n\geq 1} \frac{f_n}{n} z^n\right). \tag{1}$$

The dynamical zeta function is sometimes also refered to as the *Artin-Mazur zeta function*, named after Michael Artin and Barry Mazur [4], as they employed it to study the asymptotic behaviour of isolated periodic points of diffeomorphisms on manifolds. In this thesis, however, we will be mainly interested in the case (sometimes referred to as *algebraic dynamics* [46]) where the set S is the set of (closed) points of an algebraic variety X over an algebraically closed field k (and f is a morphism of algebraic varieties).[1]

Before diving into dynamics on algebraic varieties, let us consider an example of a *finite* discrete dynamical system.

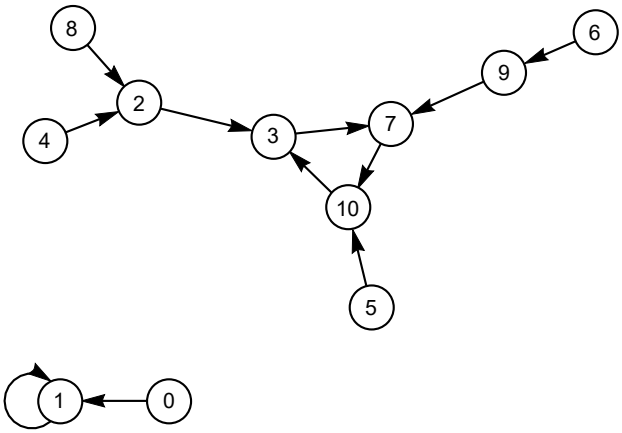


Figure 1: The graph associated to a finite discrete dynamical system.

[1] Although it should be noted that the main situation in the work of Artin and Mazur is, perhaps unexpectedly, quite similar to ours: an important tool they use is the theory of real algebraic approximations by Nash [34], allowing them to reduce the study of diffeomorphisms on manifolds to that of morphisms of Nash manifolds, thus landing in a (semi-)algebraic setting.

Example 1.1 Let $S := \mathbf{F}_{11}$, the finite field of 11 elements, and let $f : \mathbf{F}_{11} \to \mathbf{F}_{11}$ be the polynomial map given by $f(x) := x^2 - x + 1$. Then we can picture (see Figure 1) the dynamical system (S, f) by a directed graph. Here the vertices of the graph are the elements of $\mathbf{F}_{11}$, and for every point x there is a directed edge pointing from x to $f(x)$. We can read off from the picture that the fixed point sequence is given by

$$f_n = \begin{cases} 4 & \text{if } 3 \mid n; \\ 1 & \text{if } 3 \nmid n. \end{cases}$$

From this information we can compute the dynamical zeta function, which turns out to be rational:

$$\zeta_f(z) = \frac{1}{1-z} \cdot \frac{1}{1-z^3}.$$

☆

Example 1.2 Suppose that X is a quasi-projective algebraic variety defined over a finite field $\mathbf{F}_q$, and that $f : X \to X$ is the q-Frobenius. Then f_n (counted over the algebraic closure) is simply the number of points of X over $\mathbf{F}_{q^n}$, so ζ_f becomes the *Weil zeta function* of $X/\mathbf{F}_q$. It is known that ζ_f is in this case rational by Dwork [18] and Grothendieck [21, Cor. 5.2]. ☆

Example 1.3 Suppose that $X = \mathbf{P}^1/\mathbf{C}$; the projective line over the field of complex numbers, and that $f : X \to X$ is any rational map of degree at least two. Hinkkanen [24, Thm. 1] showed that ζ_f is then rational. This result can be extended to any algebraically closed field k of characteristic zero using, e.g. the Lefschetz principle [26, p. 224]; [19] (indeed, by simultaneously embedding the coefficients of f into $\mathbf{C}$, we can determine f_n by solving the same problem for a rational function with complex coefficients). ☆

The general question that arises, in our case for a confined endomorphism f of an algebraic variety X over an algebraically closed field k, is:

Q: *What is the nature of the dynamical zeta function ζ_f?*

For example, is it (generically) rational? [41, Question 4.5]; [28], or perhaps just algebraic over $\mathbf{C}(z)$? [4, Question 2] Does it have (many) singularities as a complex function? [5]; [10]. It turns out that these questions are, in general, difficult to answer. This might be as expected, since the very special case of Example 1.2 already turned out to be quite hard (indeed, starting from the Weil conjectures [48], it took about ten years to solve, but the case for curves had already been conjectured 25 years before that by Artin [3], and the origin of the problem can even be traced back to Gauss [29]). The general philosophy is that rationality of the zeta function tells us that the periodic behavior of the map f is, in a sense, *regular*. In particular, it implies that the fixed point sequence (f_n) is linear recurrent (Proposition 2.2). Given the examples seen so far, one might expect dynamical zeta functions of morphisms of varieties to always be rational, but this is far from the case. In fact, one can determine, as we will see in Section 3, that for a certain special class of maps (called *dynamically affine maps*) on the projective line in *positive* characteristic, rationality is the *exception* rather than the rule.[2] The following example involves such a special map.

[2]Perhaps we should stress here that we are counting the sequence (f_n) of fixed points *without* multiplicity. If we were to include multiplicities, the story would be quite different; then, for any map $f : \mathbf{P}^1 \to \mathbf{P}^1$ of degree at least two, we "obtain" $f_n = \deg(f)^n + 1$, thus yielding a rational zeta function $\zeta_f(z) = (1-z)^{-1}(1-\deg(f)z)^{-1}$. In fact, the "exceptional" maps within the special class referred to above that have a rational zeta function, turn out to be precisely the ones for which the fixed points of all iterates of f occur with multiplicity one. Over $\overline{\mathbf{F}}_p$, these are precisely the maps (within the special class) for which f is inseparable, which is indeed a non-generic condition.

Example 1.4 Let $X = \mathbf{P}^1/\overline{\mathbf{F}_p}$ for some prime number p, and let $f : \mathbf{P}^1 \to \mathbf{P}^1$, $x \mapsto x^m$ for some integer $m \in \mathbf{Z}$ with $|m| \geq 2$. If $p \nmid m$, then ζ_f is transcendental over $\mathbf{Q}(z)$, while if $p \mid m$, then ζ_f is rational [8, Thm. 1]. ☆

The nature of the zeta function for general maps, even on $\mathbf{P}^1/\overline{\mathbf{F}_p}$, remains a mystery. Let us illustrate, in the form of a non-rigorous discussion, the behavior of some "generic" maps on the projective line. First, consider $f : \mathbf{P}^1/\overline{\mathbf{F}_p} \to \mathbf{P}^1/\overline{\mathbf{F}_p}$, $f(x) = x^2 + 1$, for which, if $p \geq 5$, we do not know whether the corresponding dynamical zeta function ζ_f is rational or not. Since the projective line is an infinite set, we unfortunately cannot draw a directed graph for f similar to the one we saw in Figure 1. However, $\mathbf{P}^1/\overline{\mathbf{F}_p} = \bigcup_{n\geq 1} \mathbf{F}_{p^n} \cup \{\infty\}$, so the behaviour of the dynamical system $(\mathbf{P}^1, f)$ is in a sense *approximated* by the behaviour of the map f over finite fields.[3]

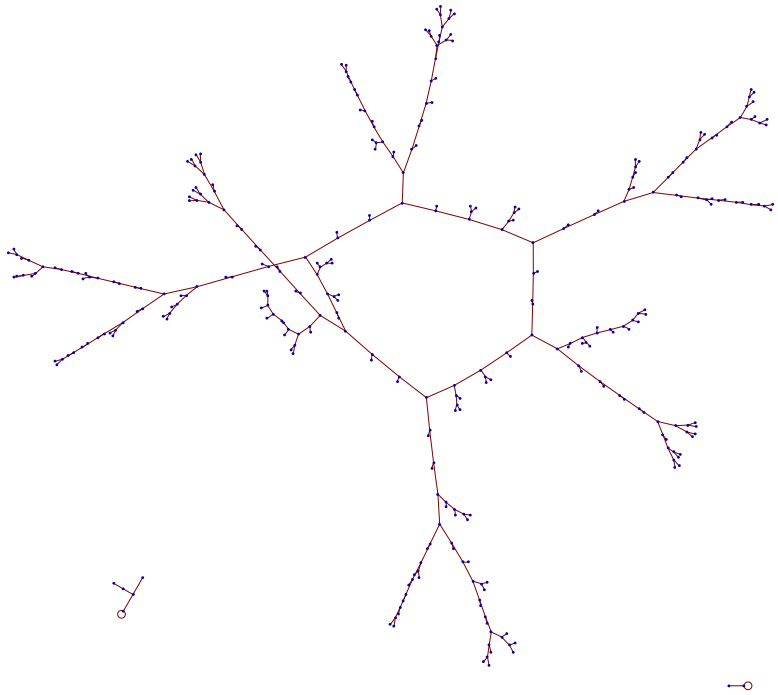
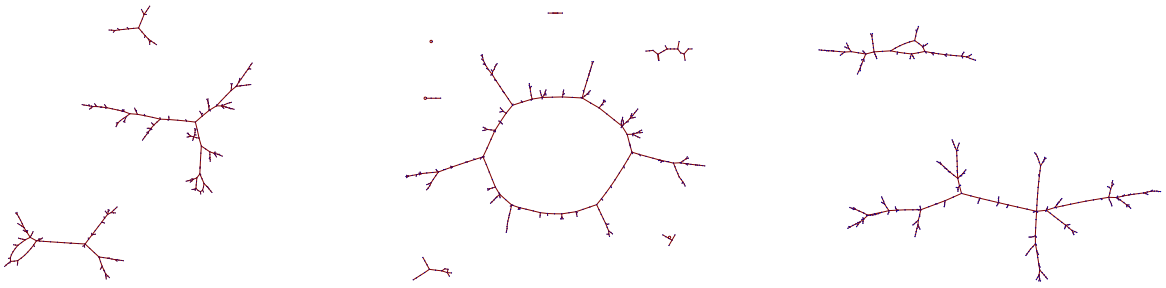


Figure 2: The map $x^2 + 1$ on $\mathbf{F}_{7^3}$.

In Figure 2 we have plotted the graph (in the same spirit as for Figure 1, but without labels on the vertices and without arrows on the edges) associated to the map f on $\mathbf{F}_{7^3}$. What one might immediately notice is that the graph appears to be quite "random". This is especially striking when we compare it to graphs of actually random[4] maps $\mathbf{F}_{7^3} \to \mathbf{F}_{7^3}$, found in Figure 3.

[3] In fact, since the equation $f^{\circ n}(x) = x$ is polynomial of degree $\deg(f)^n$, we can calculate f_n by only considering points lying in the finite fields $\mathbf{F}_{p^m}$ up to $m = \deg(f)^n$.

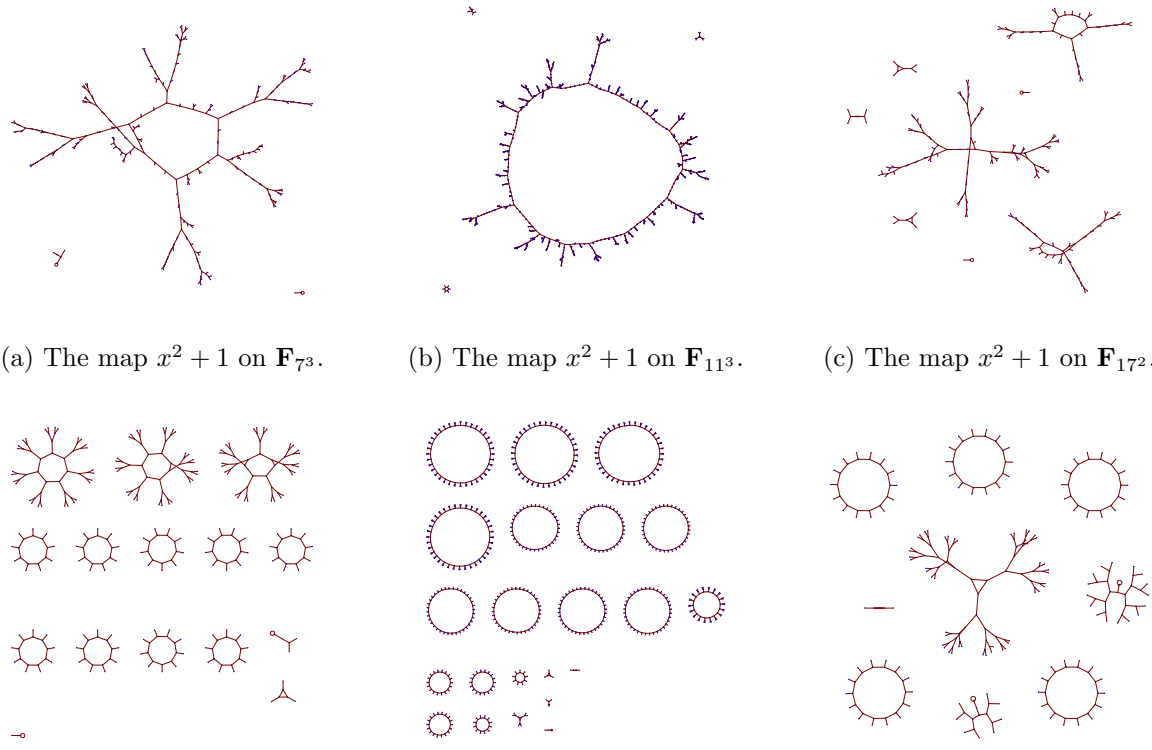
[4] Random in the sense that for every element $x \in \mathbf{F}_{7^3}$, we select a (computer-generated) random element $f(x) \in \mathbf{F}_{7^3}$.



(a) (b) (c)

Figure 3: Three random maps on $\mathbf{F}_{7^3}$.

Due to the irregular (seemingly random) nature of the map x^2+1 on $\mathbf{P}^1/\overline{\mathbf{F}_p}$, we would definitely expect the corresponding dynamical zeta function to be irrational. However, precisely due to its erratic behaviour, we are, at the moment of writing, unable to control the fixed point sequence (f_n) in any meaningful way (cf. [8, Question 2]). This very much changes when considering the, at first appearance similar, map $g(x) = x^2 - 2$. In Figure 4 we see that the graphs associated to g look quite different compared to the ones for f. This is reflected in our knowledge of the zeta function ζ_g, which, as we will see in Section 3, we can determine to be rational in characteristic 2 and 3, and irrational in characteristic ≥ 5.



(a) The map $x^2 + 1$ on $\mathbf{F}_{7^3}$. (b) The map $x^2 + 1$ on $\mathbf{F}_{11^3}$. (c) The map $x^2 + 1$ on $\mathbf{F}_{17^2}$.

(d) The map $x^2 - 2$ on $\mathbf{F}_{7^3}$. (e) The map $x^2 - 2$ on $\mathbf{F}_{11^3}$. (f) The map $x^2 - 2$ on $\mathbf{F}_{17^2}$.

Figure 4: Comparison of the maps $x^2 + 1$ and $x^2 - 2$ over various finite fields.

Before we can understand what makes g different from f, we will require some definitions. It turns out that the underlying structure that makes g behave in a controlled manner, is that of a hidden *algebraic group*.

Let k denote an algebraically closed field.

Definition 1.5 An *algebraic group* over k is an algebraic variety G/k, together with an identity element $e \in G$, and morphisms $G \times G \to G, (x, y) \mapsto x \cdot y$; $G \to G, x \mapsto x^{-1}$, with respect to which G is a group. △

Example 1.6 As we will see in Section 3.3.1, there are precisely three types of connected algebraic groups of dimension one:

(i) the *multiplicative group* $\mathbf{G}_m(k) \cong k^\times \cong \mathbf{P}^1 \setminus \{0, \infty\}$;

(ii) the *additive group* $\mathbf{G}_a(k) \cong (k, +) \cong \mathbf{P}^1 \setminus \{\infty\}$;

(iii) the *elliptic curves* E. ☆

A morphism of algebraic groups is a morphism of varieties that is also a group homomorphism. If G is commutative, the set $\mathrm{End}(G)$ of endomorphisms of G admits a ring structure, where the multiplication is given by composition and the addition is induced (pointwise) by the group operation.

Definition 1.7 Let $(G/k, +)$ be a commutative algebraic group. An *affine morphism* of G is a map $\psi : G \to G$ that can be written as $\psi(g) = \sigma(g) + h$ for a confined endomorphism with finite kernel $\sigma \in \mathrm{End}(G)$ and some $h \in G$. △

This definition differs slightly from the one established by Silverman [40, §6.8]. We will briefly discuss this choice in Section 3.1.

Definition 1.8 Let V/k be a variety, and let $f : V \to V$ be a morphism. We say that f is *dynamically affine* if there exists

(i) a connected commutative algebraic group G;

(ii) an affine morphism $\psi : G \to G$;

(iii) a finite subgroup $\Gamma \subseteq \mathrm{Aut}(G)$; and

(iv) an inclusion $\iota : G/\Gamma \to V$ that identifies G/Γ with a Zariski-dense open subset of V,

such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\psi} & G \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ G/\Gamma & \longrightarrow & G/\Gamma \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ V & \xrightarrow{f} & V \end{array}$$

△

Example 1.9 Let us consider some dynamically affine maps $V = \mathbf{P}^1$. It follows from the definition that V needs to have the same dimension as the algebraic group G, so we may assume that G is one of the algebraic groups listed in Example 1.6, e.g. let us consider $G = \mathbf{G}_m$. Then $\mathrm{End}(G) = \{x^m \mid m \in \mathbf{Z}\} \cong \mathbf{Z}$, and $\mathrm{Aut}(G) = \{x, x^{-1}\}$, thus leaving two choices for Γ; either $\Gamma \cong \{1\}$ or $\Gamma \cong \{\pm 1\}$. If $\Gamma \cong \{1\}$ then $G/\Gamma \cong \mathbf{P}^1 \setminus \{0, \infty\}$ (which canonically embeds into $\mathbf{P}^1$). The dynamically affine maps f that arise are the "affine power maps" $f(x) = ax^m$ for some $a \in k^\times$. If $\Gamma \cong \{\pm 1\}$, then $G/\Gamma \cong \mathbf{A}^1$, giving rise instead to "Chebyshev polynomials" [39, §6.2]. The map $g(x) = x^2 - 2$ we considered before is the unique Chebyshev polynomial of degree two. ☆

The underlying structure of the algebraic group will be very important in allowing us to control the fixed point sequence (f_n), and hence the dynamical zeta function ζ_f, associated to a dynamically affine map f. Our main result will be stated after the following definition:

Definition 1.10 Let $F \in \mathbf{C}[\![z]\!]$ be a power series over the complex numbers. We will say that F has a *natural boundary* when it has a positive radius of convergence $\rho \in \mathbf{R}_{>0}$, and a dense set of singularities along the boundary ∂D of the disk of convergence $D = \{z \in \mathbf{C} \mid |z| < \rho\}$. △

Theorem A (= Theorem 3.11) *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be a dynamically affine map on the projective line over an algebraically closed field of positive characteristic. Then the following dichotomy holds:*

(i) If $\sigma^n - 1$ is separable for all $n \in \mathbf{Z}_{>0}$, then ζ_f is rational.

(ii) Otherwise, ζ_f has a natural boundary.

This generalizes (as we will see in Section 2.1) a recent result by Andrew Bridy [9]. He proves a similar dichotomy, but with "has a natural boundary" replaced by "is transcendental over $\mathbf{C}(z)$". His proof, which we briefly reflect on in Section 5, relies heavily on *automata theory*. Although we use tools similar to Bridy's in order to control the fixed point sequence (f_n), our eventual argument is different: instead of using automata, our proof is fundamentally complex analytic in nature; much more reminiscent of e.g. [5].

