Master's Thesis

Iteration of Rational Functions in Positive Characteristic

Author
Lois van der Meijden

Supervisor
Prof. Dr. Gunther Cornelissen

Second reader
Prof. Dr. Frits Beukers

Utrecht University

Department of Mathematics

June 2017

ABSTRACT

For a dynamical system consisting of a set S and a map $f : S \to S$, the *dynamical zeta function* $\zeta_{f,S}(T)$ encodes all information on the (finite) number of fixed points of all nth iterates of f on S. We are particularly interested in the case where $S = X(\overline{K})$, with X an algebraic variety over K, and f a morphism of degree at least two.

If $X = \mathbb{P}^1_K$, where K is a field of characteristic zero, and f is a rational map of degree at least 2, then the dynamical zeta function is a rational function over $\mathbb{Q}(T)$. However, if K has positive characteristic, then the dynamical zeta function of *dynamically affine maps*, which are morphisms of a strongly group-theoretical nature, becomes transcendental over $\mathbb{Q}(T)$.

Under some assumptions, we prove new results for separable endomorphisms on an elliptic curve E over a field K of characteristic $p > 0$, and for multiplication-by-m maps on abelian varieties, where $p \nmid m$.

Such transcendence results indicate that for characteristic $p > 0$ the number of fixed points does not have an easy pattern. The *tame dynamical zeta function* is introduced as an alternative for the original dynamical zeta function; it only counts nth iterates for $p \nmid n$. We prove a new theorem which tells us that for dynamically affine maps, the tame dynamical zeta function is algebraic.

ACKNOWLEDGEMENTS

First and foremost I would like to thank my supervisor Prof. Dr. Gunther Cornelissen. He provided me with an immensely interesting topic and several exciting research questions. Our biweekly meetings were always helpful: he would answer all my question patiently and listened to my mathematical endeavors with the utmost attention. His enthusiasm and knowledge always inspired me to make the most out of this project.

I would also like to thank Prof. Dr. Frits Beukers for taking the time to be my second reader.

Furthermore, I would like to thank Dr. Andrew Bridy and Prof. Dr. Ben Moonen for their quick and useful responses to my questions, Dr. Jakub Byszewski for his input on the subject during his visit, and Prof. Dr. Frans Oort for taking the time to share his knowledge on schemes, abelian varieties and other topics with me.

My fellow students who participated in the master's thesis seminar with me deserve recognition as well. Our weekly meetings were always fruitful and enjoyable.

Of course, I am very thankful to Jan-Willem, Casper, Tom and Twan for reading my thesis and the comments they gave me.

Lastly, I would like to express my gratitude to all my friends and family for their support throughout this project.

CONTENTS

1

INTRODUCTION

An *arithmetic dynamical system* is a pair (f, X) where X is an algebraic variety over a field K and $f : X \to X$ is a morphism.

When working with dynamical systems we are often interested in all orbits of f. When an orbit is finite, all its elements are periodic points of f, i.e. fixed points of its iterates. We will investigate the patterns in the number of fixed points of the nth iterate $f^{\circ n}$ on $X(\overline{K})$ via the *dynamical zeta function*:

$$\zeta_{f,X}(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#\mathrm{Fix}(f^{\circ n})}{n} T^n\right).$$

Here we assume the number of fixed points is finite. A more precise introduction of arithmetic dynamical systems is presented in Chapter 2.

This zeta function was first introduced by Artin and Mazur in [AM65] for a diffeomorphism on a topological space in order to study the asymptotic behaviour of its fixed points. Later Hinkkanen proved in [Hin94] that if $X = \mathbb{P}^1_{\mathbb{C}}$ and f is a rational map of degree at least 2, then the dynamical zeta function is a rational function in T. This was later generalized to arbitrary fields of characteristic zero by Lee in [Lee15]. A detailed proof is included in Chapter 4.

The case where K is a field of positive characteristic had remained more mysterious, until Bridy proved in [Bri12] and later in [Bri16] that the dynamical zeta function is transcendental for some sufficiently nice separable morphisms. These morphisms are called *dynamically affine maps* and include power maps, Chebyshev polynomials, Lattès maps, and when the characteristic is positive also (sub)additive polynomials.