Example 1.11 Let us consider the power maps $f(x) = x^m$ for $m \in \mathbf{Z}_{\geq 2}$, defined on the projective line in characteristic $\mathrm{char}(k) = p \geq 3$, that were first introduced in Example 1.4 (they are dynamically affine by Example 1.9). Then f_n is the number of distinct solutions in $\mathbf{P}^1$ to the equation $x^{m^n} - x = 0$; that is,

$$x = 0, \quad x = \infty \quad \text{or} \quad x^{m^n - 1} = 1.$$

The rightmost equation counts the number of $(m^n - 1)$-th roots of unity in k, which is $(m^n - 1)|m^n - 1|_p$ (here $|\cdot|_p$ denotes the p-adic norm). In case $p \mid m$, we thus see that $f_n = 2 + (m^n - 1) = m^n + 1$, from which it follows that $\zeta_f(z) = (1 - z)^{-1}(1 - mz)^{-1}$ (indeed rational, as claimed in Example 1.4). Now suppose that $p \nmid m$. Denote by s the multiplicative order of m modulo p, i.e. let $s \in \mathbf{Z}_{>0}$ minimal such that $|m^s - 1|_p < 1$. Then $|m^n - 1|_p = 1$ when $s \nmid n$, while

$$m^{sn} - 1 = (1 + (m^s - 1))^n - 1 = \sum_{k=1}^{n} \binom{n}{k} (m^s - 1)^k = n(m^s - 1) + \sum_{k=2}^{n} \binom{n}{k} (m^s - 1)^k.$$

One can show (cf. Proposition 2.16(iii)) by induction on $v_p(n)$ that

$$\left|\sum_{k=2}^{n}\binom{n}{k}(m^s-1)^k\right|_p < |n(m^s-1)|_p,$$

thus $|m^{sn}-1|_p = |n(m^s-1)|_p$, from which we find

$$f_n = \begin{cases} m^n-1 & \text{if } s \nmid n; \\ (m^n-1)|m^s-1|_p|n|_p & \text{if } s \mid n. \end{cases} \tag{2}$$

Therefore the "logarithmic derivative" $\mathcal{Z}_f(z) := z\zeta_f'(z)/\zeta_f(z)$ of the dynamical zeta function satisfies:

$$\begin{aligned} \mathcal{Z}_f(z) &= \sum_{n\geq 1} f_n z^n = \sum_{n\geq 1}(m^n-1)z^n - \sum_{n\geq 1}(m^{sn}-1)z^{sn} + |m^s-1|_p\sum_{n\geq 1}(m^n-1)|n|_p z^n \\ &= \frac{z}{1-mz} - \frac{z}{1-z} - \frac{z}{1-m^s z^s} + \frac{z}{1-z^s} + |m^s-1|_p\left(\sum_{n\geq 1}|n|_p(mz)^n - \sum_{n\geq 1}|n|_p z^n\right). \end{aligned}$$

Now, $\sum_{n\geq 1}|n|_p z^n$ has singularities at all p^k-th roots of unity: this follows from the fact that it satisfies a Mahler-style functional equation (cf. [6]; the details will be provided in Lemma 3.10). From this observation we obtain that $\mathcal{Z}_f$ has a dense set of singularities at the circle of radius $1/m$ around the origin. This circle coincides with the boundary of its disk of convergence (since $\limsup_{n\to\infty}|n|_p^{1/n} = 1$), thus $\mathcal{Z}_f$ has a natural boundary, and we conclude (Lemma 2.1) that the same holds for ζ_f. ☆

An interesting observation is that the natural boundary for the zeta function in Example 1.11 is "caused" solely by the occurrence of terms, in the formula (2) for f_n, depending on $|n|_p$. Indeed, if we were to replace all of the $|n|_p$'s by 1, then $\mathcal{Z}_f(z)$ becomes just an ordinary rational function of z. This turns out to be a general phenomenon: in some sense, the "irregularities" in the sequence (f_n) that cause the zeta function in the second case of Theorem A to have a natural boundary are "contained" in the terms of index divisible by p. This advocates the use of a *tame dynamical zeta function*, as first considered in [10] (for f a confined endomorphism of an algebraic variety over an algebraically closed field of characteristic $p > 0$), defined by

$$\zeta_f^*(z) := \exp\left(\sum_{p\nmid n}\frac{f_n}{n}z^n\right). \tag{3}$$

For the tame dynamical zeta function, have the following result:

Theorem B (= Theorem 3.12) *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be dynamically affine map on the projective line over an algebraically closed field of characteristic $p > 0$. Then the tame dynamical zeta function ζ_f^* is algebraic. In fact, there exists a positive integer $t \in \mathbf{Z}_{>0}$ such that $\left(\zeta_f^*(z)\right)^t \in \mathbf{Q}(z)$.*

Example 1.12 For the special case of the power map considered in Example 1.11, the tame zeta function takes the form

$$\zeta_f^*(z) = \frac{1-z}{1-mz} \cdot \frac{(1-(mz)^p)^{1/p}}{(1-z^p)^{1/p}} \cdot \left(\frac{1-z^s}{1-(mz)^s} \cdot \frac{(1-(mz)^{ps})^{1/p}}{(1-z^{ps})^{1/p}} \right)^{\beta},$$

where $\beta = (|m^s - 1|_p - 1)/s$. ☆

The outline of the thesis will be roughly as follows:

Section 2 will consist of a complete overview of preliminary results. We will discuss some generalities for sequences and power series, focussing in particular on elementary properties of (dynamical) zeta functions. In Section 2.3, we derive some general results regarding discrete valuations, which we will need to control the fixed point sequence (f_n) for dynamically affine maps. We also include, in Section 2.4, a summary of basic results on algebraic groups that we will use later on.

Section 3 will be concerned with the study of dynamically affine maps, including the proof of Theorem A and B. In order to achieve maximal generality, this will be organized based on certain *hypotheses* (introduced in Section 3.2) that can be associated to a dynamically affine map f. We will show that the proofs of the theorems apply, as long as these hypotheses are satisfied, to a general dynamically affine map on an arbitrary variety V. We then obtain the results discussed above as a corollary by verifying (in Section 3.3) that the hypotheses always hold in the special case where V is the projective line.

In Section 4, we turn to a slightly purer point of view: instead of studying the dynamical zeta function of maps *derived from* algebraic groups (as for dynamically affine maps), we will consider the dynamics associated to maps *on* algebraic groups. We work towards the following main conjecture:

Conjecture C (= Conjecture 4.1) *Let σ be a confined endomorphism of a connected (not necessarily commutative) algebraic group G over an algebraically closed field of characteristic $p > 0$. Then the fixed point sequence (σ_n) takes the following form:*

$$\sigma_n = d_n m_n a_n,$$

where, for some $\omega \in \mathbf{Z}_{>0}$ not divisible by p,

(i) there exists an integer $t \in \mathbf{Z}_{>0}$ such that $\exp(\sum_n d_n z^n/n)^t \in \mathbf{Q}(z)$;

(ii) we can write $m_n = r_n |n|_p^{s_n}$, for sequences $r_n \in \mathbf{Q}^\times$ and $s_n \in \mathbf{Z}$ satisfying $r_n = r_{\gcd(\omega,n)}$ and $s_n = s_{\gcd(\omega,n)}$;

(iii) we can write $a_n = p^{|n|_p^{-1} t_n}$ for a sequence $t_n \in \mathbf{Z}$ satisfying $t_n = t_{\gcd(\omega,n)}$.

In Section 5, we will explore ways to simplify and generalize Bridy's proof [9] of his weaker version of Theorem A, and show that it can be applied to find an alternative proof (cf. [10]) of a rational/transcendental dichotomy for the dynamical zeta function of a confined endomorphism of an abelian variety.

Finally, in Section 6, we will explore some questions for further research.

The results of Section 3 and Section 4 of this thesis will be published, in collaboration with Byszewski and Cornelissen, in two separate joint research papers.

2 Preliminaries

2.1 Sequences and Power Series

A power series $F(z) \in \mathbf{C}[\![z]\!]$ is called *holonomic* (sometimes also called *D-finite*) if it satisfies a linear differential equation with coefficients in $\mathbf{C}[z]$. That is, there exists a $d \in \mathbf{Z}_{\geq 0}$ and $p_0(z), \cdots, p_d(z) \in \mathbf{C}[z]$, $p_d \neq 0$, such that

$$p_0(z)F(z) + p_1(z)F'(z) + \cdots + p_d(z)F^{(d)}(z) = 0.$$

A complex function defined by a holonomic power series with non-zero radius of convergence can only have singularities at the roots of p_0, hence in particular has finitely many singularities [20, Thm. 1]. We will say that a power series over the complex numbers with positive radius of convergence $\rho > 0$ has a *natural boundary* if it has a dense set of singularities along the boundary of the disk of convergence $\{z \in \mathbf{C} \mid |z| = \rho\}$. It is called a natural boundary because the complex function defined by such a power series cannot be extended meromorphically beyond its disk of convergence. Note that, by the previous remark, holonomic power series (with positive radius of convergence) cannot have a natural boundary, since a having natural boundary in particular implies having infinitely many singularities. Now, since algebraic power series are holonomic [44, Thm. 6.4.6], we have the following "hierarchy" for power series with positive radius of convergence:

$$\text{rational} \subseteq \text{root-rational} \subseteq \text{algebraic} \subseteq \text{holonomic} \subseteq \text{finite set of singularities} \subseteq \text{no nat. boundary} \quad (4)$$

Here, a power-series F is called *root-rational* if there exists a $t \in \mathbf{Z}_{>0}$ such that F^t is rational. If we want to refer explicitly to the exponent t, then we will say that F is *t-root-rational*.

For a sequence $(a_n)_{n\geq 1}$ of complex numbers, we define the *zeta function* $\zeta_{(a_n)}(z) \in \mathbf{C}[\![z]\!]$ to be the power series given by

$$\zeta_{(a_n)}(z) := \exp\left(\sum_{n\geq 1} \frac{a_n}{n} z^n\right). \quad (5)$$

We define the *naive zeta function* $\mathcal{Z}_{(a_n)}(z) \in \mathbf{C}[\![z]\!]$ corresponding to the sequence (a_n) to be

$$\mathcal{Z}_{(a_n)}(z) := \sum_{n\geq 1} a_n z^n = z\frac{\zeta'_{(a_n)}(z)}{\zeta_{(a_n)}(z)}. \quad (6)$$

Some "properties" seen in the hierarchy (4) pass from the zeta function to the naive zeta function. For example, it follows immediately from (6) that rationality (in the variable z) of $\zeta_{(a_n)}$ implies rationality of $\mathcal{Z}_{(a_n)}$, and similar for algebraicity over $\mathbf{C}(z)$. However, this implication fails for holonomicity, since the multiplicative inverse of a holonomic function is not necessarily holonomic. For example, $F(z) := e^z - 1$ is holonomic, but $1/F(z)$ is not (since it has infinitely many singularities). In fact, if $\zeta_{(a_n)}(z)$ and $1/\zeta_{(a_n)}(z)$ are both holonomic, then $\mathcal{Z}_{(a_n)}(z)$ is necessarily algebraic [23]. On the other hand, having a natural boundary passes from the naive zeta function to the zeta function:

Lemma 2.1 *Let (a_n) be a sequence of complex numbers, and suppose $\mathcal{Z}_{(a_n)}$ has a natural boundary. Then so does $\zeta_{(a_n)}$.*

Proof. [5, Lem. 1]. □

Proposition 2.2 *Let $(a_n)_{n\geq 1}$ be a sequence of complex numbers.*

(i) The following are equivalent:

(a) $(a_n)_{n\geq 1}$ is linear recurrent.

(b) $\mathcal{Z}_{(a_n)}(z) \in \mathbf{C}(z)$.

(c) There exist complex numbers λ_i and polynomials $q_i \in \mathbf{C}[z]$ such that $a_n = \sum_{i=1}^{s} q_i(n)\lambda_i^n$ for all n sufficiently large.

(ii) The following are equivalent:

(a) $\zeta_{(a_n)}(z) \in \mathbf{C}(z)$.

(b) There exist complex numbers λ_i and integers $m_i \in \mathbf{Z}$ such that $a_n = \sum_{i=1}^{s} m_i\lambda_i^n$ for all $n \in \mathbf{Z}_{>0}$.

Furthermore, in case $(a_n)_{n\geq 1}$ is a sequence of rational numbers, then all statements hold with "$\mathbf{C}$" replaced by "$\mathbf{Q}$". Also, we then have $\lambda_i \in \overline{\mathbf{Q}}$.

Proof. (i) This follows from [43, Thm. 4.1.1 & Prop. 4.2.2].

(ii) This is [43, Ex. 4.8].

The final statement follows from the fact that $\mathbf{C}(z) \cap \mathbf{Q}[\![z]\!] \subseteq \mathbf{Q}(z)$ [32, Lem. 27.9]. □

Definition 2.3 The λ_i in Proposition 2.2(i) are called the *roots* of the linear recurrence $(a_n)_{n\geq 1}$. The polynomial $q_i(z)$ is called the *multiplicity* of the root λ_i. A root λ_d of maximal absolute value (as a complex number) among the λ_i is called a *dominant root*. If there is exactly one dominant root (possibly with multiplicity), we say the linear recurrence $(a_n)_{n\geq 1}$ satisfies the *dominant root assumption*. △

Definition 2.4 For two sequences $(a_n)_{n\geq 1}, (b_n)_{n\geq 1}$ of elements of a ring R, we define the *Hadamard product* [22] to be the sequence $(a_n) \odot (b_n) := (a_n b_n)$. △

Proposition 2.2 allows for some interesting remarks regarding root-rationality of the zeta function:

Remark 2.5 (i) A sequence (a_n) of complex numbers has t-root-rational zeta function if and only if we can write $a_n = \sum_{i=1}^{s} q_i\lambda_i^n$ for rational numbers $q_i \in \mathbf{Q}$ with every denominator dividing t.

(ii) The sum $(a_n + b_n)$ of two sequences (a_n), (b_n) with t- and u-root-rational zeta functions respectively has $\mathrm{lcm}(t,u)$-root-rational zeta function.

(iii) The Hadamard product of two sequences (a_n) and (b_n) with t- and u-root-rational zeta functions respectively has (tu)-root-rational zeta function. ♢

Lemma 2.6 *Let $(a_n)_{n\geq 1}$ be a sequence with t-root-rational zeta function and let $m \in \mathbf{Z}_{>0}$. Then*

$$\zeta_1(z) = \exp\left(\sum_{m|n} \frac{a_n}{n} z^n\right), \quad \text{and} \quad \zeta_2(z) = \exp\left(\sum_{m\nmid n} \frac{a_n}{n} z^n\right)$$

are (tm)-root-rational.

Proof. Note that

$$\exp\left(\sum_{m|n}\frac{a_n}{n}z^n\right)=\exp\left(\sum_{n\geq 1}\frac{a_{mn}}{mn}z^{mn}\right)=\exp\left(\sum_{n\geq 1}\frac{a_{mn}}{n}z^{mn}\right)^{1/m}.$$

Using the criterion of Proposition 2.2(ii), it is clear that the sequence $(a_{mn})_{n\geq 1}$ has t-root-rational zeta function, hence ζ_1 is indeed (tm)-root-rational. The result for ζ_2 follows by noting that $\zeta_2=\zeta_1/\zeta_{(a_n)}$. □

Lemma 2.6 implies in particular that, for any $d\in\mathbf{Z}_{>0}$, the zeta function corresponding to the *divisor indicator sequence*

$$\mathbf{1}_{d|n}:=\begin{cases}1 & \text{if } d\mid n;\\ 0 & \text{else.}\end{cases}$$

is d-root-rational. We can also see this directly from Proposition 2.2(ii), by noting that (see e.g. Lemma 2.17)

$$\mathbf{1}_{d|n}=\frac{1}{d}\sum_{\zeta^d=1}\zeta^n,$$

where the sum is over all d-th roots of unity ζ in $\mathbf{C}$. We will call a periodic sequence (r_n) of period ω a *gcd sequence* if $r_n=r_{\gcd(n,\omega)}$ for all $n\in\mathbf{Z}_{>0}$. Note that a sequence (over a certain ring R) is a gcd sequence if and only if it can be written as an R-linear sum of divisor indicator sequences. Using this "decomposition" we find that a gcd sequence of period ω with values in the integers has an ω-root-rational zeta function. In fact, it turns out that the converse is also true:

Proposition 2.7 *Let $(a_n)_{n\geq 1}$ be a periodic sequence of rational numbers. Then the zeta function corresponding to (a_n) is root-rational if and only if (a_n) is a gcd sequence.*

Proof. " $\Longleftarrow$ " is shown above, so it suffices to prove " $\Longrightarrow$ ". Let ω be the period of (a_n), and suppose that $\zeta_{(a_n)}$ is root-rational. Denote by $\leq^*$ any total order on the set of positive integers $\mathbf{Z}_{>0}$ satisfying $m\mid n \implies m\leq^* n$.[5] Assume to the contrary that (a_n) is not a gcd sequence. Then, among the divisors of ω, there exists a maximal one (with respect to $\leq^*$), say m, such that $(b_n):=(a_{mn})$ is not a gcd sequence. The sequence (b_n) has root-rational zeta function (since (a_n) does), has period $s:=\omega/m$, and for every divisor $d>1$ of s, the subsequence (b_{dn}) is a gcd sequence, hence also has root-rational zeta function. We thus find that the sequence (c_n) defined by

$$c_n:=\begin{cases}b_n & \text{if } \gcd(n,s)=1;\\ 0 & \text{else,}\end{cases}$$

[5] E.g. by unique prime factorisation there is a bijection between $\mathbf{Z}_{>0}$ and the set

$$S:=\bigcup_{p \text{ prime}}\{(e_2,e_3,e_5,\cdots,e_p,0,\cdots)\in\mathbf{Z}_{\geq 0}^{\infty}\}$$

of eventually zero sequences of nonnegative integers, and the lexicographical order on S induces an order on $\mathbf{Z}_{>0}$ satisfying the desired condition.

has a root-rational zeta function. Writing

$$c_n = \sum_{\substack{\zeta \in \mathbf{C} \\ \zeta^s = 1}} \left(\sum_{\substack{1 \le i \le s \\ \gcd(i,s)=1}} b_i \zeta^i \right) \zeta^{-n},$$

we find using Proposition 2.2(ii) that

$$\sum_{\substack{1 \le i \le s \\ \gcd(i,s)=1}} b_i \zeta^i \in \mathbf{Q},$$

for all s-th roots of unity ζ. Applying this to a primitive s-th root of unity, and using the fact that the primitive s-th roots of unity are linearly independent over $\mathbf{Q}$, we find that the b_i (for i coprime to s) are all equal, contradicting the assertion that (b_n) is not a gcd sequence. □

2.2 Dynamics

Definition 2.8 A *discrete dynamical system* is a pair (S, f), where S is a set and $f : S \to S$ is map. △

Definition 2.9 Let (S, f) be a discrete dynamical system. If the cardinality of the set

$$\mathrm{Fix}(f^{\circ n}) := \{x \in S \mid \underbrace{f \circ \cdots \circ f}_{n \text{ times}}(x) = x\}$$

is finite for all n, we say that the map f is *confined*. For a confined map f, we define the *fixed point sequence* $(f_n)_{n \ge 1}$, by setting $f_n := \#\,\mathrm{Fix}(f^{\circ n})$. The *dynamical zeta function* ζ_f associated to the dynamical system (S, f) is defined to be the zeta function (5) associated to the sequence (f_n). That is,

$$\zeta_f(z) := \exp\left(\sum_{n \ge 1} \frac{f_n}{n} z^n \right). \tag{7}$$

△

Just like the Riemann zeta function, the dynamical zeta function also has a product expansion over "primes". In this case the relevant notion of a prime is a *prime orbit*.

Definition 2.10 Let (S, f) be a discrete dynamical system. An *orbit* X of S under f is a collection of (not necessarily distinct) elements $x_1, \cdots, x_m \in S$ such that $f(x_1) = x_2, f(x_2) = x_3, \cdots, f(x_m) = x_1$. If the x_i are all distinct, we say that X (which can then be regarded as a subset of S) is a *prime orbit*. △

Note that, if we denote by $\mathcal{P}(d)$ the set of prime orbits of length d, we have

$$\#\,\mathrm{Fix}(f^{\circ n}) = \sum_{d \mid n} d \cdot \#\mathcal{P}(d).$$

Hence (as equalities of formal power series)

$$\begin{aligned}\zeta_f(z) &= \exp\left(\sum_{\substack{d,n\geq 1\\ d|n}} \#\mathcal{P}(d)\frac{d}{n}z^n\right) = \exp\left(\sum_{d\geq 1}\sum_{n\geq 1}\#\mathcal{P}(d)\frac{d}{dn}z^{dn}\right)\\ &= \prod_{d\geq 1}\exp\left(\#\mathcal{P}(d)\sum_{n\geq 1}\frac{z^{dn}}{n}\right) = \prod_{d\geq 1}\left(\frac{1}{1-z^d}\right)^{\#\mathcal{P}(d)}. \end{aligned} \tag{8}$$

Rewriting (8), we obtain an expression similar to the Euler product formula for the Riemann zeta function:

$$\zeta_f(z) = \prod_{P\in\mathcal{P}}\frac{1}{1-z^{\#P}}, \tag{9}$$

where $\mathcal{P} = \bigcup_{d\geq 1}\mathcal{P}(d)$ is the set of all prime orbits.

Lemma 2.11 *Let S be any finite set and $f : S \to S$ any map. Then $\zeta_f(z)$ is rational.*

Proof. Since $\#\mathcal{P}(d)$ is zero for $d > \#S$, this follows immediately from (8). □

Definition 2.12 Let V be an algebraic variety of an algebraically closed field k with $\mathrm{char}(k) = p > 0$, and let $f : V \to V$ be a confined endomorphism. We define the *tame dynamical zeta function* $\zeta_f^*(z) \in \mathbf{C}[\![z]\!]$ (cf. [10, p. 4]) by

$$\zeta_f^*(z) := \exp\left(\sum_{p\nmid n}\frac{f_n}{n}z^n\right). \tag{10}$$

△

Proposition 2.13 *For (V, f) a discrete dynamical system as in Definition 2.12, the tame and "full" dynamical zeta function are related by the following equalities (of formal power series):*

$$\zeta_f^*(z) = \frac{\zeta_f(z)}{(\zeta_{f^{\circ p}}(z^p))^{1/p}}, \qquad \zeta_f(z) = \prod_{i\geq 0}\left(\zeta^*_{f^{\circ p^i}}(z^{p^i})\right)^{1/p^i}. \tag{11}$$

Proof. For the first equality, note that

$$\log\left(\zeta_f^*(z)\right) = \sum_{n\geq 1}\frac{f_n}{n}z^n - \frac{1}{p}\sum_{m\geq 1}\frac{f_{pm}}{m}z^{pm} = \log\left(\zeta_f(z)\zeta_{f^{\circ p}}(z^p)^{-1/p}\right).$$

The second equality follows by applying the first one repeatedly. Alternatively, we can compute:

$$\log(\zeta_f(z)) = \sum_{i\geq 0}\sum_{p\nmid m}\frac{f_{p^i m}}{p^i m}z^{p^i m} = \sum_{i\geq 0}\frac{1}{p^i}\sum_{p\nmid m}\frac{f_m^{\circ p^i}}{m}\left(z^{p^i}\right)^m = \log\left(\prod_{i\geq 0}\left(\zeta^*_{f^{\circ p^i}}(z^{p^i})\right)^{1/p^i}\right).$$

□

2.3 Discrete Valuations

Definition 2.14 Let R be a (not necessarily commutative) ring. A map $v : R \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ is called a *(discrete) valuation on* R if, for all $x, y \in R$, the following hold:

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$;

(iii) $v(x + y) \geq \min(v(x), v(y))$. △

For a ring R with discrete valuation v, it follows from property (ii) that $v(1) = 0$. Indeed, we have $v(1) = v(1^2) = 2v(1)$. Now let $0 \neq m = 1 + \cdots + 1 \in R$ be minimal such that $v(m) > 0$, and define $\rho(R, v) := v(m)$. We set $\rho(R, v) = 0$ if m does not exist or $\mathrm{char}(R) \neq 0$ (note that this makes sense because of Proposition 2.16(ii) combined with part (ii) of the definition; indeed, in prime characteristic, any non-zero integer m has finite multiplicative order, hence $v(m) = 0$).

Definition 2.15 Let R be a ring with discrete valuation v. The set $\{x \in R \mid v(x) > 0\}$ is a prime ideal called the *valuation ideal* of R. △

Now it follows that, if m as above exists, then it must be prime. Indeed (for $\mathrm{char}(R) = 0$), the restriction of v to $\mathbf{Z} \subseteq R$ is a valuation on $\mathbf{Z}$, with valuation ideal $m\mathbf{Z}$.

Proposition 2.16 *Let R be a ring with discrete valuation $v : R \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$. Then the following statements hold for all $x, y \in R$ and $n \in \mathbf{Z}_{\geq 0}$:*

(i) R has no zero divisors.

(ii) If the characteristic of R is positive, then it is prime.

(iii) $v(xy - yx) \geq v(x - y)$.

(iv) $v(x^n - y^n) \geq v(x - y)$.

Now suppose additionally that x and y commute, that $v(x) = v(y) = 0$, and that $v(x-y) \geq \frac{\rho(R,v)+1}{p-1}$. Then

(v) $$v(x^n - y^n) = \begin{cases} v(x - y) + v(n) & \text{if } \mathrm{char}(R) = 0; \\ v(x - y)p^{v_p(n)} & \text{if } \mathrm{char}(R) = p > 0. \end{cases}$$

Finally, if there exists a positive integer $s \in R$ such that $v(s) > 0$ (i.e. the composition $\mathbf{Z} \setminus \{0\} \to R \xrightarrow{v} \mathbf{Z}_{\geq 0} \cup \{\infty\}$ is not identically zero), then

(vi) Let $z \in R$, and assume that $v(z - 1) > 0$. Then $v(z^r - 1)$ is unbounded when r ranges over $\mathbf{Z}_{>0}$.

Proof. (i) If $x, y \in R$ are such that $xy = 0$, then $v(x) + v(y) = v(xy) = v(0) = \infty$, hence $v(x) = \infty$ or $v(y) = \infty$, so $x = 0$ or $y = 0$.

(ii) If $\mathrm{char}(R) > 0$ is not prime, then it is the product of two non-zero integers in R, so R would have zero divisors, contradicting (i).

(iii) We have $v(xy - yx) = v((x - y)x - x(x - y)) \geq \min(v((x - y)x), v(x(x - y))) \geq v(x - y)$.

(iv) We have $x^n - y^n = (y+(x-y))^n - y^n = y^n - y^n + z$, where z is in the two-sided ideal of R generated by $(x-y)$, so $v(x^n - y^n) = v(z) \geq v(x-y)$.

(v) Since $xy = yx$, we have

$$x^n - y^n = (y+(x-y))^n - y^n = \sum_{k=1}^{n} \binom{n}{k} (x-y)^k y^{n-k} = n(x-y)y^{n-1} + \sum_{k=2}^{n} \binom{n}{k} (x-y)^k y^{n-k}. \quad (12)$$

If $v(n) = 0$, then we see that $v\left(\binom{n}{k}(x-y)^k y^{n-k}\right) > v(n(x-y)y^{n-1})$ for all $2 \leq k \leq n$, so it follows from (12) that $v(x^n - y^n) = v(n(x-y)y^{n-1}) = v(x-y)$.

Now suppose that $\mathrm{char}(R) = 0$ and that $p \in \mathbf{Z}_{>0}$ is minimal such that $v(p) > 0$ (so $v(p) = \rho(R, v)$). If p does not exist, then the desired statement is already true by the remark above, so suppose that p exists. Then by the same remark yet again, the statement holds if $p \nmid n$. Suppose that $n = p$. We would like to show that $v\left(\binom{p}{k}\right) + kv(x-y) = v\left(\binom{n}{k}(x-y)^k y^{n-k}\right) > v(n(x-y)y^{n-1}) = v(p) + v(x-y)$ for all $2 \leq k \leq n$, since then $v(x^p - y^p) = v(x-y) + v(p)$, which is the desired result. If $2 \leq k < p$, then

$$v\left(\binom{p}{k}\right) + (k-1)v(x-y) \geq v(p) + (k-1)v(x-y) > v(p).$$

While if $k = p$, then

$$v\left(\binom{p}{k}\right) + (k-1)v(x-y) = (p-1)v(x-y) \geq v(p) + 1 > v(p),$$

so the desired result follows. Now the result follows for general n by induction on $v_p(n)$.

If $\mathrm{char}(R) = p > 0$ and $p \nmid n$, then clearly we have $v\left(\binom{n}{k}\right) \geq 0 = v(n)$, so we see immediately from (12) that $v(x^n - y^n) = v(x-y)$. On the other hand, if $n = p^\ell$ is a power of p, then $v(x^n - y^n) = v\left((x-y)^{p^\ell}\right) = v(x-y)p^\ell = v(x-y)p^{v_p(n)}$. The desired result now follows for general n by factorizing $n = p^\ell n'$ where $p \nmid n'$.

(vi) Using the same expansion as in (12), we find

$$z^s - 1 = (1 + (z-1))^s - 1 = s(z-1) + \sum_{k=2}^{s} \binom{s}{k} (z-1)^k.$$

Since all the terms appearing on the right hand side have valuation $> v(z-1)$, we find that $v(z^s - 1) > v(z-1)$, thus raising to successive powers of s yields the desired result. □

Part (v) of Proposition 2.16 will turn out to be very important in being able to control the growth of the inseparability degree of endomorphisms on algebraic groups. Bridy [9, §6] refers to this result as "lifting the exponent", and proves it in three special cases. It should be noted, however, that the statement of Lemma 6.2 in his paper is false. Here he considers a certain valuation on a maximal order $\mathcal{O}$ in the quaternion algebra B over $\mathbf{Q}$ that is ramified precisely at p (for some prime p) and ∞. More precisely, if π denotes a uniformizer for the localization $\mathcal{O}_p$ of $\mathcal{O}$ at p, he lets v be the valuation on $\mathcal{O}$ associated to the ideal $I := \pi\mathcal{O}_p \cap \mathcal{O}$. It is claimed that lifting the exponent holds for $x, y \in \mathcal{O}$ as in Proposition 2.16(v) *even when x and y do not commute*. However, if p is any prime, and we set $s \geq \max\left(\frac{\rho(\mathcal{O},v)+1}{p-1}, 2v_p(2)+1\right)$, $x = p^s j + i$, and $y = i$, then $v(x^2 - y^2) = v(y(x-y) + (x-y)y + (x-y)^2) = v(ip^s j + p^s ji + p^{2s} j^2) =$

$2sv(p) \neq sv(p) + 2v_p(2) = v(x-y) + 2v_p(2)$. In Bridy's paper this mistake does not form an issue, since only the case where x and y *do* commute is considered in later proofs (in fact he only considers the case $y = 1$).

Finally, for future reference, we record the following Lemma:

Lemma 2.17 *Let R be a (not necessarily commutative) ring without zero divisors, and let $\Gamma \subseteq \mathrm{Aut}(R)$ be a finite subgroup. Then*

$$\sum_{\gamma \in \Gamma} \gamma = \begin{cases} 1 & \text{if } \Gamma = \{1\} \\ 0 & \text{else.} \end{cases}$$

Proof. For any $\gamma_0 \in \Gamma$, we have

$$(1 - \gamma_0) \sum_{\gamma \in \Gamma} \gamma = \sum_{\gamma \in \Gamma} \gamma - \sum_{\gamma \in \Gamma} \gamma_0 \gamma = \sum_{\gamma \in \Gamma} \gamma - \sum_{\gamma \in \Gamma} \gamma = 0.$$

Thus, if there exists a $\gamma_0 \in \Gamma \setminus \{1\}$, it follows that $\sum_{\gamma \in \Gamma} \gamma = 0$. □

2.4 Algebraic Groups

Let k be an algebraically closed field.

Definition 2.18 An *algebraic group* G over k is an algebraic variety G/k, together with an (identity) element $e \in G$, and morphisms of varieties $\mu : G \times G \to G$, $(x, y) \mapsto x \cdot y$ and $i : G \to G$, $x \mapsto x^{-1}$, with respect to which G is a group. A *morphism of algebraic groups* is a map between algebraic groups that is both a morphism of varieties and a group homomorphism. △

We will denote by $\mathrm{End}(G)$ and $\mathrm{Aut}(G)$ the set of endomorphisms and automorphisms of G respectively. When G is commutative, the set of endomorphisms (which we will then refer to as the *endomorphism ring*) admits a ring structure, given by $(\sigma\tau)(g) = (\sigma \circ \tau)(g)$ and $(\sigma + \tau)(g) := \sigma(g) + \tau(g)$ for $\sigma, \tau \in \mathrm{End}(G)$.

Definition 2.19 An algebraic group that is affine as a variety is called a *linear algebraic group*. An algebraic group that is projective as a variety is called an *abelian variety*. △

An important example of a linear algebraic group is the general linear group GL_n/k of invertible $n \times n$ matrices over k. Any closed algebraic subgroup of GL_n is a linear algebraic group, and conversely, any linear algebraic group is isomorphic to a closed algebraic subgroup of GL_n for some n [42, Thm. 2.3.7], hence explaining the name *linear* algebraic group. It also turns out that the group structure of abelian varieties is (as the name suggests) indeed always commutative [30, Cor. 1.4]. An elliptic curve is an abelian variety of dimension one.

Remark 2.20 For our purposes, we will view the underlying variety of an algebraic group as a (reduced) classical algebraic variety. From this point of view, all algebraic groups (over an algebraically closed field) are smooth (all classical algebraic varieties have a smooth point, and algebraic groups look locally everywhere the same, because translating by an element of the group is an automorphism of the underlying variety). When one wants, for example, to take proper scheme-theoretic kernels of morphisms, then it is

more natural to consider algebraic groups to be group schemes of finite type over a field (and these need not be smooth). ◊

Definition 2.21 Let G be a linear algebraic group. An element $u \in G$ is called *unipotent* if for every isomorphism ϕ from G to some closed subgroup of GL_n, the element $\phi(u)$ is unipotent; i.e. $\phi(u) - 1$ is nilpotent. We will call G unipotent if every element of G is unipotent. △

The subgroup $U_n \subseteq \mathrm{GL}_n$ of upper-triangular matrices with all diagonal entries equal to one is an example of a unipotent algebraic group. It turns out that any unipotent algebraic group is isomorphic to a closed subgroup of U_n for some n [42, Prop. 2.4.12].

Definition 2.22 Let G be an algebraic group. A *Borel subgroup* B of G is a maximal closed connected solvable algebraic subgroup of G. △

The following result, known as Chevalley's structure theorem for algebraic groups, will very be important later on.

Theorem 2.23 (Chevalley) *Let G be a connected algebraic group. Then there exists a unique normal connected linear algebraic closed subgroup N of G for which G/N is an abelian variety.*

Proof. By Chevalley [11]. A modern proof can be found under [15, Thm. 1.1]. □

Lemma 2.24 *Let $\phi : G \to G'$ be a morphism of connected algebraic groups, and let $N \subseteq G$ and $N' \subseteq G'$ as in Theorem 2.23, so that $A := G/N$ and $A' := G'/N'$ are abelian varieties. Then $\phi(N) \subseteq \phi(N')$. In particular, ϕ induces a morphism $\tilde{\phi} : A \to A'$.*

Proof. Theorem 2.23 gives us short exact sequences $1 \to N \to G \to A \to 1$ and $1 \to N' \to G' \to A' \to 1$. Since the map $N \to G \xrightarrow{\phi} G' \to A'$ is constant by [15, Lemma. 2.3], the desired result follows. □

Lemma 2.24 tells us that a morphism $\phi : G \to G'$ of connected algebraic groups induces a morphism of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & A & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi|_N} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \tilde{\phi}} & & \\ 1 & \longrightarrow & N' & \longrightarrow & G' & \longrightarrow & A' & \longrightarrow & 1 \end{array} \tag{13}$$

where N, N' are connected linear algebraic groups and A, A' are abelian varieties. Note that the Snake Lemma [33, Ex. 5.7] implies that, if $\phi|_N$ is surjective, we have a short exact sequence $1 \to \ker(\phi|_N) \to \ker(\phi) \to \ker(\tilde{\phi}) \to 1$ of (group-theoretic) kernels. This shows in particular that, if $\ker(\phi)$ is finite, then so are $\ker(\phi|_N)$ and $\ker(\tilde{\phi})$.

Lemma 2.25 *Let G be a connected algebraic group. Then G is irreducible (as an algebraic variety).*

Proof. This follows from [42, Prop. 2.2.1]. □

Lemma 2.26 *Let G be a linear algebraic group and let H be a closed normal algebraic subgroup. Then the quotient G/H is a linear algebraic group.*

Proof. [7, Thm. 6.8]. □

Lemma 2.27 *Let $\phi : G \to G'$ be a morphism of algebraic groups. Then*

(i) The (group-theoretic) kernel of ϕ is a closed normal algebraic subgroup of G.

(ii) The image $\phi(G)$ is a closed algebraic subgroup of G'.

In particular, if either G or G' is a linear algebraic group, then so is $\phi(G)$.

Proof. [42, Prop. 2.2.5]. The last statement follows from Lemma 2.26. □

Definition 2.28 A morphism $\phi : G \to G'$ of algebraic groups is called an *isogeny* if ϕ has finite kernel and is surjective. △

Lemma 2.29 *Let $\phi : G \to G'$ be a morphism of connected algebraic groups. Then the following are equivalent:*

(a) ϕ is an isogeny.

(b) $\dim(G) = \dim(G')$ and ϕ has finite kernel.

(c) $\dim(G) = \dim(G')$ and ϕ is surjective.

Proof. By [31, Thm. 10.9], we have, for all $y \in \phi(G')$, $\dim(\phi^{-1}(y)) \geq \dim(\phi(G)) - \dim(G)$, with equality holding on a non-empty open subset U of $\phi(G')$. Since the fibers (over points in the image) of a morphism of algebraic groups are isomorphic (for $x \in \phi^{-1}(y)$, the map $\phi^{-1}(1) \to \phi^{-1}(y)$, $z \mapsto zx$ is an explicit isomorphism), it follows that we in fact have

$$\dim(\phi^{-1}(y)) = \dim(\phi(G)) - \dim(G) \tag{14}$$

for all $y \in \phi(G)$. Now it it clear that (a) implies that $\dim(G') = \dim(\phi(G)) = \dim(G)$, hence (a) implies (b) and (c). It is clear that (b) and (c) together imply (a), thus it remains to show that (b) and (c) are equivalent; suppose for the remainder of the proof that we are in the case $\dim(G) = \dim(G')$.

"(b) $\implies$ (c)" If ϕ is surjective, then it follows immediately from (14) that $\dim(\phi^{-1}(y)) = 0$ for all $y \in \phi(G) = G'$, and hence in particular that $\ker(\phi)$ is finite.

"(c) $\implies$ (b)" If $\ker(\phi)$ is finite, then by (14) we have $\dim(\phi(G)) = \dim(G)$. In the case that G is an abelian variety or a linear algebraic group, this immediately implies that ϕ is surjective (since $\phi(G)$ and G' are irreducible by Lemma 2.25, and $\phi(G) \subseteq G'$ is a closed subvariety by Lemma 2.27). Thus, in diagram (13), both $\phi|_N$ and $\tilde{\phi}$ are surjective (using the remark after the diagram). The Four Lemma [27, Lem. 3.2] now implies that ϕ is also surjective. □

Definition 2.30 Let $\phi : G \to G'$ be a surjective morphism of connected algebraic groups. The *degree* $\deg(\phi)$ and *inseparability degree* $\deg_i(\phi)$ of ϕ are defined to be the degree and inseparability degree of the extension of function fields $k(G)/\phi^* k(G')$ respectively. We call ϕ *separable* when $\deg_i(\phi) = 1$. △

Definition 2.31 An endomorphism σ of a connected commutative algebraic group is called *coseparable* when $\sigma^n - 1$ is a separable isogeny for all $n \in \mathbf{Z}_{>0}$. △

3 Dynamically Affine Maps

Let k denote an algebraically closed field. All algebraic varieties are assumed to be over k.

3.1 Definitions

An *affine morphism* of a commutative algebraic group G/k is, roughly speaking, a composition of an endomorphism σ of G with a translation. Before giving the precise definition, we should provide a disclaimer: in his definition of a dynamically affine map, Silverman [39, §6.8] assumes that σ is finite and of degree at least 2. For connected one-dimensional G, this assumption implies that σ is confined (in fact, it is almost equivalent to σ being confined; see Lemma 3.19), which is precisely the condition that is, for our purposes, convenient. However, for higher dimensional G, assuming $\deg(\sigma) \geq 2$ does not always imply that σ is confined (see Example 3.1). Precisely this issue causes a mistake in (the last line of) the proof of [9, Lemma 2.4]. In fact, the statement of this particular lemma (which is Lemma 3.6 below) is false when using Silverman's notion of an affine morphism. In order to avoid some unnatural case distinctions, we will therefore use a slightly alternative notion of an affine morphism, and hence of a dynamically affine map (Definition 3.3).

Example 3.1 Let E be an elliptic curve, and $G := E \times E$. Let $\sigma := [-1] \times [2] \in \mathrm{End}(G)$, where $[m]$ denotes the multiplication-by-m map. Then $\deg(\sigma) = 4$, but $\sigma^2 - 1 = [0] \times [4]$, so σ is not confined. ☆

Definition 3.2 Let G/k be a commutative algebraic group. An *affine morphism* of G is a map $\psi : G \to G$ that can be written as $\psi(g) = \sigma(g) + h$ for some confined isogeny $\sigma \in \mathrm{End}(G)$ and some $h \in G$. △

Now, a *dynamically affine map* can roughly be viewed as a "finite quotient" of an affine morphism on a connected commutative algebraic group. Let V/k denote an algebraic variety.

Definition 3.3 We call a morphism $f : V \to V$ *dynamically affine* if there exists

(i) a connected commutative algebraic group G;

(ii) an affine morphism $\psi : G \to G$;

(iii) a finite subgroup $\Gamma \subseteq \mathrm{Aut}(G)$; and

(iv) an inclusion $\iota : G/\Gamma \to V$ that identifies G/Γ with a Zariski-dense open subset of V,

such that the following diagram commutes:

$$\begin{array}{ccc} G & \xrightarrow{\psi} & G \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ G/\Gamma & \longrightarrow & G/\Gamma \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ V & \xrightarrow{f} & V \end{array} \tag{15}$$

△

When talking about dynamically affine maps $f : V \to V$, we will often use the notation provided by the definition to refer to the underlying constituents $\{G, \psi, \sigma, h, \Gamma, \iota\}$.