His proofs rely on the theory of *automata*: finite-state machines that take strings of input and give an output following a deterministic protocol. Therefore, Chapter 3 is included to introduce all necessary theory on automata.

We were able to rewrite some of his results as simple corollaries of the following theorem:

Theorem (5.1.1)**.** *Let p be a prime and $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$ and $b, c, d, e, \varepsilon \in \mathbb{Z}_{\geq 0}$ with $\varepsilon \in \{0, 1\}$ and $A \in \mathbb{Q}^\times$. Define the sequence $(a_n)_{n\geq 1}$ by*

$$a_n := A\left((m^n - 1)^b |m^n - 1|_p^c + \varepsilon (m^n + 1)^d |m^n + 1|_p^e\right).$$

If $p \nmid m$, then $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ *is transcendental over* $\mathbb{Q}(T)$*. However, if* $p \mid m$*, then* $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ *is algebraic over* $\mathbb{Q}(T)$*. In particular, when* $p \mid m$ *and* $A \in \mathbb{Z}$*, then* $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ *is rational over* $\mathbb{Q}(T)$*.*

By some basic algebraic computations, we can see that this theorem applies to power maps, Lattès maps and Chebyshev polynomials. Looking at the proof for Lattès maps, it became clear that a similar result should hold for endomorphisms of elliptic curves as well. We proved:

Theorem (5.2.14)**.** *Let E be an elliptic curve over a field K of characteristic $p > 3$, and let $f : E \to E$ be an isogeny of degree at least 2. If f is separable, then $\zeta_{f,E}(T)$ is transcendental over $\mathbb{Q}$.*

The proof consist of the same steps as Theorem 5.1.1, yet generalized to suit all endomorphisms of elliptic curves. As the proof relies on the structure of kernels of the endomorphisms, the idea arose to generalize this to abelian varieties. For multiplication-by-m maps it was not hard to see it is in fact a corollary of Theorem 5.1.1:

Theorem (5.2.7)**.** *Let A be an abelian variety over a field K of characteristic $p > 0$, and let $[m] : A \to A$ be the multiplication-by-m map, with $|m| > 1$. If $p \nmid m$, then $\zeta_{[m],A}(T)$ is transcendental over $\mathbb{Q}(T)$. However, if $p \mid m$, then $\zeta_{[m],A}(T)$ is rational over $\mathbb{Q}(T)$.*

Although the majority of steps in the proof of Theorem 5.2.14 apply to general isogenies of abelian varieties, there was one step in the form of Lemma 5.2.13, regarding the inseparable degree of an isogeny, which proved to be more complicated for abelian varieties. This problem is reviewed in Chapter 7.

One studies the dynamical zeta function as a way to understand the patterns in the number of fixed points. The fact that we obtain transcendence results tells us that simple patterns are not easy to detect. Therefore, G. Cornelissen and J. Byszewski came up with an alternative to the dynamical zeta function, namely the *tame dynamical zeta function*, which omits all 'problematic' terms:

$$\zeta^*_{f,X}(T) := \exp \sum_{\substack{n=1, \\ p\nmid n}}^{\infty} \frac{\#\mathrm{Fix}(f^{\circ n})}{n} T^n.$$

One naively expects that its behaviour is similar to the (full) dynamical zeta function in characteristic zero. By computing the tame dynamical zeta function for dynamically affine maps we observe:

Theorem (6.1.2)**.** *Let K be a field of characteristic $p > 0$, and let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a morphism of degree at least 2. If f is a power map, Chebyshev polynomial, Lattès map induced by a multiplication-by-m map or a (sub)additive polynomial, then the tame dynamical zeta function $\zeta^*_{f,\mathbb{P}^1_K}(T)$ is algebraic over $\mathbb{Q}(T)$.*