Definition 3.4 A dynamically affine map f is called *coseparable* when σ is coseparable (see Definition 2.31). △

Lemma 3.5 *Let $f : V \to V$ be a dynamically affine map.*

(i) There exists a group automorphism $\alpha : \Gamma \to \Gamma$ such that for any $\gamma \in \Gamma$, $\psi \circ \gamma = \alpha(\gamma) \circ \psi$;

(ii) $(\psi^n - \gamma)^{-1}(0)$ is finite for all $n \in \mathbf{Z}_{>0}$ and $\gamma \in \Gamma$.

Proof. (i) By [39, Prop. 6.77(a)], for every $\gamma \in \Gamma$ there exists a (unique) $\gamma' \in \Gamma$ such that $\psi \circ \gamma = \gamma' \circ \psi$. This induces a map $\alpha : G \to G$, $\gamma \mapsto \gamma'$. Now note that $\alpha(\gamma_1 \circ \gamma_2) \circ \psi = \psi \circ (\gamma_1 \circ \gamma_2) = (\psi \circ \gamma_1) \circ \gamma_2 = \alpha(\gamma_1) \circ \alpha(\gamma_2) \circ \psi$, hence, by surjectivity of ψ, α is a group endomorphism. To see why α is bijective, or, equivalently, injective, let $\gamma \in \ker(\alpha)$. Then $\psi \circ (\gamma - 1) = 0$, hence $\mathrm{im}(\gamma - 1) \subseteq \ker(\psi)$. Since $\ker(\psi)$ is finite by Lemma 2.29 and $\mathrm{im}(\gamma - 1)$ is connected (because G is connected), we conclude that $\mathrm{im}(\gamma - 1) = \{0\}$, hence $\gamma = 1$.

(ii) Let $\gamma \in \Gamma$, and suppose that $x \in G$ is such that $\psi^n(x) = \gamma(x)$. Then

$$\psi^{dn}(x) = \left(\alpha^{(d-1)n}(\gamma) \cdots \alpha^n(\gamma)\gamma\right)(x) = \left(\beta^{d-1}(\gamma) \cdots \beta(\gamma)\gamma\right)(x),$$

where $\beta := \alpha^n$. Since β is injective,

$$\beta^{r+s}(\gamma) \cdots \beta^r(\gamma) = 1 \iff \beta^r(\beta^s(\gamma) \cdots \beta(\gamma)\gamma) = 1 \iff \beta^s(\gamma) \cdots \beta(\gamma)\gamma = 1.$$

Thus, since Γ is finite, there exists a $d \in \mathbf{Z}_{>0}$ such that $\beta^{d-1}(\gamma) \cdots \beta(g)\gamma = 1$. Therefore $(\psi^n - \gamma)^{-1}(0) \subseteq (\psi^{dn} - 1)^{-1}(0)$. Since σ, hence ψ, is confined by assumption, we have that $(\psi^{dn} - 1)^{-1}(0)$ is finite, and the desired result follows. □

The following lemma is crucial, as it allows to count the fixed point sequence (f_n) of a dynamically affine map f in terms of kernels of endomorphisms on the algebraic group G:

Lemma 3.6 (Bridy, [9, Lemma 2.4]) *Let $f : V \to V$ be a dynamically affine map. Then*

$$\#\,\mathrm{Fix}(f^{\circ n}) = \#(\mathrm{Fix}(f^{\circ n}) \setminus \iota(G/\Gamma)) + \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \#\ker(\sigma^n - \gamma).$$

Proof. Let $S := \bigcup_{\gamma \in \Gamma} (\psi^n - \gamma)^{-1}(0)$. Then

$$\#\,\mathrm{Fix}(f^{\circ n}) = \#(\mathrm{Fix}(f^{\circ n}) \setminus \iota(G/\Gamma)) + \#(\mathrm{Fix}(f^{\circ n}) \cap \iota(G/\Gamma)) = \#(\mathrm{Fix}(f^{\circ n}) \setminus \iota(G/\Gamma)) + \pi(S).$$

If $g \in S$, then $\psi^n(g) = \gamma_g(g)$ for some $\gamma_g \in \Gamma$. Let α as in Lemma 3.5. Then for any $\gamma \in \Gamma$, we have $\psi^n(\gamma(g)) = \alpha(\gamma)\psi^n(g) = \alpha(\gamma)\gamma_g(g) = (\alpha(\gamma)\gamma_g\gamma^{-1})(\gamma(g))$, so $\gamma(g) \in S$. We thus see that $\gamma \mapsto (g \mapsto \gamma(g))$ defines an action of Γ on S, and that $\#(\mathrm{Fix}(f^{\circ n}) \cap \iota(G/\Gamma)) = \#S/\Gamma$. Now, for $\gamma \in \Gamma$, denote by S^γ the

set of $g \in S$ fixed by γ, and for $g \in G$, denote by Γ_g the set of $\gamma \in \Gamma$ that fix g. By the Counting Theorem [2, Thm. 18.1],

$$\begin{aligned} \#S/\Gamma &= \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}|S^\gamma| = \frac{1}{|\Gamma|}\sum_{g\in G}|\Gamma_g| = \frac{1}{|\Gamma|}\sum_{g\in G}\#\{\gamma\in\Gamma \mid \gamma(g)=g\} \\ &= \frac{1}{|\Gamma|}\sum_{g\in G}\#\{\gamma\in\Gamma \mid g=\gamma^{-1}\gamma_g(g)\} = \frac{1}{|\Gamma|}\sum_{g\in G}\#\{\gamma\in\Gamma \mid g\in(\psi^n-\gamma)^{-1}(0)\} \\ &= \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\#\{g\in G \mid g\in(\psi^n-\gamma)^{-1}(0)\} = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\#(\psi^n-\gamma)^{-1}(0). \end{aligned}$$

Now, since $\psi^n(g) = \sigma^n(g) + \sum_{i=0}^{n-1}\sigma(h)$ and $\sigma^n - \gamma$ is surjective (by Lemma 3.5(ii) combined with Lemma 2.29), we find that $\#(\psi^n-\gamma)^{-1}(0) = \#\ker(\sigma^n-\gamma)$. □

3.2 Introduction to Hypotheses

For the remainder of this section, we will assume that $\mathrm{char}(k) = p > 0$.

Let $f : V \to V$ be a dynamically affine map. In order to determine the dynamical zeta function ζ_f, we need to control the fixed point sequence (f_n). For any isogeny $\tau : G \to G$, we can write

$$\#\ker(\tau) = \deg(\tau)/\deg_i(\tau). \tag{16}$$

Thus, using Lemma 3.6, controlling the fixed point sequence (f_n) can be achieved by controlling, for every $\gamma \in \Gamma$,

(a) the sequence $c_n := \#(\mathrm{Fix}(f^{\circ n}) \setminus \iota(G/\Gamma))$;

(b) the "inseparability degree sequence" $\deg_i(\sigma^n - \gamma)$;

(c) the "degree sequence" $\deg(\sigma^n - \gamma)$.

In order to be able to do this, we will need to make some extra assumptions associated to the dynamically affine map f, in the form of four *hypotheses*:

(H1) The sequence (c_n) has a rational zeta function.

(H2) All non-zero elements of $\mathrm{End}(G)$ are isogenies, and there exists a discrete valuation $v : \mathrm{End}(G) \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ such that $\deg_i(\tau) = p^{v(\tau)}$ for all isogenies τ.

Before introducing the last two hypotheses, we will set up some notation.

Notation. Let v be as in **(H2)**. For $m \in \mathbf{Z}_{\geq 0}$, we let $\Gamma_m := \{\gamma \in \Gamma \mid v(\gamma - 1) \geq m\}$. This defines a descending filtration of normal subgroups $\Gamma = \Gamma_0 \supseteq \Gamma_1 \supseteq \cdots \supseteq \Gamma_N = 1$, where $N := \max\{v(\gamma - \gamma') \mid \gamma, \gamma' \in \Gamma, \gamma \neq \gamma'\} + 1$. Moreover, we let $s_m \in \mathbf{Z}_{>0}$ be minimal (if it exists) such that $v(\sigma^{s_m} - \gamma_m) \geq m$ for some $\gamma_m \in \Gamma$. Denote $s := s_N$ and $\tilde{\gamma} := \gamma_N$.

(H3) Let $m \in \mathbf{Z}_{\geq 0}$. If s_m exists, then

$$\exp\left(\sum_{\substack{n\geq 1\\ \gamma\in\Gamma_m}} \frac{\deg(\sigma^{s_m n} - \gamma\gamma_m^n)}{n} z^n\right) \in \mathbf{C}(z).$$

(H4) If s exists, then $(\deg(\sigma^{sn} - \tilde{\gamma}^n))_{m \geq 1}$ satisfies the dominant root assumption (see Definition 2.3).[6]

Here, **(H1)**, **(H2)** and **(H3)** serve to control the sequences listed above under (a), (b) and (c) respectively, while **(H4)** is a technical hypothesis that we will use in order to avoid cancellation of certain singularities. The main results are (note that **(H3)** with $m = 0$ shows in particular that ζ_f has a positive radius of convergence):

Theorem 3.7 *Let V be an algebraic variety over an algebraically closed field of characteristic $p > 0$, and let $f : V \to V$ be a dynamically affine map satisfying* **(H1)**-**(H4)**. *Then the following dichotomy holds:*

(i) If f is coseparable, then ζ_f is root-rational.

(ii) Otherwise, ζ_f has a natural boundary.

Theorem 3.8 *Let V be an algebraic variety over an algebraically closed field of characteristic $p > 0$, and let $f : V \to V$ be a dynamically affine map satisfying* **(H1)**-**(H3)**. *Then ζ_f^* is root-rational.*

In order to prove these results, we use two important lemmas. The first one tells us in particular that σ^s and $\tilde{\gamma}$ (as in **(H4)**) commute.

Lemma 3.9 *Let f be a dynamically affine map satisfying* **(H2)**. *Suppose that $n \in \mathbf{Z}_{>0}$ and $\gamma \in \Gamma$ are such that $v(\sigma^n - \gamma) \geq N$. Then σ^n and γ commute.*

Proof. Let $\alpha \in \mathrm{Aut}(\Gamma)$ as in Lemma 3.5, so that $\sigma\gamma = \alpha(\gamma)\sigma$. Then

$$N \leq v(\sigma^n - \gamma) \leq v(\sigma^n\gamma - \gamma\sigma^n) = v((\alpha(\gamma) - \gamma)\sigma^n) = v(\alpha(\gamma) - \gamma).$$

We conclude that $\alpha(\gamma) = \gamma$ by definition of N. □

The second lemma is a natural boundary result for two basic maps:

Lemma 3.10 *Let $h \in \mathbf{R}_{>0}$ and $0 < \beta < 1$. Define the following formal power series (over $\mathbf{C}$):*

$$G_h(z) := \sum_{n \geq 1} |n|_p^h z^n, \qquad H_\beta(z) := \sum_{n \geq 1} \beta^{|n|_p^{-1}} z^n.$$

Then G_h and H_β have the unit circle as a natural boundary.

Proof. First of all, we note that G_h and H_β both have radius of convergence equal to one by, for example, the (Cauchy) root test. Now, note that G_h and H_β satisfy the following functional equations:

$$\frac{1}{p^h} G_h(z^p) = \frac{1}{p^h} \sum_{n \geq 1} |n|_p^h z^{pn} - \sum_{n \geq 1} |pn|_p^h z^{pn} = G_h(z) - \left(\frac{z}{1-z} - \frac{z^p}{1-z^p} \right). \tag{17}$$

$$H_{\beta^p}(z^p) = \sum_{n \geq 1} \beta^{|pn|_p^{-1}} z^{pn} = H_\beta(z) - \sum_{p \nmid n} \beta^{|n|_p^{-1}} z^n = H_\beta(z) - \beta \left(\frac{z}{1-z} - \frac{z^p}{1-z^p} \right). \tag{18}$$

[6] Note that, by applying **(H3)** with $m = N$, the sequence is indeed linear recurrent.

We will first show that G_h and H_β both have poles at all p-th roots of unity. It is clear that they have a pole at 1, so let ω_p be a primitive p-th root of unity. Since $\sum_{n=1}^{p} \omega_p^n = 0$ (for example by Lemma 2.17), we find $\sum_{n=1}^{p} |n|_p^h \omega_p^n = p^{-h} - 1$. Generalizing to multiples of p, we find

$$\sum_{n=1}^{pm} |n|_p^h \omega_p^n \leq m(p^{-h} - 1)$$

for all $m \in \mathbf{Z}_{>0}$. Now, as $m(p^{-h} - 1) \xrightarrow{m\to\infty} -\infty$, and the terms between consecutive multiples of p are bounded, we conclude that G_h has a pole at ω_p. A similar argument works for H_β, using the analogous estimate

$$\sum_{n=1}^{pm} \beta^{|n|_p^{-1}} \omega_p^n \leq m(\beta^p - 1).$$

Now, by the functional equations (17) and (18), it follows by induction on k that G_h and H_β have poles at all p^k-th roots of unity, so we can conclude that they have a natural boundary (at the unit circle). □

We will now present the idea of the proof of Theorem 3.7 and 3.8: the actual proof can be found in Section 3.4. Using Lemma 3.6, we first write

$$f_n = c_n + \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} \deg(\sigma^n - \gamma) / \deg_i(\sigma^n - \gamma).$$

By **(H1)**, the sequence (c_n) has a rational zeta function, so it produces a rational factor in ζ_f. By Lemma 2.6, the contribution of c_n to ζ_f^* is also root-rational. Since we are only interested in statements for the (tame) zeta function *up to root-rationality*, we may thus "disregard" the c_n completely. The same holds for the factor $1/|\Gamma|$, as we can eliminate it taking the $|\Gamma|$-th power. The interesting part of f_n that remains can be rewritten using **(H2)** as

$$\sum_{\gamma \in \Gamma} \deg(\sigma^n - \gamma) p^{-v(\sigma^n - \gamma)}. \tag{19}$$

Now, if σ is coseparable, then $v(\sigma^n - \gamma) = 0$ for all γ and n. Applying **(H3)** with $m = 0$, we conclude that both ζ_f and ζ_f^* are root-rational.

On the other hand, if σ is not coseparable, then $v(\sigma^n - \gamma)$ gets arbitrarily large (i.e. all of the s_m and γ_m exist) by application of Proposition 2.16(vi). By Lemma 3.9, σ^s commutes with $\tilde{\gamma}$, which means that we can use Proposition 2.16(v) to control the following "subsequence" of (19):[7]

$$\deg(\sigma^{sn} - \tilde{\gamma}^n) p^{-v(\sigma^{sn} - \tilde{\gamma}^n)} = \deg(\sigma^{sn} - \tilde{\gamma}^n) \cdot \text{"something depending on } |n|_p\text{"}. \tag{20}$$

To justify being able to consider just this subsequence without discarding any non-root-rational parts, **(H3)** is used. The "part depending on $|n|_p$" will resemble one of the power series of Lemma 3.10, and therefore produces a lot of singularities. We then employ **(H4)** to make sure that the singularities found at the boundary of the disk of convergence (i.e. the circle of radius $1/|\Lambda|$, where Λ denotes the unique dominant root), cannot in any way cancel out. This allows us to conclude that the zeta function has a natural boundary. On the other hand, when only considering n not divisible by p, the dependence on $|n|_p$ is removed, which means that we can use **(H3)** (with m sufficiently large) to conclude that the tame zeta function corresponding to the sequence in (20), and hence ζ_f^* itself, is root-rational.

[7] Technically, we will possibly have to consider yet another subsequence of this to make sure the requirement for Proposition 2.16(vi) is met. Luckily, "something depending on $|n|_p$" is sufficiently vague, so (20) is in a sense still true. The details are (of course) provided in the actual proof.

3.3 The Projective Line

Before giving the complete proof of the main results, let us discuss what happens for the special case where V is the projective line, for which we will verify that the hypotheses **(H1)**-**(H4)** always hold. Here, Theorem 3.7 and 3.8 take the following form:

Theorem 3.11 (= Theorem A) *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be a dynamically affine map. Then the following dichotomy holds:*

(i) If f is coseparable, then ζ_f is rational.

(ii) Otherwise, ζ_f has a natural boundary.

Theorem 3.12 (= Theorem B) *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be a dynamically affine map. Then ζ_f^* is root-rational.*

These results follow directly from Theorems 3.7 and 3.8 after showing that:

Proposition 3.13 *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be a dynamically affine map. Then*

(i) f satisfies **(H1)**-**(H4)**.

(ii) If f is coseparable, then ζ_f is rational.

For the remainder of this subsection, we will focus on proving the first part of the proposition, eventually also proving the second part with the tools and calculations developed. Note that **(H1)** is the only hypothesis explicitly associated to the map f; the others (although **(H3)** and **(H4)** are *implicitly* associated to f) are statements purely about the group G and its endomorphisms. It follows from the definition of a dynamically affine map (a finite quotient of G lies Zariski-dense in V) that the connected group G must have same dimension as the variety V. Thus, to verify hypotheses **(H2)**-**(H4)** for dynamically affine maps on the projective line, we need to study the endomorphism structure of connected commutative algebraic groups of dimension one. However, let us start by verifying **(H1)**:

Lemma 3.14 *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be a dynamically affine map. Then the sequence $(c_n)_{n\geq 1}$ given by $c_n := \#(\mathrm{Fix}(f^{\circ n}) \setminus \iota(G/\Gamma))$ has rational zeta function.*

Proof. Since, $\iota(G/\Gamma)$ lies Zariski-open in $\mathbf{P}^1$ (which has the cofinite topology), we know that $S := \mathbf{P}^1 \setminus \iota(G/\Gamma)$ is finite. In particular, S contains finitely many of the periodic points of f, and the desired result follows from Lemma 2.11 (applied to the (finite) union of all orbits of f intersecting with S). □

3.3.1 Structure of Connected Algebraic Groups of Dimension One

By Theorem 2.23, any connected algebraic group G of dimension one fits into a short exact sequence

$$1 \to N \to G \to A \to 1,$$

where N is a connected linear algebraic group and A is an abelian variety. Since $\dim(G) = 1$, we have $\dim(N), \dim(A) \in \{0, 1\}$.

If $\dim(N) = 1$, then it follows from Lemma 2.29 that $N = G$, so G is a connected linear algebraic group of dimension one. By [42, Thm. 3.4.9], it follows that either

(i) $G \cong \mathbf{G}_a$, the *additive group of* k (which, as a variety, is isomorphic to $\mathbf{P}^1 \setminus \{\infty\}$); or

(ii) $G \cong \mathbf{G}_m$, the *multiplicative group of* k (which as a variety is isomorphic to $\mathbf{P}^1 \setminus \{0, \infty\}$).

If $\dim(A) = 1$, then by Lemma 2.29, N is finite, hence trivial (because it is connected), so

(iii) $G \cong E$, an *elliptic curve*.

Note that these connected algebraic groups of dimension one are all commutative, so the above list completely classifies the groups G from which a dynamically affine map on the projective line could arise. We will summarize some results that Bridy [9] uses about the structure of their endomorphism rings, which will be important for the proof of Proposition 3.13. In particular, in order to verify **(H2)**, we will need to understand the inseparability degree of endomorphisms of G, while for **(H3)** and **(H4)**, we need to control their degree. Nothing we will claim here is new; all statements can already be found (somewhat scattered) in [9].

The endomorphism ring

(i) The endomorphisms of $\mathbf{G}_a$ are the "additive maps", which are precisely the polynomials in the Frobenius $\phi : x \mapsto x^p$. So $\mathrm{End}(\mathbf{G}_a) \cong k\langle\phi\rangle$, the non-commutative polynomial ring over k in the "variable" ϕ, with multiplication rule $\phi a = a^p \phi$ for $a \in k$. The automorphism group $\mathrm{Aut}(\mathbf{G}_a)$ (i.e. the unit group of $\mathrm{End}(\mathbf{G}_a)$) is $k^\times$, consisting of the non-zero linear maps $x \mapsto ax$.

(ii) The endomorphisms of $\mathbf{G}_m$ are the "multiplicative maps", i.e. the power maps $x \mapsto x^m$ for $m \in \mathbf{Z}$. Hence, the endomorphism ring is $\mathrm{End}(\mathbf{G}_m) \cong \mathbf{Z}$, with automorphism group $\mathrm{Aut}(\mathbf{G}_m) = \{x, x^{-1}\} \cong \{\pm 1\}$.

(iii) For elliptic curves E, the endomorphism ring is an order in $\mathrm{End}(E) \otimes \mathbf{Q}$; the latter depending on the type of elliptic curve. Note that $\mathrm{End}(E)$ always contains the multiplication-by-m maps $[m]$ for $m \in \mathbf{Z}$. If the j-invariant of E is transcendental over $\mathbf{F}_p$, then these are the only endomorphisms, so we have $\mathrm{End}(E) \cong \mathbf{Z}$. If $j(E) \in \overline{\mathbf{F}_p}$, then we distinguish two options: either E is ordinary, or E is supersingular. If E is ordinary, then $\mathrm{End}(E) \otimes \mathbf{Q}$ is isomorphic to an imaginary quadratic number field L. If E is supersingular, then $\mathrm{End}(E) \otimes \mathbf{Q}$ is isomorphic to a quaternion algebra B over $\mathbf{Q}$ [40, Thm. V.3.1]. The automorphism group $\mathrm{Aut}(E)$ is a finite group of order dividing 24 (depending on the j-invariant and on $\mathrm{char}(k)$) [40, Thm. 10.1].

The degree

(i) For (non-zero) $\sigma = f(\phi) \in k\langle\phi\rangle = \mathrm{End}(\mathbf{G}_a)$, we have $\deg(\sigma) = p^{\deg_\phi(f)}$.

(ii) For (non-zero) $\sigma = m \in \mathbf{Z} = \mathrm{End}(\mathbf{G}_m)$, we have $\deg(\sigma) = |m|$.

(iii) For an elliptic curve E, let $N : \mathrm{End}(E) \otimes \mathbf{Q} \to \mathbf{Q}$ be the norm map $x \mapsto x\overline{x}$, where $\overline{x}$ denotes the conjugate of x (so if $\mathrm{End}(E) \otimes \mathbf{Q} \cong \mathbf{Q}$, N is given by $x \mapsto x^2$, if $\mathrm{End}(E) \otimes \mathbf{Q} \cong L$ for an imaginary quadratic number field L, $N = N_{L/\mathbf{Q}}$ is the usual norm for field extensions, and if $\mathrm{End}(E) \otimes \mathbf{Q} \cong B$ for a quaternion algebra B over $\mathbf{Q}$, N is the usual (reduced) norm for quaternion algebras). Then, for $\sigma \in \mathrm{End}(E) \setminus \{0\}$, we have $\deg(\sigma) = N(\sigma)$.

The inseparability degree

We can directly verify **(H2)**. That is,

Lemma 3.15 *Let G be a connected algebraic group of dimension one. There exists a discrete valuation $v : \mathrm{End}(G) \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ on the endomorphism ring such that, for all $\sigma \in \mathrm{End}(G) \setminus \{0\}$, we have $\deg_i(\sigma) = p^{v(\sigma)}$.*

Proof. (i) For $\mathbf{G}_a$, the set of inseparable endomorphisms (including zero) is the ideal $(\phi) \subseteq k\langle\phi\rangle$ generated by the Frobenius, and we have $\deg_i(\sigma) = p^{v_\phi(\sigma)}$.

(ii) For $\mathbf{G}_m$, the set of inseparable endomorphisms is the maximal ideal $p\mathbf{Z} \subseteq \mathbf{Z} = \mathrm{End}(\mathbf{G}_m)$, and we have $\deg_i(\sigma) = p^{v_p(\sigma)}$.

(iii) For an elliptic curve E, it once again depends on the type of elliptic curve. If the j-invariant is transcendental, then we have $\deg_i(\sigma) = p^{v_p(\sigma)}$. Else, if E is ordinary, then $\deg_i(\sigma) = p^{v_\mathfrak{p}(\sigma)}$, where $\mathfrak{p}$ is the extension of the ideal of inseparable endomorphisms in $\mathrm{End}(E)$ to the ring of integers $\mathcal{O}_L$ of the imaginary quadratic number field $L = \mathrm{End}(E) \otimes \mathbf{Q}$. Finally, if E is supersingular, then $\deg_i(\sigma) = p^{v_p(N(\sigma))}$ where $N : B \to \mathbf{Q}$ (as above) is the reduced norm map associated to the quaternion algebra $B = \mathrm{End}(E) \otimes \mathbf{Q}$ [9, Prop. 5.2, 5.3 & 5.5]. □

We summarize the results in the diagram below:

G	$\mathrm{End}(G)$	$\mathrm{Aut}(G)$	$\deg(\sigma)$	$\log_p(\deg_i(\sigma))$
$\mathbf{G}_a$	$k\langle\phi\rangle$	$k^\times$	$p^{\deg_\phi(\sigma)}$	$v_\phi(\sigma)$
$\mathbf{G}_m$	$\mathbf{Z}$	$\{\pm 1\}$	$\lvert\sigma\rvert$	$v_p(\sigma)$
E	$\mathcal{O} \subseteq \mathrm{End}(E) \otimes \mathbf{Q}$	Finite of order dividing 24	$N(\sigma)$	$v_\mathfrak{p}(\sigma)$ or $v_p(N(\sigma))$

Table 1: Endomorphism structure of connected algebraic groups of dimension 1.

3.3.2 Verifying (H3) and (H4)

Let G be a connected commutative algebraic group of dimension one.

Lemma 3.16 *Let $\sigma \in \mathrm{End}(G)$ be a confined isogeny, and let $\gamma, \gamma_0 \in \mathrm{Aut}(G)$, both of finite order. Then the following statements hold:*

(i) For any non-trivial finite subgroup $\{1\} \neq \Gamma \subseteq \mathrm{Aut}(G)$, the zeta function corresponding to the sequence $(\delta_n)_{n\geq 1}$ given by $\delta_n := \sum_{\gamma\in\Gamma} \deg(\sigma^n - \gamma\gamma_0^n)$ is rational.

(ii) If γ_0 commutes with σ, then the zeta function corresponding to the sequence $(d_n)_{n\geq 1}$ given by $d_n := \deg(\sigma^n - \gamma_0^n)$ is rational, and (d_n) satisfies the dominant root assumption, with dominant root $\deg(\sigma)$.

Proof. (i) We want to show that (δ_n) satisfies the criterion given by Proposition 2.2(ii). Suppose first that $G = \mathbf{G}_a$. Then we can identify σ with an element of $k\langle\phi\rangle$. If $\deg(\sigma) = 1$, then confinedness of σ implies that $\sigma = a \in k\langle\phi\rangle$, where $a \in k^\times$ is transcendental over $\overline{\mathbf{F}_p}$ (i.e. is not a root of unity).

It follows that $\deg(\sigma^n - \gamma\gamma_0^n) = 1 = \deg(\sigma)^n$ for all $n \in \mathbf{Z}_{>0}$. If $\deg(\sigma) \geq 2$, then we also find (by viewing σ as an element of $k\langle\phi\rangle$ of positive degree in ϕ)

$$\deg(\sigma^n - \gamma\gamma_0^n) = \deg(\sigma)^n. \tag{21}$$

Thus, in any case, $\delta_n = |\Gamma| \deg(\sigma)^n$.

Now suppose that $G = \mathbf{G}_m$. Then we can identify σ with an element of $\mathbf{Z}$ (so that $\gamma, \gamma_0 \in \{\pm 1\}$). We obtain

$$\deg(\sigma^n - \gamma\gamma_0^n) = |\sigma^n - \gamma\gamma_0^n| = |\sigma|^n - \gamma\gamma_0^n \operatorname{sgn}(\sigma)^n = \deg(\sigma)^n - \gamma\gamma_0^n \operatorname{sgn}(\sigma)^n. \tag{22}$$

Hence $\delta_n = |\Gamma| \deg(\sigma)^n$.

Finally, for the case $G = E$, we compute

$$\begin{aligned}
\sum_{\gamma\in\Gamma} \deg(\sigma^n - \gamma\gamma_0^n) &= \sum_{\gamma\in\Gamma} (\sigma^n - \gamma\gamma_0^n)(\overline{\sigma}^n - \overline{\gamma_0}^n\overline{\gamma}) \\
&= \sum_{\gamma\in\Gamma} ((\sigma\overline{\sigma})^n - \gamma\gamma_0^n\overline{\sigma}^n - \sigma^n\overline{\gamma_0}^n\overline{\gamma} + 1) \\
&= |\Gamma|(\deg(\sigma)^n + 1) - \left(\sum_{\gamma\in\Gamma} \gamma\right) \gamma_0^n\overline{\sigma}^n - \sigma^n\overline{\gamma_0}^n \left(\sum_{\gamma\in\Gamma} \gamma^{-1}\right) \\
&= |\Gamma|(\deg(\sigma)^n + 1),
\end{aligned}$$

where the last equality follows from Lemma 2.17.

(ii) For the cases $G = \mathbf{G}_a$ and $G = \mathbf{G}_m$ the desired result is immediate by substituting $\gamma = 1$ in (21) and (22) above. For $G = E$, we note that, if σ and γ_0 commute,

$$\deg(\sigma^n - \gamma_0^n) = \deg(\sigma)^n + 1 - (\gamma_0\overline{\sigma})^n - (\sigma\overline{\gamma_0})^n. \tag{23}$$

Confinedness of σ implies that $\deg(\sigma) \geq 2$, hence the desired result follows by noting that (absolute values taken as complex algebraic numbers) $|\gamma_0\overline{\sigma}| = |\sigma\overline{\gamma_0}| = \sqrt{\sigma\overline{\sigma}} = \sqrt{\deg(\sigma)}$. □

Proof of Proposition 3.13. (i) **(H1)** and **(H2)** are precisely the statements of Lemma 3.14 and 3.15 respectively. **(H3)** for the case that Γ_m is non-trivial follows from Lemma 3.16(i), while **(H3)** for Γ_m trivial and **(H4)** both follow from combining Lemma 3.16(ii) with Lemma 3.9.

(ii) If f is coseparable, then using Lemma 3.6 we obtain

$$f_n = c_n + \frac{1}{|\Gamma|} \sum_{\gamma\in\Gamma} \deg(\sigma^n - \gamma).$$

Now apply the calculations of Lemma 3.16 with $\gamma_0 = 1$, and notice that in each case (by the appearance of a factor $|\Gamma|$), the sequence $\sum_{\gamma\in\Gamma} \deg(\sigma^n - \gamma)/|\Gamma|$, and hence f_n by **(H1)**, has the desired form for application of Proposition 2.2(ii). □

Remark 3.17 A precise consideration of the value of c_n shows that

$$c_n = \begin{cases} 0 & \text{if } [G = \mathbf{G}_m,\ \Gamma = \{1\} \text{ and } \operatorname{sgn}(\sigma)^n = -1] \text{ or } [G = E]; \\ 1 & \text{if } [G = \mathbf{G}_a] \text{ or } [G = \mathbf{G}_m \text{ and } \Gamma = \{\pm 1\}]; \\ 2 & \text{if } [G = \mathbf{G}_m,\ \Gamma = \{1\} \text{ and } \operatorname{sgn}(\sigma)^n = 1]. \end{cases}$$

Combined with the calculations we saw in Lemma 3.16, this shows that for any coseparable dynamically affine map f on the projective line, we have $f_n = \deg(\sigma)^n + 1$ (note that the "case" of equation (23), where $G = E$ and $\Gamma = \{1\}$, does not give rise to a dynamically affine map on $\mathbf{P}^1$, because elliptic curves cannot be embedded into the projective line). Since $\deg(\sigma) = \deg(f)$ (follows from the commutative diagram (15)), and maps g on the projective line (that are not the identity) have exactly $\deg(g) + 1$ fixed points *with* multiplicity, this shows that the coseparable dynamically affine maps f on the projective line are precisely the ones for which f_n is *maximal* (i.e. each fixed point has multiplicity one). ◊

Remark 3.18 Bridy [9] proves his results from a slightly more explicit point of view. He classifies dynamically affine maps f on the projective line by categorizing the polynomials f_c to which they are (by a fractional linear transformation) conjugate, according to the diagram below: (here, $\mu_d \subseteq k^\times$ denotes the subgroup of d-th roots of unity)

G	Γ	$G/\lvert\Gamma\rvert$	f_c
$\mathbf{G}_a$	$\{1\}$	$\mathbf{P}^1 \setminus \{\infty\}$	Additive polynomial
	μ_d		Subadditive polynomial
$\mathbf{G}_m$	$\{1\}$	$\mathbf{P}^1 \setminus \{0, \infty\}$	Power map
	$\{\pm 1\}$	$\mathbf{P}^1 \setminus \{\infty\}$	Chebyshev polynomial
E	$\neq \{1\}$	$\mathbf{P}^1$	Lattès map

Table 2: Classification of dynamically affine maps on $\mathbf{P}^1$.

Using this terminology, f is coseparable precisely when f_c is either inseparable, or a separable (sub)additive polynomial for which $f_c'(0)$ is transcendental over k (cf. [9, Thm. 1.2 & 1.3]). ◊

As a final remark, we describe the relation between our definition and Silverman's definition [40, §6.8] for dynamically affine maps in dimension one; it turns out that the only difference is that we "allow" (while Silverman does not) $\sigma : \mathbf{G}_a \to \mathbf{G}_a$ to be equal to the map $x \mapsto a_0 x$, for $a_0 \in k^\times$ transcendental over $\mathbf{F}_p$.

Lemma 3.19 *Let G be a connected (commutative) algebraic group of dimension one, and let $\sigma \in \operatorname{End}(G)$ be an isogeny.*

(i) If $\deg(\sigma) \geq 2$, then σ is confined.

(ii) If σ is confined and not coseparable, then $\deg(\sigma) \geq 2$ (in other words, "confined automorphisms are coseparable").

Proof. Since G is connected of dimension one, 0 is the only endomorphism with infinite kernel, so σ is confined if and only if $\sigma^n \neq 1$ for all $n \in \mathbf{Z}_{>0}$. This makes (i) clear. For (ii), suppose that σ has degree

one, i.e. $\sigma \in \mathrm{Aut}(G)$. If σ has finite order, then σ is not confined. This proves the cases $G = \mathbf{G}_m$ and $G = E$ by finiteness of $\mathrm{Aut}(G)$. Now suppose that $\sigma \in \mathrm{Aut}(\mathbf{G}_a)$ has infinite order. Then $\sigma = a_0$ for some $a_0 \in k$ transcendental over $\mathbf{F}_p$, and we see that $\sigma^n - 1$ has degree one for all $n \in \mathbf{Z}_{>0}$, hence σ is coseparable. □

3.4 Proof of Main Results

In this section, we will prove Theorems 3.7 and 3.8. Let $f : V \to V$ be a dynamically affine map satisfying **(H1)**-**(H4)**.

Using Lemma 3.6, we can write

$$\zeta_f(z) = \exp\left(\sum_{n\geq 1} \frac{c_n}{n} z^n\right) \exp\left(\sum_{\substack{n\geq 1\\ \gamma\in\Gamma}} \frac{\#\ker(\sigma^n - \gamma)}{n} z^n\right)^{1/|\Gamma|}.$$

If σ is coseparable, then $\#\ker(\sigma^n - \gamma) = \deg(\sigma^n - \gamma)$ for all $\gamma \in \Gamma$, so it follows immediately from **(H1)** and **(H3)** (applied with $m = 0$) that ζ_f is root-rational. By Lemma 2.6, ζ_f^* is also root-rational.

Suppose now that σ is not coseparable. Let s_m, γ_m, Γ_m and N as in the statement of the hypotheses, which, by Proposition 2.16(vi), then all exist.

Lemma 3.20 *Let $m \in \mathbf{Z}_{\geq 0}$. Then*

(i) $S_m := \{n \in \mathbf{Z}_{>0} \mid v(\sigma^n - \gamma) \geq m \text{ for some } \gamma \in \Gamma\} = s_m\mathbf{Z}_{>0}$.

(ii) For every $n \in \mathbf{Z}_{>0}$, $\{\gamma \in \Gamma \mid v(\sigma^{s_m n} - \gamma) \geq m\} = \Gamma_m \gamma_m^n$.

Proof. (i) By Proposition 2.16(iv), we have $v(\sigma^{s_m n} - \gamma_m^n) \geq v(\sigma^s - \gamma_m) \geq m$, so $S_m \supseteq s_m\mathbf{Z}_{>0}$. Now suppose to the contrary that there exists an $n \in S_m \setminus s_m\mathbf{Z}_{>0}$. Then there exists a $\gamma \in \Gamma$ such that $v(\sigma^n - \gamma) \geq m$, and we can write $n = ds_m + r$ for $0 < r < s_m$. We obtain

$$m \leq v(\sigma^n - \gamma) = v(\sigma^r(\sigma^{ds_m} - \gamma_m^d) + (\sigma^r - \gamma\gamma_m^{-d})\gamma_m^d) = v(\sigma^r - \gamma\gamma_m^{-d}) < m,$$

a contradiction.

(ii) We know that $v(\sigma^{s_m n} - \gamma_m^n) \geq m$, so for any $\gamma \in \Gamma$,

$$v(\sigma^{s_m n} - \gamma) \geq m \iff v(\gamma - \gamma_m^n) \geq m \iff v(\gamma\gamma_m^{-n} - 1) \geq m \iff \gamma\gamma_m^{-n} \in \Gamma_m \iff \gamma \in \Gamma_m\gamma_m^n.$$

□

Proof of Theorem 3.7 and Theorem 3.8. Define

$$Z_{f,\geq m} := \sum_{n\geq 1} \sum_{\substack{\gamma\in\Gamma\\ v(\sigma^n-\gamma)\geq m}} \deg(\sigma^n - \gamma) p^{-v(\sigma^n-\gamma)} z^n, \quad Z_{f,m} := p^{-m} \sum_{n\geq 1} \sum_{\substack{\gamma\in\Gamma\\ v(\sigma^n-\gamma)=m}} \deg(\sigma^n - \gamma) z^n,$$

and denote by $\zeta_{f,\geq m}$ and $\zeta_{f,m}$ the corresponding "full zeta analogues". By Lemma 3.20, we have

$$Z_{f,\geq m} = \sum_{n\geq 1}\sum_{\gamma\in\Gamma_m} \deg(\sigma^{s_m n} - \gamma\gamma_m^n) p^{-v(\sigma^{s_m n}-\gamma\gamma_m^n)} z^{s_m n},$$

and

$$\begin{aligned} Z_{f,m} &= Z_{f,\geq m} - Z_{f,\geq(m+1)} \\ &= p^{-m}\left(\sum_{n\geq 1}\sum_{\gamma\in\Gamma_m} \deg(\sigma^{s_m n} - \gamma\gamma_m^n) z^{s_m n} - \sum_{n\geq 1}\sum_{\gamma\in\Gamma_{m+1}} \deg(\sigma^{s_{m+1} n} - \gamma\gamma_{m+1}^n) z^{s_{m+1} n}\right). \end{aligned}$$

In particular, we see that $\zeta_{f,m}$ is $(p^m s_{m+1})$-root-rational by **(H3)**. We thus obtain an infinite product expansion for the full zeta function ζ_f in terms of root-rational power series as follows:

$$\zeta_f(z) = \exp\left(\sum_{n\geq 1}\frac{c_n}{n} z^n\right)\left(\prod_{m\geq 0}\zeta_{f,m}\right)^{1/|\Gamma|}. \tag{24}$$

Now, the "tail" of this expansion can be written as (recall that we defined $s := s_N$ and $\tilde{\gamma} := \gamma_N$)

$$\prod_{m\geq N}\zeta_{f,m} = \zeta_{f,\geq N} = \exp\left(\sum_{n\geq 1}\frac{\deg(\sigma^{sn} - \tilde{\gamma}^n)}{sn} p^{-v(\sigma^{sn}-\tilde{\gamma}^n)} z^{sn}\right).$$

By Lemma 3.9, σ^s and $\tilde{\gamma}$ commute. Thus, when we define $\tau := \sigma^s\tilde{\gamma}^{-1}$, we can rewrite this in terms of the naive zeta function as

$$Z_{f,\geq N} = \sum_{n\geq 1}\deg(\tau^n - 1) p^{-v(\tau^n-1)} z^{sn}.$$

Now let $R := \mathrm{End}(G)$, and $M := \max\{N, (\rho(R,v)+1)/(p-1)\}$ (cf. Proposition 2.16(v)). Define $r := s_M$, and $\kappa := \tau^{r/s}$. Then

$$Z_{f,\geq M} = \sum_{n\geq 1}\deg(\kappa^n - 1) p^{-v(\kappa^n-1)} z^{rn}.$$

If we set $C := v(\kappa^n - 1) \geq M$, then Proposition 2.16(v) tells us that

$$v(\kappa^n - 1) = \begin{cases} C + v(n) & \text{if } \mathrm{char}(R) = 0; \\ C p^{v_p(n)} & \text{if } \mathrm{char}(R) = p > 0. \end{cases}$$

By **(H4)**, the linear recurrence $\deg(\tau^n - 1)$ satisfies the dominant root assumption, let us say with unique dominant root $\lambda \in \mathbf{C}$. This implies that the sequence $\deg(\kappa^n - 1)$ has unique dominant root $\Lambda := \lambda^{r/s}$; let us say with multiplicity $\mu \in \mathbf{Z}$ (the multiplicity is integral by **(H3)** and Proposition 2.2(ii)). Expanding $\deg(\kappa^n - 1)$ in terms of its roots, we find

$$Z_{f,\geq M} = \sum_{n\geq 1}\mu\Lambda^n z^n \cdot \begin{cases} p^{-C}|n|_p & \text{if } \mathrm{char}(R) = 0 \\ p^{-C|n|_p^{-1}} & \text{if } \mathrm{char}(R) = p \end{cases} + R(z),$$

where $R(z)$ is some power series with radius of convergence $> 1/|\Lambda|$. Lemma 3.10 with $h = 1$ and $\beta = p^{-C}$ now shows that $Z_{f,\geq M}$ has a natural boundary at the circle of radius $1/|\Lambda|$, hence the same holds for $\zeta_{f,\geq M}$ (Lemma 2.1). The expansion into root-rational functions (24) thus splits up as

$$\zeta_f = \underbrace{\exp\left(\sum_{n\geq 1}\frac{c_n}{n}z^n\right)\left(\prod_{0\leq m<M}\zeta_{f,m}\right)^{1/|\Gamma|}}_{\text{root-rational}}\underbrace{\Big(\zeta_{f,\geq M}(z)\Big)^{1/|\Gamma|}}_{\text{natural boundary}},$$

which shows that ζ_f has a natural boundary, hence completing the proof of Theorem 3.7.