The algebraicity of the tame dynamical zeta function of such f suggests that its structure might be similar to the dynamical zeta function of a corresponding map $\tilde{f}$ over characteristic zero. It turns out that there is a natural way of lifting power maps, Chebyshev polynomials and Lattès maps to maps over characteristic zero. This allows us to compare the tame dynamical zeta function of a dynamically affine map f to the dynamical zeta function of its lift $\widetilde{f}$. For power maps we found promising results, e.g. when $p \nmid m$ we have Equation 6.2.1.6:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{\zeta_{x^m,\mathbb{G}_{m,K,0}}(T)}{\zeta_{x^{mp},\mathbb{G}_{m,K,0}}(T^p)^{1/p}} \cdot \left(\frac{\zeta_{x^{m^s},\mathbb{G}_{m,K,0}}(T^s)}{\zeta_{x^{m^{ps}},\mathbb{G}_{m,K,0}}(T^{ps})^{1/p}}\right)^{(A-1)/s},$$

where $\mathbb{G}_{m,\mathbb{F}_p}$ is the multiplicative group over $\overline{\mathbb{F}_p}$, and $\mathbb{G}_{m,K,0}$ the multiplicative group of $\overline{K}$, a field of characteristic zero. Here s and A are constants depending on m. When the tame dynamical zeta function can be written in this way we call it *expressible over its lift*.

However, it turns out that such a relation does not exist for (most) separable Chebyshev polynomials and all separable Lattès maps induced by a multiplication-by-m map:

Theorem (6.3.3.(v,vi,vii))**.** *Let K be a field of characteristic $p > 0$, and let $f : X \to X$ be a dynamically affine map. Then $\zeta^*_{f,X}(T)$ is not expressible over its lift if f is one of the following:*

- *Chebyshev polynomial T_d on $\mathbb{G}_{a,p}(\overline{K})$, with $p \nmid d$ and $p \neq 2$;*
- *Chebyshev polynomial T_d on $\mathbb{G}_{a,p}(\overline{K})$, with $p = 2$, and $d \equiv 1 \mod 4$;*
- *Lattès map L_m on $\mathbb{P}^1_{K,p}(\overline{K})$, with $p \nmid m$.*

There are several aspects of dynamical systems over positive characteristic which have potential for further study. An overview of interesting problems is presented in Chapter 7.

2

ARITHMETIC DYNAMICAL SYSTEMS

In this chapter we will discuss the basic notions in the field of arithmetic dynamical systems and more algebraic notions of how or where we will apply these. The first section is a brief introduction which only discusses the necessary definitions. The second section will focus for algebraic structures for which we will consider these dynamical systems.

2.1 DYNAMICAL SYSTEMS

A *(discrete) dynamical system* consists of a set S and a self-map $f : S \to S$. When considering such a system, we will be interested in the behaviour of f when it is iterated multiple times. Hereinafter, let S and f be such a dynamical system.

Definition 2.1.1. Let S be a set and $f : S \to S$ a map. We define the **n-fold composition** of f as $f^{\circ n} := \underbrace{f \circ \ldots \circ f}_{n \text{ times}}$, such that $f^{\circ n} : S \to S$. Any $f^{\circ n}$ is called an **iterate** of f.

Definition 2.1.2. Let S be a set and $f : S \to S$ a map. We call $x \in S$ a **fixed point** of f if $f(x) = x$. With $\mathrm{Fix}(f)$ we denote the set of all fixed points of f in S.

Clearly, not every point is fixed for f itself, and hence it is interesting to consider points being fixed for the n-fold composition.

Definition 2.1.3. Let S be a set and $f : S \to S$ a map. We call $x \in S$ **periodic** if there exists $n \in \mathbb{Z}_{\geq 1}$ such that $f^{\circ n}(x) = x$. Moreover, the smallest such integer n_0 is called the **exact** or **minimal period** of x.

We are interested in determining how many fixed points we have for each iteration of f. In other words, we are interested in the sequence $|\mathrm{Fix}(f^{\circ n})|$. This information can be given in the form of a generating function defined as a formal power series, similar to the Hasse-Weil zeta function of an algebraic variety over a finite field.