A similar expression for the tame zeta function

$$\zeta_f^* = \underbrace{\exp\left(\sum_{p\nmid n}\frac{c_n}{n}z^n\right)\left(\prod_{0\leq m<M}\zeta_{f,m}^*\right)^{1/|\Gamma|}}_{\big(p^M|\Gamma|r\big)\text{-root-rational}}\underbrace{\Big(\zeta_{f,\geq M}^*(z)\Big)^{1/|\Gamma|}}_{\big(p^{C+1}|\Gamma|r\big)\text{-root-rational}},$$

proves Theorem 3.8. □

Remark 3.21 The proof shows that ζ_f^* is $\big(p^{C+1}|\Gamma|r\big)$-root-rational. Note however that we could, at the cost of a messier explicit "exponent", weaken **(H1)** and **(H3)** slightly; replacing the rationality assumption with just root-rationality, the argument still works. ◊

Remark 3.22 Despite the fact that ζ_f for non-coseparable f has a natural boundary (and thus, is far from being root-rational (4)), it still has several (infinite) product expansions in terms of root-rational functions: we have the (very general) prime orbit expansion (9); the expansion in terms of tame zeta functions (11); and the explicit expansion (24) given in the proof. ◊

For completeness we record:

Proof of Theorem 3.11 and 3.12. This follows by combining Theorem 3.7 & 3.8 with Proposition 3.13. □

4 Dynamics on Algebraic Groups

We now turn to the study of the Artin-Mazur zeta function for endomorphisms of algebraic groups. Let G be a connected algebraic group over an algebraically closed field k of characteristic $p > 0$, and let $f : G \to G$ be a confined endomorphism. We will again denote by f_n the (finite) number of fixed points of $f^{\circ n}$. The main conjecture is:

Conjecture 4.1 *We can write*

$$f_n = d_n m_n a_n, \tag{25}$$

where, for gcd sequences $r_n \in \mathbf{Q}^\times, s_n, t_n \in \mathbf{Z}$; all with period not divisible by p,

(i) (d_n) *has root-rational zeta function;*

(ii) $m_n = r_n |n|_p^{s_n}$;

(iii) $\log_p(a_n) = |n|_p^{-1} t_n$.

As of now, the proof of this conjecture is almost, but not entirely, complete. In particular, we do not yet know how to control the "degree sequence" $\deg(\sigma^n - 1)$, where σ is an endomorphism of $\mathbf{G}_a^r$ for $r \in \mathbf{Z}_{\geq 2}$.

4.1 Splitting up an Algebraic Group

The idea of attacking the conjecture is to repeatedly reduce the problem to "simpler" algebraic groups by finding a normal algebraic subgroup preserved by the endomorphism. The starting point for this is the following lemma.

Lemma 4.2 *Suppose $N \lhd G$ is a connected normal algebraic subgroup such that $f(N) \subseteq N$. Let $g := f|_N : N \to N$ and $h := \tilde{f} : G/N \to G/N$ be the induced endomorphisms. Then g and h are confined and $f_n = g_n h_n$ for all $n \in \mathbf{Z}_{>0}$.*

Proof. Replacing f^n by f, it suffices to prove the result for $n = 1$. Note that confinedness of g follows immediately from confinedness of f. Now, by [45, Thm. 10.1], the map (not necessarily a morphism of algebraic groups) $N \to N$, $n \mapsto g(n)n^{-1}$ is surjective. Suppose $a \in A$ is a fixed point of $\tilde{f}$. Then a lifts to an $x \in G$ such that $f(x) = nx$ for some $n \in N$. Now, if $m := m_x \in N$ is such that $g(m)m^{-1} = n$, then $m^{-1}x$ is a lift of a that is a fixed point of f. For any fixed point b of g, we now have that $bm^{-1}x$ is a fixed point of f.

Conversely, suppose that $f(y) = y$ for some lift $y \in G$ of a. Write $y = n_y x$ for some $n_y \in N$ and define $b_y := n_y m \in N$. Then $y = b_y m^{-1} x$, and $b_y = y(m^{-1}x)^{-1}$ is a fixed point of g. We thus obtain a bijection $\mathrm{Fix}(g) \times \mathrm{Fix}(h) \to \mathrm{Fix}(f)$, $(b, \tilde{x}) \mapsto (bm_x^{-1}x)$. □

Now, the "reduction process" goes as follows:

(i) By Chevalley's structure theorem for algebraic groups (Theorem 2.23), we can reduce the case of a general connected algebraic group G to the case of a connected linear algebraic group N and an abelian variety A by applying Lemma 4.2. Indeed, note that $f(N) \subseteq N$, because otherwise we would obtain a non-trivial morphism $N \xrightarrow{f} N \to G/N = A$, which is impossible [15, Lem. 2.3].

(ii) The case of an abelian variety is covered in [10]. Here we see that the fixed point sequence indeed has the desired form (25) (with $a_n \equiv 1$), by combining [loc. cit., Prop. 2.3 & 2.7].

(iii) The case of a linear algebraic group N can be reduced by considering the *radical* $R \lhd N$, defined to be the unique maximal connected solvable normal subgroup of N. It is preserved under endomorphisms [45, 7.1(c)]. The quotient $S := N/R$ has trivial radical, i.e. is *semisimple*. Since R is the identity component of the intersection of all Borel subgroups (see Definition 2.22) of G [42, Thm. 6.2.7(iii)], it follows that R is closed in N. Therefore, by Lemma 2.26, both R and S are again linear algebraic groups.

(iv) The number of fixed points of an endomorphism σ of a connected semisimple linear algebraic group S are given by [45, Thm. 11.16]. Here it is shown that if σ permutes the *simple components* [33, Thm. 21.51] of S in a single orbit, say of size ℓ, then there exists a positive real algebraic number $q = q(\sigma)$, integers $D_j \in \mathbf{Z}_{\geq 0}$ and roots of unity $\epsilon_j = \epsilon_j(\sigma) \in \overline{\mathbf{Q}}$, such that

$$\#\operatorname{Fix}(\sigma) = q^N \prod_j \left(q^{D_j} - \epsilon_j\right), \tag{26}$$

where $N = \sum_j (D_j - 1)$. For $n \in \mathbf{Z}_{>0}$ coprime to ℓ, we have $q(\sigma^n) = q(\sigma)^n$ and $\epsilon_j(\sigma^n) = \epsilon_j(\sigma)^n$, while the integers D_j are independent of n. For arbitrary $\sigma : S \to S$, however, the simple components of S might not be permuted in a single orbit, so in general $\#\operatorname{Fix}(\sigma)$ is a product of factors of the form (26). Every power σ^n of σ acts as a different permutation on the simple components, but this permutation only depends on $\gcd(n, L)$, where $L := \prod_i \ell_i$ denotes the product of the sizes ℓ_i of the orbits under σ of the simple components of S. We thus obtain a formula of the following form: (here $\mathbf{1}_{\gcd(n,L)=d}$ is one when $\gcd(n, L) = d$, and zero otherwise)

$$\#\operatorname{Fix}(\sigma^n) = \sum_{d|L} \mathbf{1}_{\gcd(n,L)=d} \prod_i \left[q_{d,i}^{N_{d,i}(n/d)} \prod_j \left(q_{d,i}^{D_{d,i,j}(n/d)} - \epsilon_{d,i,j}^{(n/d)} \right) \right].$$

Thus, by applying Proposition 2.2(ii) and 2.7 combined with Remark 2.5, it follows that that ζ_σ is (L-)root-rational (hence the fixed point sequence of σ has the desired form (25) with $m_n \equiv a_n \equiv 1$).

(v) The case of a connected solvable algebraic group R (the radical arising from (iii)) can be further reduced: there exists [33, Thm. 16.33] a normal connected unipotent algebraic subgroup U of R such that the quotient R/U is a *torus* T, i.e. isomorphic to $\mathbf{G}_m^s$ for some $s \in \mathbf{Z}_{\geq 0}$. There are no non-trivial morphisms $U \to T$ [16, Cor. IV.2.2.4], so U is preserved by any endomorphism of R.

(vi) A unipotent algebraic group U is solvable [42, Cor. 2.4.13]. The commutator subgroup of a connected algebraic group is closed and connected [42, Cor. 2.2.8], and is preserved by endomorphisms (since group homomorphisms send commutators to commutators). As the quotient of a unipotent algebraic group by a closed normal subgroup is unipotent [16, Prop. IV.2.2.3], we thus reduce to the case of general U to the case of (several) connected commutative unipotent algebraic groups.

(vii) The structure of connected commutative unipotent algebraic groups U is well known. Indeed, [37, Thm. VII.1] such U are always isogenous[8] to a direct product $W_1 \times \cdots \times W_t$ of additive groups of rings W_i of *truncated Witt vectors* over k. For a complete (but irrelevant for our purposes) introduction to Witt vectors, we refer to [35]. It turns out that the *ring of Witt vectors* $W(k)$ over k is a discrete

[8] We call two algebraic groups G, H *isogenous* when there exist isogenies $\sigma : G \to H$ and $\tau : H \to G$.

valuation ring of characteristic zero with uniformizer p and residue field k [49, Satz 6], while a *truncated ring of Witt vectors* $W^{(d)}$ (of which the additive group has the structure of an algebraic group with underlying variety $\mathbf{A}^d$) is (defined to be) the quotient $W(k)/(p^d)$ for some $d \in \mathbf{Z}_{\geq 0}$. In particular, $p^d W^{(d)} = 0$. Since U is isogenous to a product of such $W^{(d)}$, we obtain a decomposition series of connected commutative unipotent (using [16, Prop. IV.2.2.3] again) algebraic groups

$$U \supseteq pU \supseteq p^2U \supseteq \cdots \supseteq 0,$$

in which each successive quotient is a connected commutative unipotent algebraic group of elements of order (dividing) p, hence, by [37, Prop. VII.11], is isomorphic to $\mathbf{G}_a^r$ for some $r \in \mathbf{Z}_{\geq 0}$. Since pU is clearly preserved by an endomorphism of U, we thus reduce the case of an arbitrary commutative unipotent algebraic group U to that of a power $\mathbf{G}_a^r$ of the additive group.

The following diagram illustrates the reduction process described above:

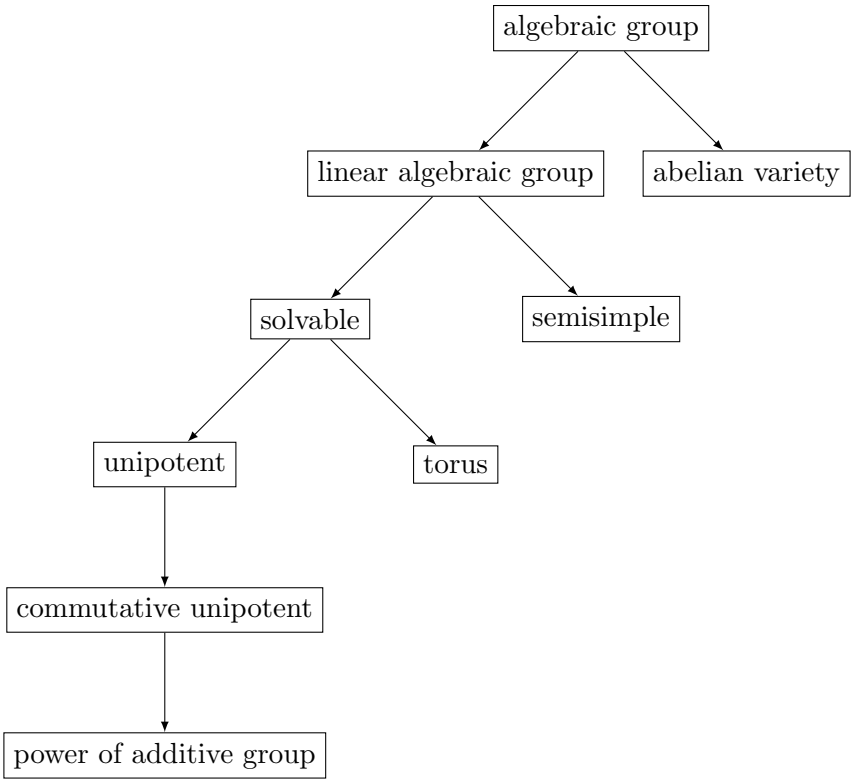


Figure 5: Splitting up an algebraic group.

We have already solved the case for abelian varieties (step (ii)) and semisimple algebraic groups (step (iv)), so it remains to determine the fixed point sequence $\#\operatorname{Fix}(\sigma^n)$ for confined endomorphisms σ of $\mathbf{G}_m^s$ and of $\mathbf{G}_a^r$. This will be the main concern of the next two subsections. Since we are now dealing with *commutative* algebraic groups, the set of endomorphisms $\operatorname{End}(\mathbf{G}_m^s)$ and $\operatorname{End}(\mathbf{G}_a^r)$ admits a ring structure. We can therefore (similar to Section 3) "count" the fixed point sequence in terms of kernels of endomorphisms:

$$\#\operatorname{Fix}(\sigma^n) = \#\ker(\sigma^n - 1) = \deg(\sigma^n - 1)/\deg_i(\sigma^n - 1),$$

where it thus suffices to control the degree sequence $\deg(\sigma^n - 1)$ and the inseparability degree sequence $\deg_i(\sigma^n - 1)$. To prepare for this we will first introduce some algebra. Let R be a (possibly non-commutative) ring with unit and without zero divisors. We will say that R is a *principal ideal domain* when every right ideal is a principal right ideal (i.e. of the form xR for some $x \in R$) and every left ideal is a principal left ideal. For elements $a, b \in R$, we will say that a is a *total divisor* of b if there exists a two-sided ideal $I \subseteq R$ such that $bR \subseteq I \subseteq aR$ (or, equivalently [25, p. 40], if there exists a two-sided ideal I such that $Rb \subseteq I \subseteq Ra$). We will denote by $M_n(R)$ the ring of $n \times n$ matrices with entries in R, and by $\mathrm{GL}_n(R) \subseteq M_n(R)$ the unit group.

Lemma 4.3 *Let R be a (possibly non-commutative) principal ideal domain, and let $x \in M_n(R)$. Then there exist $P, Q \in \mathrm{GL}_n(R)$ such that PxQ is in diagonal form $\{e_1, \cdots, e_s, 0, \cdots\}$, with e_i a total divisor of e_j whenever $i < j$.*

Proof. [25, Thm. 3.16]. □

The diagonal matrix PxQ in Lemma 4.3 is called the "Smith normal form" of R.

4.2 Powers of the Multiplicative Group

Let $T \cong \mathbf{G}_m^s$ for some $s \in \mathbf{Z}_{\geq 0}$ be a torus. Then $\mathrm{End}(T) \cong M_s(\mathbf{Z})$, the ring of $s \times s$ matrices with coefficients in $\mathbf{Z}$.

Proposition 4.4 *Let $\sigma \in \mathrm{End}(T) \cong M_s(\mathbf{Z})$. Then*

$$\deg(\sigma) = |\det(\sigma)|, \qquad \deg_i(\sigma) = p^{v_p(\det(\sigma))}. \tag{27}$$

Proof. Using Lemma 4.3, let $P, Q \in \mathrm{GL}_s(\mathbf{Z})$ such that $P\sigma Q$ is in Smith normal form. Since $P\sigma Q$ is diagonal, we have $\deg(P\sigma Q) = |\det(P\sigma Q)|$ and $\deg_i(P\sigma Q) = p^{v_p(\det(P\sigma Q))}$. We also know that $\deg(P) = \deg(Q) = 1$, because P and Q automorphisms of T. Therefore $\deg(\sigma) = \deg(P\sigma Q) = |\det(P\sigma Q)| = |\det(\sigma)|$, and $\deg_i(\sigma) = \deg_i(P\sigma Q) = p^{v_p(\det(P\sigma Q))} = p^{v_p(\det(\sigma))}$. □

Using the proposition we can now control the fixed point sequence $\#\,\mathrm{Fix}(\sigma^n)$ for $\sigma \in \mathrm{End}(T)$ as follows: let $\tau = P\sigma P^{-1} \in M_s(\overline{\mathbf{Q}_p})$ conjugate to σ and upper triangular with diagonal $\{\lambda_1, \cdots, \lambda_s\}$. Then (here, $|\cdot|_p$ denotes the p-adic norm on $\overline{\mathbf{Q}_p}$)

$$\begin{aligned} \#\ker(\sigma^n - 1) &= \det(\sigma^n - 1)|\det(\sigma^n - 1)|_p \\ &= \det(\tau^n - 1)|\det(\tau^n - 1)|_p \\ &= \prod_{i=1}^{s} (\lambda_i^n - 1)|\lambda_i^n - 1|_p. \end{aligned}$$

The λ_i are algebraic integers, since they are the eigenvalues of the matrix σ, which has integer entries. Let L be the finite extension of $\mathbf{Q}_p$ obtained by adjoining all λ_i, denote by $\mathcal{O} \subseteq L$ the ring of integers, and let $\mathfrak{m} = \{x \in \mathcal{O} \mid |x|_p < 1\}$ denote the unique maximal ideal of $\mathcal{O}$. The maximal ideal $\mathfrak{m}$ gives rise to a discrete valuation $v : \mathcal{O} \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ satisfying $|x|_p = p^{-v(x)/e}$, where e denotes the ramification index of $L/\mathbf{Q}_p$. For a given i there are two options:

(a) If $\lambda_i \notin \mathcal{O}^\times$, then $|\lambda_i^n - 1|_p = 1$ for all $n \in \mathbf{Z}_{>0}$.

(b) If $\lambda_i \in \mathcal{O}^\times$, then, since $\mathcal{O}/\mathfrak{m}$ is a finite field, we find that $\lambda^t - 1 \in \mathfrak{m}$ for some $t \in \mathbf{Z}_{>0}$. Using Proposition 2.16(vi), we thus have that $v(\lambda^r - 1)$ gets arbitrarily large as r ranges over $\mathbf{Z}_{>0}$. Denote by $t_j \in \mathbf{Z}_{>0}$ the smallest positive integer such that $v(\lambda_i^{t_j} - 1) \geq j$. Then $t_j \mid t_{j+1}$ for all j. For any $m \in \mathbf{Z}_{>0}$, the sequence (b_n) defined by

$$b_n := \begin{cases} v(\lambda_i^n - 1) & \text{if } t_m \nmid n; \\ v(\lambda_i^{t_m} - 1) & \text{else,} \end{cases}$$

is a gcd sequence: indeed, $b_n = \max_j\{t_j \mid n\} = \max_j\{t_j \mid \gcd(n, t_m)\} = b_{\gcd(n,t_m)}$. Now set $m := (e+1)/(p-1)$ and $t := t_m$. Using Proposition 2.16(v), we obtain $v(\lambda_i^n - 1) = b_n + \mathbf{1}_{t|n} v(n)$. Hence

$$|\lambda_i^n - 1|_p = p^{-b_n/e} |n|_p^{\mathbf{1}_{t|n}}.$$

In both cases, $(\lambda_i^n - 1)|\lambda_i^n - 1|_p$ satisfies the desired form (25), hence the same holds for σ_n.

4.3 Powers of the Additive Group

The last piece needed for solving Conjecture 4.1, is understanding the fixed point sequence for endomorphisms of $A := \mathbf{G}_a^r$, for some $r \in \mathbf{Z}_{\geq 0}$. We have $\mathrm{End}(A) \cong M_r(R)$, where $R := k\langle\phi\rangle$ denotes the non-commutative polynomial ring in the Frobenius ϕ, with multiplication rule $\phi a = a^p \phi$ for $a \in k$. As we did for tori, we would like to determine a way to "measure" the degree and inseparability degree of an endomorphism $\sigma \in \mathrm{End}(A)$. We could hope for something similar to (27), but, since R is non-commutative, there is not a straightforward notion of "determinant" on $M_r(R)$. Instead, we will use (cf. [47]) the *Dieudonné determinant* [17], which can be defined for a matrix ring over any (not necessarily commutative) local[9] ring S with unit as follows: if we denote by $(S^\times)^{\mathrm{ab}} := S^\times/[S^\times, S^\times]$ the abelianization of the unit group, then the Dieudonné determinant is the function $\mathrm{ddet} : \mathrm{GL}_r(S) \to (S^\times)^{\mathrm{ab}}$ uniquely determined [36, Thm. 2.2.5] by the following properties:

(a) $\mathrm{ddet}(1) = 1$.

(b) ddet is invariant under elementary row operations.

(c) If $M \in \mathrm{GL}_n(S)$, $a \in S^\times$, and M' is obtained from M by left-multiplying one of the rows of M by a, then $\mathrm{ddet}(M') = \overline{a}\,\mathrm{ddet}(M)$, where $\overline{a}$ denotes the reduction of a to $(S^\times)^{\mathrm{ab}}$.

It turns out that [loc. cit.] ddet is multiplicative; i.e. $\mathrm{ddet}(AB) = \mathrm{ddet}(A)\,\mathrm{ddet}(B)$.

Now denote by Q the (left) skew field of fractions of R (see [14, Cor. 1.3.3 & Prop. 1.3.4]). Then Q is (obviously) local, so we can apply the above to obtain a map $\mathrm{ddet} : \mathrm{GL}_r(Q) \to (Q^\times)^{\mathrm{ab}}$, which can be extended to a semigroup homomorphism $\mathrm{ddet} : M_r(Q) \to Q^{\mathrm{ab}} := (Q^\times)^{\mathrm{ab}} \cup \{0\}$ by setting it zero outside of $\mathrm{GL}_r(Q)$.[10] Now consider the map $\deg : R \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ measuring the degree in ϕ. We can extend

[9] Meaning that the subset of non-units forms a two-sided ideal.

[10] Note that R is also a local ring, so we can also construct a map $\mathrm{ddet} : \mathrm{GL}_r(R) \to (R^\times)^{\mathrm{ab}}$ (which is indeed the restriction of $\mathrm{ddet} : \mathrm{GL}_r(Q) \to (Q^\times)^{\mathrm{ab}}$ to $\mathrm{GL}_r(R)$). However, without introducting Q, there is no straightforward way of extending it to $M_r(R)$. We could, similar to the above, define $\mathrm{ddet} : M_r(R) \to (R^\times)^{\mathrm{ab}} \cup \{0\}$ by setting it zero outside of $\mathrm{GL}_r(R)$, but then we discard valuable information: for example, $\phi \in R \cong M_1(R)$ would get mapped to zero; we really have to consider the "extended" version of ddet for it to retain information about the degree and inseparability degree of endomorphisms.

this [47] to a well-defined map $\deg : Q \to \mathbf{Z} \cup \{\infty\}$ satisfying $\deg(ab) = \deg(a) + \deg(b)$, by setting $\deg(r/s) := \deg(r) - \deg(s)$. Since deg is zero on commutators, it factors over $Q \to Q^{\mathrm{ab}}$, so we obtain a semigroup homomorphism $\deg : Q^{\mathrm{ab}} \to \mathbf{Z} \cup \{\infty\}$. Similarly we can extend the semigroup homomorphism $v_\phi : k\langle\phi\rangle \to \mathbf{Z}_{\geq 0} \cup \{\infty\}$ to a map $v_\phi : Q^{\mathrm{ab}} \to \mathbf{Z} \cup \{\infty\}$.

Proposition 4.5 *Let $\sigma \in \mathrm{End}(A) \cong M_r(R)$. Then*

$$\deg(\sigma) = p^{\deg(\mathrm{ddet}\,\sigma)}, \qquad \deg_i(\sigma) = p^{v_\phi(\mathrm{ddet}\,\sigma)} \tag{28}$$

Proof. This follows from the same argument we saw in Proposition 4.4: it is clear that deg and $\deg_i$ take the desired form on diagonal elements, and both are (just like ddet) invariant under taking Smith normal forms. □

Note that an immediate corollary of the proposition is that for $u \in \mathrm{GL}_r(R)$, we have $\deg(\mathrm{ddet}\,u) = 0 = v_\phi(\mathrm{ddet}\,u)$. Now, as we did for tori following Proposition 4.4, we would like to use (28) to control the fixed point sequence $\#\,\mathrm{Fix}(\sigma^n) = \deg(\sigma^n - 1)/\deg_i(\sigma^n - 1)$ for a confined endomorphism σ of A. At the time of writing, we do not yet know how to control the degree sequence, so let us show what happens for the inseparability degree sequence instead:

Lemma 4.6 *Let $\sigma \in \mathrm{End}(A) \cong M_r(R)$ be a confined endomorphism. There exists a gcd sequence $t_n \in \mathbf{Z}$ with period not divisible by p such that $\deg_i(\sigma^n - 1) = p^{|n|_p^{-1} t_n}$.*

Proof. Let $\tau \in \mathrm{End}(A)$ be any endomorphism, and let $u, v \in \mathrm{GL}_r(R)$ such that $u\tau v$ is in Smith normal form with diagonal entries $e_1, \cdots, e_r \in R$. Then

$$v_\phi(\mathrm{ddet}(\tau)) = v_\phi(\mathrm{ddet}(u)) + v_\phi(\mathrm{ddet}(\tau)) + v_\phi(\mathrm{ddet}(v)) = v_\phi(\mathrm{ddet}(u\tau v)) = \sum_i v_\phi(e_i)$$

In particular, $v_\phi\,\mathrm{ddet}\,\tau > 0$ if and only if $e_i \equiv 0 \pmod{\phi}$ for at least one i, which happens precisely when the composition $M_r(R) \xrightarrow{(\mathrm{mod}\ \phi)} M_r(k) \xrightarrow{\det} k$ is zero at $u\tau v$. Since u, v remain invertible modulo ϕ, we thus find that $v_\phi\,\mathrm{ddet}\,\tau > 0 \iff \det\bar{\tau} = 0$, where $\bar{\tau} \in M_r(k)$ denotes the reduction of τ modulo ϕ.

Now let $n \in \mathbf{Z}_{>0}$, and write $n = p^m u$, where u is coprime to p. Then

$$\deg_i(\sigma^n - 1) = \deg_i(\sigma^u - 1)^{p^m} = \deg_i(\sigma^u - 1)^{|n|_p^{-1}}.$$

Now, if we denote by Φ_d the d-th cyclotomic polynomial, then $\sigma^u - 1 = \prod_{d|u} \Phi_d(\sigma)$, so

$$\log_p \deg_i(\sigma^u - 1) = v_\phi\,\mathrm{ddet}(\sigma^u - 1) = \sum_{d|u} v_\phi\,\mathrm{ddet}(\Phi_d(\sigma)).$$

Now, if $v_\phi\,\mathrm{ddet}(\Phi_d(\sigma)) > 0$, then

$$\det(\Phi_d(\bar{\sigma})) = \prod_{\substack{\zeta \in k \\ \Phi_d(\zeta) = 0}} \det(\bar{\sigma} - \zeta) = 0,$$

so a d-th primitive root of unity ζ is an eigenvalue of $\bar{\sigma}$. This can only hold for a finite set of $d_j \in \mathbf{Z}_{>0}$ (all coprime to p), so we obtain, for all $n \in \mathbf{Z}_{>0}$

$$\log_p \deg_i(\sigma^n - 1) = |n|_p^{-1} t_n,$$

where $t_n := \sum_j \mathbf{1}_{d_j|n} v_\phi(\mathrm{ddet}(\Phi_{d_j}(\sigma)))$ is a gcd sequence with period $\prod_j d_j$. □

5 A Note on Bridy's Proof

In this section, k denotes an integer, while we reserve the letter K for an algebraically closed field.

Bridy's proof [9] of a weaker version of Theorem A, i.e. with "has a natural boundary" replaced by "is transcendental", relies heavily on the theory of *automatic sequences*; which we will quickly introduce here. Our main reference is [1]. Let $k \in \mathbf{Z}_{\geq 2}$. A *$k$-automaton* over a certain set S (called the *output alphabet*) is a finite directed graph with edges labelled by elements of $\{0, \cdots, k-1\}$ and vertices labelled by elements of S, together with a distinguished "start" vertex v_{start}. Associated to a k-automaton is a sequence $(a_n)_{n\geq 0}$ of elements of S, produced in the following way:

1. For $n \in \mathbf{Z}_{\geq 0}$, write $n = n_0 + n_1 k + \cdots + n_r k^r$ in base k.
2. Starting at v_{start}, trace the graph associated to the k-automaton (moving from vertex to vertex) in order along the edges labelled by $n_0, n_1, \cdots, n_r$, ending at a certain vertex v_{end} (in the case that $n = 0$, we have $v_{\text{end}} = v_{\text{start}}$).
3. Define $a_n \in S$ to be the label of v_{end}.

We will call a sequence $(a_n)_{n\geq 0}$ of elements of S *k-automatic* if there exists a k-automaton producing it according to the recipe above. Essential for Bridy's proof are the following two results from automata theory:

Theorem 5.1 (Christol, [12]) *A formal power series $\sum_{n\geq 0} a_n t^n \in \mathbf{F}_p[[t]]$ is algebraic over $\mathbf{F}_p(t)$ if and only if (a_n) is p-automatic.*

Proof. [1, Thm. 12.2.5]. □

Theorem 5.2 (Cobham, [13]) *Let $p, q \in \mathbf{Z}_{>0}$ be multiplicatively independent positive integers (that is, $\log(p)/\log(q) \notin \mathbf{Q}$). If a sequence (a_n) is both p-automatic and q-automatic, then it is eventually periodic.*

Proof. [1, Thm. 11.2.2]. □

The following lemma is also frequently used:

Lemma 5.3 *Let S_1, S_2, S_3 be sets, and let $(a_n)_{n\geq 0}$ be a k-automatic sequence with values in S_1.*

(i) For any $m \in \mathbf{Z}_{>0}$ and $b \in \mathbf{Z}_{\geq 0}$, the subsequence $(a_{mn+b})_{n\geq 0}$ is k-automatic.

(ii) If $(b_n)_{n\geq 0}$ is a k-automatic sequence with values in S_2, and $f : S_1 \times S_2 \to S_3$ is any map, then the sequence $(f(a_n, b_n))_{n\geq 0}$ is k-automatic.

Proof. The first result is [1, Thm. 6.8.1]. The second result is [1, Cor. 5.4.5]. □

The idea of Bridy's argument is now as follows: suppose to the contrary that the dynamical zeta function ζ_f associated to a dynamically affine map $f : \mathbf{P}^1 \to \mathbf{P}^1$ on the projective line, arising from a non-coseparable $\sigma \in \mathrm{End}(G)$, is algebraic over $\mathbf{Q}(t)$. Then the same holds for the naive zeta function $\sum_{n\geq 1} f_n z^n = z\zeta_f'(z)/\zeta_f(z)$. Reducing modulo a prime ℓ, the same again holds [1, Thm. 12.6.1] for $\sum_{n\geq 1} \overline{f_n} z^n \in \mathbf{F}_\ell[[z]]$, hence by Christol's Theorem, $(\overline{f_n})$ is ℓ-automatic. For a suitable choice of $\ell \neq p$, one then proceeds to show

that (a suitable subsequence[11] of) the sequence $(\overline{f_n})$ is also p-automatic, but not periodic, thus obtaining a (desired) contradiction with Cobham's Theorem.

The proof requires quite some computational effort, and even the construction of an explicit automaton [8, Lemma 7]. We think the method may be improved by considering a more general approach, still using the results of Christol and Cobham, but without automata. The starting point for this is a translation of the requirement of being an automatic sequence to something more mathematically accessible:

Definition 5.4 Let $(a_n)_{n\geq 0}$ be a sequence of elements of some set S, and let $k \in \mathbf{Z}_{>0}$. We define the *k-kernel* of (a_n) to be the set of subsequences

$$\ker_k(a_n) := \left\{ \left(a_{k^i \cdot n+j}\right)_{n\geq 0} \middle| \, 0 \leq i, \, 0 \leq j < k^i \right\}.$$

△

Proposition 5.5 *Let $k \geq 2$. The sequence $(a_n)_{n\geq 0}$ is k-automatic if and only if $\ker_k(a_n)$ is finite.*

Proof. [1, Thm. 6.6.2]. □

Interestingly enough, in the proof of Theorem 5.1 cited, both implications actually use Proposition 5.5 to translate the notion of being k-automatic to that of having a finite k-kernel; perhaps suggesting that it is more natural to consider the "k-kernel point of view" to begin with. Moreover, from the new perspective[12], [8, Lemma 7] can be proved rather quickly without any explicit construction of automata:

Lemma 5.6 (Bridy, [8, Lemma 7]) *Let d be an integer. If β_n is a function of the equivalence class modulo d of $v_p(n)$, then the sequence $(\beta_n)_{n\geq 1}$ is p-automatic.*

Proof. For any $i \in \mathbf{Z}_{\geq 0}$ and $0 \leq j < k^i$, we have

$$v_p(p^i n + j) \pmod d = \begin{cases} v_p(j) \pmod d & \text{if } j > 0 \\ i + v_p(n) \pmod d & \text{if } j = 0. \end{cases}$$

Since $v_p(j)$ and i can only take finitely many values modulo d, it follows that the sequence $(v_p(n) \pmod d)_n$ has finite p-kernel, hence the same holds for (β_n). □

The remainder of this section will be dedicated to finding a generalization and simplification of Bridy's argument in the "language of k-kernels". The result on dynamically affine maps on $\mathbf{P}^1$ will be the same as Bridy's (hence weaker than Theorem A), but the technique might also be applicable in a broader setting. For example, a corollary will be a rational/transcendental dichotomy for endomorphisms of abelian varieties (cf. [10, Thm. 4.3]).

Let us start with a lemma very similar to Lemma 5.6 (cf. [9, Prop. 7.6]).

Lemma 5.7 *Let $\ell \neq p$ be a prime. Then $(|n|_p \pmod \ell)_n$ has finite p-kernel.*

[11] Here Lemma 5.3(i) is used.

[12] Of course, this perspective is not actually new, as it is e.g. frequently used to prove many results about automatic sequences in [1]. However, we discuss it because it is different from Bridy's, and we think it might be more insightful in the context of dynamically affine maps.

Proof. This follows either from a direct computation similar to the one in the proof of Lemma 5.6, or by noting that $|n|_p \equiv p^{-v_p(n)} \pmod{\ell}$ depends only on the equivalence class of $v_p(n)$ modulo the multiplicative order d of p modulo ℓ, and applying Lemma 5.6. □

The following lemma serves to provide us with some extra control on the "degree sequence" (e.g. it applies to the degree sequence $d_n = \deg(\sigma^n - 1)$ for an endomorphism σ of an elliptic curve; see the computation in the proof of Lemma 3.16).

Lemma 5.8 *Suppose that $(d_n)_{n\geq 1}$ is a sequence with values in $\mathbf{Z}_{>0}$, given by*

$$d_n = \prod_{i=1}^{q} (\xi_i^n - 1)^{\nu_i}$$

for some $\xi_i \in \overline{\mathbf{Q}}$ and $\nu_i \in \mathbf{Z}_{>0}$. Denote by L the number field of degree $N \in \mathbf{Z}_{>0}$ obtained by adjoining the ξ_i to $\mathbf{Q}$ and denote by $\mathcal{O}_L$ its ring of integers. Let p be a prime number. Let $k \in \mathbf{Z}_{>0}$ such that there is an element in $(\mathbf{Z}/p^k\mathbf{Z})^\times$ of order larger than $N!$ (for instance any $k > \log_p(N!) + 2$ will work, because $(\mathbf{Z}/p^k\mathbf{Z})^\times$ always has an element of order p^{k-2}). Now let $\ell > p$ be a prime number satisfying the following conditions: (see Remark 5.9)

1. *ℓ does not divide any of the denominators of the algebraic numbers ξ_i;*
2. *ℓ does not ramify in $\mathcal{O}_L$;*
3. *ℓ does not divide any of the $d_1, \cdots, d_{p^{k-1}}$;*
4. *$p^k \nmid (\ell^{N!} - 1)$.*

Define $(b_n)_{n\geq 1}$ over $\{0, 1\}$ by

$$b_n = \begin{cases} 1 & \text{if } d_n \not\equiv 0 \pmod{\ell} \\ 0 & \text{if } d_n \equiv 0 \pmod{\ell} \end{cases}$$

Then b_n is periodic. In fact, there exists a finite set of integers S such that $b_n = 0$ precisely when n is divisible by an element of S. Moreover, $p^t \notin S$ for all $t \in \mathbf{Z}_{\geq 0}$.

Proof. Note that $d_n \equiv 0 \pmod{\ell}$ is equivalent to

$$\prod_{i=1}^{q} (\xi_i^n - 1)^{\nu_i} \in \ell\mathcal{O}_L \tag{29}$$

which is, by the Chinese Remainder Theorem, equivalent to

$$\prod_{i=1}^{q} (\xi_i^n - 1)^{\nu_i} \in \mathfrak{p} \tag{30}$$

for all $\mathfrak{p} \subseteq \mathcal{O}_L$ prime above ℓ. Now, for a given $\mathfrak{p}$, (30) holds precisely when n hits a multiple of the order $O(\mathfrak{p}, \xi_i)$ of some ξ_i modulo $\mathfrak{p}$ (using the convention that the order of zero is zero). That is, when n is divisible by an element of $S_\mathfrak{p} := \{O(\mathfrak{p}, \xi_i) \mid 1 \leq i \leq q\}$. Now since $\mathcal{O}_L/\mathfrak{p} \cong \mathbf{F}_{\ell^f}$, where the residue class degree f is bounded by N, we find that for every i we have $O(\mathfrak{p}, \xi_i) \mid (\ell^{N!} - 1)$. In particular we obtain $p^k \nmid O(\mathfrak{p}, \xi_i)$ by condition 4 on ℓ. Thus, $p^t \notin S_\mathfrak{p}$ for all $t \geq k$.

Now writing $\ell\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, we find that

$$S := \{\mathrm{lcm}(\alpha_1, \cdots, \alpha_m) \mid \alpha_1 \in S_{\mathfrak{p}_1}, \cdots, \alpha_m \in S_{\mathfrak{p}_m}\}$$

satisfies the condition that $b_n = 0$ precisely when n is divisible by an element of S. Note that for all $t \geq k$, $p^t \notin S$, because of the similar statement for every $S_{\mathfrak{p}_j}$ derived above. Also, for all $t < k$ we have $p^t \notin S$, because of condition 3 on ℓ. □

Remark 5.9 The conditions 1-4 in Lemma 5.8 hold for infinitely many ℓ: the first three can be met by taking ℓ large, while the last one can be met by using Dirichlet's result on primes in arithmetic progressions [38, Lemme III.3]; simply pick ℓ prime in the arithmetic progression $\alpha + mp^k$ where α represents an element of order larger than $N!$ in $(\mathbf{Z}/p^k\mathbf{Z})^\times$. ◊

Proposition 5.10 *Let p be a prime number, and let $(r_n)_{n\geq 1}$ and $(s_n)_{n\geq 1}$ be periodic sequences with entries in $\mathbf{Q}^\times$ and $\mathbf{Z}_{\geq 0}$ respectively. Also assume that s_n is not identically zero, and that the common period ω of r_n and s_n is not divisible by p. Suppose that the sequence $(f_n)_{n\geq 1}$ is given by one of the following two cases:*

(a) $f_n = d_n r_n |n|_p^{s_n}$, where $(d_n)_{n\geq 1}$ is as in Lemma 5.8;

(b) $f_n = d_n p^{-s_n|n|_p^{-1}}$, where $d_n = d_1^n$ for some $d_1 \in \mathbf{Z}_{>0}$.

Then there are infinitely many primes ℓ such that the reduction of $\sum_n f_n t^n$ modulo ℓ is transcendental over $\mathbf{F}_\ell(t)$.

Proof. Let $\nu \in \mathbf{Z}_{\geq 1}$ such that $s_\nu \neq 0$. Set $r := r_\nu$ and $s := s_\nu$.