Definition 2.1.4. Let S be a set and $f : S \to S$ a map. Define the **dynamical zeta function** of f over S as

$$\zeta_{f,S}(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\mathcal{N}_n}{n} T^n\right),$$

where

$$\mathcal{N}_n := \begin{cases} |\mathrm{Fix}(f^{\circ n})| & \text{if} \quad |\mathrm{Fix}(f^{\circ n})| \quad \text{is finite;} \\ 0 & \text{otherwise.} \end{cases}$$

We need $\mathcal{N}_n$ to be finite to ensure that the zeta function is well-defined. This formal power series was first introduced by Artin and Mazur in [AM65], and hence it is also referred to as the *Artin-Mazur zeta function*.

Notation. When the set S is understood we may omit it: $\zeta_f(T)$. Furthermore, we will be interested in $S = X(\overline{K})$, where X is an algebraic variety over a field K. We may just write $\zeta_{f,X}(T)$ instead of $\zeta_{f,X(\overline{K})}(T)$ as we will always count fixed points over the algebraic closure. Similarly, we can write $f : X \to X$ and then we count its fixed points over the algebraic closure: $\text{Fix}(f) := \{x \in X(\overline{K}) \mid f(x) = x\}$.

Moreover, throughout this thesis we will switch between maps over different fields, i.e. fields of different characteristic. To avoid confusion, we denote the zeta function of a map $f : X(\overline{K}) \to X(\overline{K})$ by $\zeta_{f,X_{K,0}}(T)$ when K has characteristic or $\zeta_{f,X_{K,p}}(T)$ when K has characteristic $p > 0$. When the characteristic is obvious from the field, e.g. $\mathbb{F}_p$, or if we have not specified the characteristic of K we may just write ζ_{f,X_K}.

2.2 DYNAMICALLY AFFINE MAPS

We will be particularly interested in the case where S is an algebraic variety, denoted X, over a field K and f is a morphism. Following Section 6.8 in [Sil07], we introduce a few other notions in order to discuss a specific family of morphisms on $\mathbb{P}^1_K$, called *dynamically affine maps*.

Definition 2.2.1. An **algebraic group** is a group that is also an algebraic variety, such that the multiplication and inversion operations are given by regular maps on the variety.

Definition 2.2.2. A morphism $\phi : X \to Y$ of algebraic varieties is said to be **unramified** at a point $P \in X$ if ϕ induces an isomorphism between the completion of the local rings at P and $\phi(P)$. We call ϕ **unramified** if ϕ is unramified at all points $P \in X$.

Definition 2.2.3. An unramified morphism $\phi : X \to Y$ of algebraic varieties is called a **finite morphism** if for any point $P \in \phi(X)$, the inverse image $\phi^{-1}(P)$ consists of d points, counted with multiplicity, for a certain fixed integer d, called the **degree** of ϕ.

Definition 2.2.4. Let G be a commutative algebraic group. An **affine morphism** of G is the composition of a finite endomorphism of degree at least 2 and a translation.

We can finally give the definition of a dynamically affine map.

Definition 2.2.5. A self-morphism of an algebraic variety $\phi : V \to V$ is **dynamically affine** if it is a finite quotient of an affine morphism, i.e. if there exist a connected commutative algebraic group G, an affine morphism $\psi : G \to G$, a finite subgroup $\Gamma \subset \mathrm{Aut}(G)$, and a morphism $\chi : G/\Gamma \to V$ that identifies G/Γ with a Zariski dense open subset of V, such that the following diagram is commutative:

$$\begin{CD} G @>{\psi}>> G \\ @VVV @VVV \\ G/\Gamma @>>> G/\Gamma \\ @V{\chi}VV @V{\chi}VV \\ V @>{\phi}>> V \end{CD}$$

Example 2.2.6. A power map $\phi(x) = x^m$ is an example of a dynamically affine morphism. Let $G = \mathbb{G}_m(\overline{K})$ be the multiplicative group of a field K, $\Gamma = \langle 1 \rangle$, $V = \mathbb{P}^1_K(\overline{K})$ and $\chi : \mathbb{G}_m(\overline{K}) \to \mathbb{P}^1_K(\overline{K})$, defined by identifying $\mathbb{G}_m(\overline{K})$ with $\mathbb{P}^1_K(\overline{K}) \setminus \{0, \infty\} \subset \mathbb{P}^1_K(\overline{K})$. We get the diagram:

$$\begin{CD} \mathbb{G}_m(\overline{K}) @>{x \to x^m}>> \mathbb{G}_m(\overline{K}) \\ @V{\mathrm{id}}VV @V{\mathrm{id}}VV \\ \mathbb{G}_m(\overline{K})/\langle 1 \rangle @>>> \mathbb{G}_m(\overline{K})/\langle 1 \rangle \\ @V{\chi}VV @V{\chi}VV \\ \mathbb{P}^1_K(\overline{K}) @>{x \to x^m}>> \mathbb{P}^1_K(\overline{K}) \end{CD}$$

Clearly, almost all maps are restrictions or identity maps, hence the diagram commutes.

Other dynamically affine maps we will study on $\mathbb{P}^1_K$ are Chebyshev polynomials and Lattès maps, which come from the multiplicative group or an elliptic curve, these will be introduced in Section 4.2. These three families of maps are the only rational dynamically affine morphisms on $\mathbb{P}^1_{\mathbb{C}}$ (Theorem 6.79 in [Sil07]). When K has positive characteristic we also need to consider (sub)additive polynomials, which will be introduced in 5.1.

3

AUTOMATA THEORY AND ITS NUMBER THEORETICAL APPLICATIONS

Automata theory is the study of virtual machines known as automata. An automaton is a very basic notion of a computational model and has its origin in theoretical computer science, with links to logic, combinatorics and number theory. In particular, automatic sequences are of interest to us as we can relate these to the coefficient sequences of formal power series.

3.1 AUTOMATA THEORY

In this section we will introduce the basic notions of automata theory using definitions, examples and theorems from [AS03].

Definition 3.1.1. An **alphabet** Σ is a nonempty set of symbols.

Often the alphabet consists of symbols which we will denote with numbers, like $\mathtt{0}, \mathtt{1}, \mathtt{2}, \mathtt{3}, \ldots$. Note that an alphabet is not necessarily finite.

Definition 3.1.2. Let Σ be an alphabet. A **word** or **string** is a finite or infinite list of symbols in Σ, often denoted without comma's or spacing. With Σ^* we denote the Kleene closure of Σ; it is the set of all finite words on Σ.

Example 3.1.3. One of the most ubiquitous family of alphabets in number theory is $\Sigma_k := \{\mathtt{0}, \ldots, \mathtt{k-1}\}$ for $k \geq 2$. Although, the symbols do not necessarily represent the integers, we often do identify them with each other. Let $w \in \Sigma^*$. We can write $w = w_t \cdots w_0$, where $w_t, \ldots, w_0 \in \Sigma$ and t is some non-negative integer. Then we can introduce

$$[w]_k = \sum_{i=0}^{t} w_i k^i.$$

Note that any word w will give the same value if we add zeroes on the left. For example in the decimal system: $[\mathtt{000501}]_{10} = [\mathtt{501}]_{10}$. We consider the word $\mathtt{501}$ as the *canonical* word corresponding to the integer 501 in the decimal system, as it contains no leading zeroes. We write $(n)_k$ for the canonical word of n in base k. That is $[(n)_k]_k = n$ and $(n)_k$ has no leading zeroes.

With this basic vocabulary we can now introduce automata. There are several types of automata, so we will start with a simpler version of what we will need in the end.