Suppose first that f_n is as in (a). Let $\ell > p^s$ be a prime satisfying the conditions of Lemma 5.8, that additionally does not divide any of the numerators/denominators of r or s. Assume to the contrary (Theorem 5.1) that the reduction $(f_n \pmod \ell)_{n\geq 1}$ has finite ℓ-kernel. The reduction $(d_n \pmod \ell)_{n\geq 1}$ has finite ℓ-kernel (because $(d_n)_{n\geq 1}$ is a linear recurrence sequence), hence so does the sequence $(d'_n \pmod \ell)_{n\geq 1}$ given by

$$d'_n := \begin{cases} d_n^{-1} & \text{if } d_n \not\equiv 0 \pmod \ell\,; \\ 0 & \text{if } d_n \equiv 0 \pmod \ell\,. \end{cases}$$

Now, by Lemma 5.3(ii), the Hadamard product $(a_n)_{n\geq 1} := (f_n d'_n \pmod \ell)_{n\geq 1}$ has finite ℓ-kernel. Using Lemma 5.3(i), the subsequence $(a'_n)_{n\geq 1} := (r^{-1}a_{\omega n+\nu})_{n\geq 1}$ of $(r^{-1}a_n)_{n\geq 1}$ along the arithmetic progression $\omega n + \nu$ has finite ℓ-kernel, and is given by

$$a'_n = \begin{cases} |\omega n + \nu|_p^s & \text{if } d_n \not\equiv 0 \pmod \ell\,; \\ 0 & \text{if } d_n \equiv 0 \pmod \ell\,. \end{cases}$$

Now let $(b_n)_{n\geq 1}$ as in Lemma 5.8. Then $(a'_n)_{n\geq 1}$ is the Hadamard product of a subsequence (indexed by an arithmetic progression) of $(|n|_p^s)_{n\geq 1}$ with $(b_n)_{n\geq 1}$. Both of these sequences have finite p-kernel by Lemmas 5.7 and 5.8 respectively,[13] so $(a'_n)_{n\geq 1}$ has both finite p-kernel and finite ℓ-kernel, and is therefore, by Theorem 5.2, eventually (let us say for $n > M$) periodic of some period $k \in \mathbf{Z}_{>0}$. Now let $m \in \mathbf{Z}_{>0}$ such that $v_p(\omega m + \nu) > v_p(\omega p k)$. Such m exists because $p \nmid \omega$. Define $t := \max(v_p(\omega m + \nu), M) + 1$. Note that

[13] For the result on (b_n), we use that eventually periodic sequences have finite k-kernel for all $k \in \mathbf{Z}_{>0}$.

by Lemma 5.8, there exists a $c \in \mathbf{Z}_{>0}$ such that $b_{m+cp^t} = 1$. Now $0 \neq a'_{m+cp^t} = a'_{m+cp^t+k} = a'_{m+cp^t+pk}$. That is,

$$|k|_p^s \equiv |\omega k|_p^s \equiv |\omega(m + cp^t + k) + \nu|_p^s \equiv |\omega(m + cp^t + pk) + \nu|_p^s \equiv |pk|_p^s \pmod{\ell},$$

a contradiction since $p^s \not\equiv 1 \pmod{\ell}$. This completes the proof of part (a).

Now suppose f_n is as in (b). Let ℓ be a prime such that $\ell > \max(p^{sp}, d_1)$, $\ell \not\equiv 1 \pmod{p}$ (this last requirement can again be met, for instance, by Dirichlet's theorem on primes in arithmetic progressions), and assume to the contrary that the reduction $(f_n \pmod{\ell})_n$ has finite ℓ-kernel. Then, since d_1^n is invertible modulo ℓ for every n, the same holds for $\left(p^{-s|\omega n+\nu|_p^{-1}} \pmod{\ell}\right)_n$. Let e be the order of p^s modulo ℓ. Note that by the assumptions on ℓ, we have $e > p$ and $p \nmid e$. Since $p^{-sx} \equiv p^{-sy} \pmod{\ell} \iff x \equiv y \pmod{e}$, we obtain a well defined map $(\mathbf{Z}/\ell\mathbf{Z})^\times \to \mathbf{Z}/e\mathbf{Z}$ sending $p^{-s|\omega n+\nu|_p^{-1}} \pmod{\ell}$ to $|\omega n + \nu|_p^{-1} \pmod{e}$. By Lemma 5.7 combined with Lemma 5.3, the sequence $\left(|\omega n + \nu|_p^{-1} \pmod{e}\right)_{n\geq 1}$ has both a finite p-kernel and a finite ℓ-kernel, hence is ultimately periodic. Since $e > p$, we have $p^{-1} \not\equiv 1 \pmod{e}$, hence by a special case ($s = 1$ and $d_n \not\equiv 0 \pmod{\ell}$ for all n) of the final part of the argument for case (a) above we obtain a desired contradiction. □

Corollary 5.11 *Let $f : \mathbf{P}^1 \to \mathbf{P}^1$ be a dynamically affine map (in the sense of Definition 3.3) on the projective line over an algebraically closed field K of positive characteristic $p > 0$. If σ is not coseparable, then ζ_f is transcendental over $\mathbf{Q}(z)$.*

Proof. Assume to the contrary that ζ_f is algebraic. Then the same holds for $\mathcal{Z}_f(z) = \sum_{n\geq 1} f_n z^n$. Using Lemma 3.6, we find that (v is as in Lemma 3.15)

$$\sum_{n\geq 1}\sum_{\gamma\in\Gamma} \#\ker(\sigma^n - \gamma) z^n = \sum_{n\geq 1}\sum_{\gamma\in\Gamma} \deg(\sigma^n - \gamma) p^{-v(\sigma^n-\gamma)} z^n \tag{31}$$

is algebraic. Using Proposition 2.16(vi), let $s \in \mathbf{Z}_{>0}$ and $\gamma_0 \in \Gamma$ such that $v(\sigma^s - \gamma_0)$ is sufficiently large.[14] Then σ^s and γ_0 commute by Lemma 3.9. Denoting $\tau := \sigma^s\gamma_0^{-1}$, we obtain

$$\begin{aligned}
&\sum_{n\geq 1}\sum_{\gamma\in\Gamma} \deg(\sigma^{sn} - \gamma) p^{-v(\sigma^{sn}-\gamma)} z^{sn} \\
= &\sum_{n\geq 1}\sum_{\gamma\in\Gamma} \deg(\sigma^{sn} - \gamma\gamma_0^n) p^{-v(\sigma^{sn}-\gamma\gamma_0^n)} z^{sn} \\
= &\sum_{n\geq 1}\sum_{\gamma\in\Gamma} \deg(\tau^{n} - \gamma) p^{-v(\tau^{n}-\gamma)} z^{sn} \\
= &\sum_{n\geq 1} \deg(\tau^n - 1) p^{-v(\tau^n-1)} z^{sn} + \sum_{n\geq 1}\sum_{\gamma\neq 1} \deg(\tau^n - \gamma) p^{-v(\gamma-1)} z^{sn}.
\end{aligned}$$

Using Proposition 2.16 again, we find

$$v\left(\tau^n - 1\right) = \begin{cases} v(\tau - 1) + v(n) & \text{if } \operatorname{char}(\operatorname{End}(G)) = 0; \\ v(\tau - 1)p^{v_p(n)} & \text{if } \operatorname{char}(\operatorname{End}(G)) = p. \end{cases}$$

Hence

$$g_n := \deg(\tau^n - 1) p^{-v(\tau^n-1)} = \begin{cases} \deg(\tau^n - 1) p^{-v(\tau-1)} |n|_p & \text{if } \operatorname{char}(\operatorname{End}(G)) = 0; \\ \deg(\tau^n - 1) p^{-v(\tau-1)|n|_p^{-1}} & \text{if } \operatorname{char}(\operatorname{End}(G)) = p. \end{cases}$$

[14] That is, $v(\sigma^s - \gamma_0) \geq \max\left(\max\{v(\gamma - \gamma') \mid \gamma, \gamma' \in \Gamma, \gamma \neq \gamma'\} + 1, (\rho(\operatorname{End}(G), v) + 1)/(p - 1)\right)$.

The sequence $\left(\sum_{\gamma\neq 1}\deg(\tau^n-\gamma)p^{-v(\gamma-1)}\right)_{n\geq 1}$ is linear recurrent by (the calculations in) Lemma 3.16, so since the power series (31) is algebraic, reducing modulo a to be determined prime $\ell > p$, we find (using Lemma 5.3(i) to "pass to" the subsequence) that the sequence $(g_n \pmod{\ell})_n$ has finite ℓ-kernel. From the case-by-case computation of the degree sequence $\deg(\tau^n - 1)$ that we saw in the proof of Lemma 3.16, we find that the subsequence $d_n := \deg(\tau^{2n} - 1)$ has the desired form[15] for application of Proposition 5.10. Indeed, we can write

$$g_{2n} = \begin{cases} d_n r|n|_p^s & \text{if } \operatorname{char}(\operatorname{End}(G)) = 0; \\ d_n p^{-s|n|_p^{-1}} & \text{if } \operatorname{char}(\operatorname{End}(G)) = p, \end{cases}$$

where $s \neq 0$. If we now choose ℓ prime anywhere in the infinite sequence given by Proposition 5.10, then $\sum_{n\geq 1} g_{2n}t^n \pmod{\ell}$ becomes transcendental over $\mathbf{F}_\ell$, a contradiction. □

Corollary 5.12 *Let $\sigma : A \to A$ be a confined endomorphism of an abelian variety A over an algebraically closed field K of characteristic $p > 0$, and suppose that σ is not coseparable. Then ζ_σ is transcendental.*

Proof. In the proof of [10, Prop. 2.3(i)], it is shown that $\deg(\sigma^n - 1)$ has the form d_n of Lemma 5.8. Moreover, [loc. cit., Prop. 2.7] shows that $\deg_i(\sigma^n - 1) = r_n|n|_p^{s_n}$ for sequences (r_n) and (s_n) as in Proposition 5.10. □

[15] We need to consider this particular subsequence in order to eliminate the factor $\operatorname{sgn}(\tau)$ in the formula $\deg(\tau^n - 1) = |\tau|^n - \operatorname{sgn}(\tau)^n$ for $\mathbf{G}_m$.

6 Future Questions

As mentioned in the introduction, little is known about the dynamical zeta function for general maps on the projective line in positive characteristic. An unanswered question remains:

Question A *Let k be an algebraically closed field of characteristic $p \geq 5$. Let $f : \mathbf{P}^1/k \to \mathbf{P}^1/k$ given by $f(x) = x^2 + 1$. Is ζ_f rational? What about ζ_f^*?*

We suspect both to be far from rational, but we have no idea how to approach this problem. Perhaps an easier question to answer would be:

Question B *Is there any surjective confined non-dynamically affine map f on the projective line over an algebraically closed field of positive characteristic for which we can determine whether ζ_f is rational or not?*

In Section 3.2 we discussed certain hypotheses **(H1)**-**(H4)** that we needed in the proof (Section 3.4) of our main result. For a general dynamically affine map $f : V \to V$, questions that arise are:

Question C *(i) Are there precise conditions for* **(H1)** *to hold?*

We already saw that **(H1)** always holds in the case that $V = \mathbf{P}^1$ (and the proof also works for any one-dimensional V). Similarly, if the algebraic group G is complete, then the inclusion ι has to be surjective, making the statement trivial. For general V, however, it seems unlikely for **(H1)** to always hold; especially since the complement of G/Γ in V is not "related" to an algebraic group. At the same time this means that answering this question may be as difficult as determining the dynamical zeta function for arbitrary morphisms of varieties.

(ii) Can we weaken **(H2)***?*

It follows from the definition that the "direct product" of dynamically affine maps is dynamically affine; in particular the self-product $f \times f : V \times V \to V \times V$ is dynamically affine (with underlying group $G \times G$), and since $(f \times f)_n = f_n^2$, rationality of ζ_f implies rationality of $\zeta_{f \times f}$. Similarly, the proof of the natural boundary result in Section 3.4 also works when we replace the sequence f_n by f_n^2. However, **(H2)** does not hold for products of algebraic groups; the endomorphism ring of $G \times G$ contains zero divisors (see Proposition 2.16). This suggests that we might need to consider a weaker version of **(H2)**; perhaps for a "discrete valuation" $v : \mathrm{End}(G) \to (\mathbf{Z}_{\geq 0} \cup \{\infty\})^r$ instead.

(iii) Does **(H3)** *hold in general?*

The third hypothesis can be seen as the analogue of rationality of the "degree zeta function" (cf. [10, Prop. 2.3]) in the presence of a group action. The method of the proof of the proposition cited can also be applied in the setting of dynamically affine maps arising from abelian varieties, but only for the case that the endomorphism ring is commutative. In the case that the endomorphism ring is non-commutative, we do not have a counterexample to **(H3)**; in fact, we suspect that it might always be true.

(iv) Do we really need **(H4)***?*

The requirement of **(H4)** seems slightly unnatural: it is a technical assumption that is purely

employed to avoid cancellation of singularities at the "candidate" natural boundary. However, in the (probably unlikely) case where the singularities obtained *do* cancel out, then by the very definition of a natural boundary we might somehow be able to analytically extend the dynamical zeta function beyond the disk initially restricted by the dominant root. Then, if the "runner-up" dominant root is unique, we might still be able to conclude the desired result of a natural boundary.

In Section 4, we discussed dynamics on algebraic groups. The main question that remained was:

Question D *Let $r \in \mathbf{Z}_{\geq 0}$, and let $\sigma : \mathbf{G}_a^r \to \mathbf{G}_a^r$ be a confined endomorphism. Can we find an explicit form for the fixed point sequence (σ_n)? More concretely, does it satisfy* (25)*?*

Lemma 4.6 tells us that $\sigma_n = d_n a_n$, where $d_n = \deg(\sigma^n - 1)$, and a_n has the desired form of Conjecture 4.1. Given the examples seen so far, we expect the zeta function corresponding to d_n to be rational; although just root-rationality would be enough to complete the proof of Conjecture 4.1.

References

[1] Jean-Paul Allouche and Jeffrey Shallit, *Automatic sequences*, Cambridge University Press, Cambridge, 2003.

[2] Mark A. Armstrong, *Groups and symmetry*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1988.

[3] Emil Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen. II*, Math. Z. **19** (1924), no. 1, 207–246.

[4] Michael Artin and Barry C. Mazur, *On periodic points*, Ann. of Math. (2) **81** (1965), 82–99.

[5] Jason Bell, Richard Miles, and Thomas Ward, *Towards a Pólya-Carlson dichotomy for algebraic dynamics*, Indag. Math. (N.S.) **25** (2014), no. 4, 652–668.

[6] Jason P. Bell, Michael Coons, and Eric Rowland, *The rational-transcendental dichotomy of Mahler functions*, J. Integer Seq. **16** (2013), no. 2, Article 13.2.10, 11.

[7] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[8] Andrew Bridy, *Transcendence of the Artin-Mazur zeta function for polynomial maps of* $\mathbb{A}^1(\overline{\mathbb{F}}_p)$, Acta Arith. **156** (2012), no. 3, 293–300.

[9] ———, *The Artin-Mazur zeta function of a dynamically affine rational map in positive characteristic*, J. Théor. Nombres Bordeaux **28** (2016), no. 2, 301–324.

[10] Jakub Byszewski and Gunther Cornelissen, *Dynamics on abelian varieties in positive characteristic*, preprint, arXiv:1802.07662 (2018), with an appendix by Robert Royals and Thomas Ward, to appear in Algebra & Number Theory.

[11] Claude Chevalley, *Une démonstration d'un théorème sur les groupes algébriques*, J. Math. Pures Appl. (9) **39** (1960), 307–317.

[12] Gilles Christol, *Ensembles presque periodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979), no. 1, 141–145.

[13] Alan Cobham, *On the base-dependence of sets of numbers recognizable by finite automata*, Math. Systems Theory **3** (1969), 186–192.

[14] Paul M. Cohn, *Skew fields*, Encyclopedia of Mathematics and its Applications, vol. 57, Cambridge University Press, Cambridge, 1995.

[15] Brian Conrad, *A modern proof of Chevalley's theorem on algebraic groups*, J. Ramanujan Math. Soc. **17** (2002), no. 1, 1–18.

[16] Michel Demazure and Pierre Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[17] Jean Dieudonné, *Les déterminants sur un corps non commutatif*, Bull. Soc. Math. France **71** (1943), 27–45.

[18] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[19] Paul C. Eklof, *Lefschetz's principle and local functors*, Proc. Amer. Math. Soc. **37** (1973), 333–339.

[20] Philippe Flajolet, Stefan Gerhold, and Bruno Salvy, *On the non-holonomic character of logarithms, powers, and the nth prime function*, Electron. J. Combin. **11** (2004/06), no. 2, Article 2, 16.

[21] Alexander Grothendieck, *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki, Vol. 9, Exp. No. 279, Soc. Math. France, Paris, 1995 (1965), pp. 41–55.

[22] Jacques Hadamard, *Théorème sur les séries entières*, Acta Math. **22** (1899), no. 1, 55–63.

[23] William A. Harris, Jr. and Yasutaka Sibuya, *The reciprocals of solutions of linear ordinary differential equations*, Adv. in Math. **58** (1985), no. 2, 119–132.

[24] Aimo Hinkkanen, *Zeta functions of rational functions are rational*, Ann. Acad. Sci. Fenn. Ser. A I Math. **19** (1994), no. 1, 3–10.

[25] Nathan Jacobson, *The Theory of Rings*, American Mathematical Society Mathematical Surveys, vol. II, American Mathematical Society, New York, 1943.

[26] Solomon Lefschetz, *Algebraic geometry*, Princeton University Press, Princeton, N. J., 1953.

[27] Saunders Mac Lane, *Homology*, Classics in Mathematics, Springer-Verlag, Berlin, 1995, Reprint of the 1975 edition.

[28] Anthony Manning, *Axiom A diffeomorphisms have rational zeta functions*, Bull. London Math. Soc. **3** (1971), 215–220.

[29] B. Mazur, *Eigenvalues of Frobenius acting on algebraic varieties over finite fields*, (1975), 231–261.

[30] James S. Milne, *Abelian varieties (v2.00)*, 2008, Available at `www.jmilne.org/math`, 172 pp.

[31] ———, *Algebraic geometry (v5.22)*, 2012, Available at `www.jmilne.org/math`, 260 pp.

[32] ———, *Lectures on etale cohomology (v2.21)*, 2013, Available at `www.jmilne.org/math`, 202 pp.

[33] ———, *Algebraic groups*, Cambridge Studies in Advanced Mathematics, vol. 170, Cambridge University Press, Cambridge, 2017, The theory of group schemes of finite type over a field.

[34] John Nash, *Real algebraic manifolds*, Ann. of Math. (2) **56** (1952), 405–421.

[35] Joseph Rabinoff, *The Theory of Witt Vectors*, arXiv:1409.7445, September 2014.

[36] Jonathan Rosenberg, *Algebraic K-theory and its applications*, Graduate Texts in Mathematics, vol. 147, Springer-Verlag, New York, 1994.

[37] Jean-Pierre Serre, *Groupes algébriques et corps de classes*, Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[38] ———, *Cours d'arithmétique*, Collection SUP: "Le Mathématicien", vol. 2, Presses Universitaires de France, Paris, 1970.

[39] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts Math., vol. 241, Springer, New York, 2007.

[40] ———, *The arithmetic of elliptic curves*, Graduate Texts Math., vol. 106, Springer, New York, 2009.

[41] Stephen Smale, *Differentiable dynamical systems*, Bull. Amer. Math. Soc. **73** (1967), 747–817.

[42] Tonny A. Springer, *Linear algebraic groups*, second ed., Modern Birkhäuser Classics, Birkhäuser Boston, Inc., Boston, MA, 2009.

[43] Richard P. Stanley, *Enumerative combinatorics. Vol. 1*, second ed., Cambridge Studies in Adv. Math., vol. 49, Cambridge University Press, Cambridge, 2012.

[44] ———, *Enumerative combinatorics. Vol. 2*, Cambridge Studies in Advanced Mathematics, vol. 62, Cambridge University Press, Cambridge, 1999.

[45] Robert Steinberg, *Endomorphisms of linear algebraic groups*, Memoirs of the American Mathematical Society, No. 80, American Mathematical Society, Providence, R.I., 1968.

[46] Lucien Szpiro and Thomas J. Tucker, *Algebraic dynamics*, Colloquium De Giorgi 2006, Colloquia, vol. 1, Ed. Norm., Pisa, 2006, pp. 51–57.

[47] Lenny Taelman, *Dieudonné determinants for skew polynomial rings*, J. Algebra Appl. **5** (2006), no. 1, 89–93.

[48] André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

[49] Ernst Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p*, J. Reine Angew. Math. **176** (1937), 126–140.