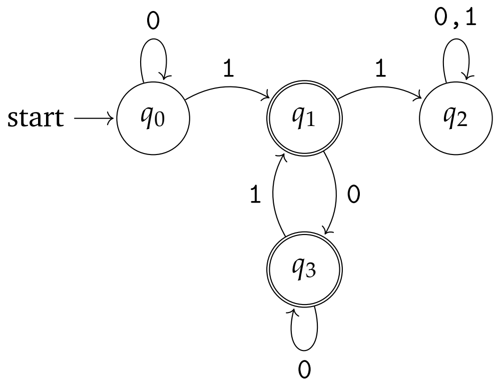
Definition 3.1.4. A **deterministic finite automaton** (DFA) is a 5-tuple $M = (Q, \Sigma, \delta, q_0, F)$, where

- Q is a finite set of states;
- Σ is an input alphabet;
- $\delta : Q \times \Sigma \to Q$ is a transition function;
- $q_0 \in Q$ is a begin state;
- $F \subset Q$ is a set of accepting states.

Note that the transition $\delta : Q \times \Sigma \to Q$ can be extended on words. Given a begin state, one can apply delta to this state and the rightmost letter of a word to get to a new state and then use the next letter to go to another state, etc. To make this more formal: we can define $\delta' : Q \times \Sigma^* \to Q$ in the following way $\delta'(q, (a_n, \ldots, a_0)) = \delta(\ldots(\delta(\delta(q, a_0), a_1), \ldots, a_n)$. We will usually denote the extended map on $Q \times \Sigma^* \to Q$ also by δ.

We can describe a DFA by a diagram: the states are represented by circles; the transition function consists of arrows between the nodes which depend on the input alphabet; the begin state will have start arrow and lastly; the accepting states are represented by taking double circles. To clarify, we give an example.

Example 3.1.5. We can think of a DFA as a machine which either accepts or rejects certain words on our input alphabet. We will give an example by defining which words the DFA will accept. Let $\Sigma = \{0, 1\}$ and we accept words which contain at least one 1, but no two consecutive 1's.



A more general notion is the following.

Definition 3.1.6. A **deterministic finite automaton with output** (DFAO) is a 6-tuple $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$, where

- Q is a finite set of states;
- Σ is the input alphabet;
- $\delta : Q \times \Sigma \to Q$ is a transition function;
- $q_0 \in Q$ is the begin state;

- Δ is the output alphabet;
- $\tau : Q \to \Delta$ is the output function.

Just like the DFA, a DFAO can also be described using a diagram: the states are represented by circles; the transition function consists of arrows between the nodes which depend on the input alphabet; the begin state will have an incoming arrow with the word "start". In some of the literature on automata the circles do not only contain the state, but also the corresponding output given by τ. However, we chose to omit the output.

We claimed that a DFAO is a more general notion than a DFA. It is easy to turn a DFA into a DFAO by the following construction. Define $\Delta = \{\text{accepting}, \text{rejecting}\}$ to be the output alphabet, and define the output function as

$$\tau(q) := \begin{cases} \text{accepting} & \text{if } q \in F; \\ \text{rejecting} & \text{if } q \notin F. \end{cases}.$$

The last type of automata we will introduce is a specific family within the DFAO's.

Definition 3.1.7. A k**-DFAO** is a DFAO $M = (Q, \Sigma, \delta, q_0, \Delta, \tau)$, where $\Sigma = \Sigma_k$ for $k \in \mathbb{Z}_{\geq 1}$.

This family allows us to talk about the notion of automatic sequences.

Definition 3.1.8. A sequence $(a_n)_{n\geq 0}$ on an alphabet Δ is called k**-automatic** for $k \in \mathbb{Z}_{\geq 1}$ if there exists a k-DFAO $M = (Q, \Sigma_k, \delta, q_0, \Delta, \tau)$, such that $a_n = \tau(\delta(q_0, w))$ for all $w \in \Sigma_k^*$ with $[w]_k = n$, for all $n \geq 0$.

Note that we demand that the automaton gives us the correct output, even when we insert a word with leading zeroes. It turns out that it suffices to just look at the canonical word. This is expressed in the following theorem.

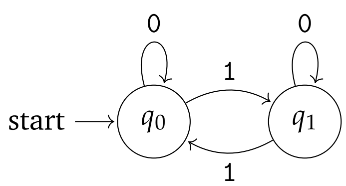
Theorem 3.1.9. *The sequence $(a_n)_{n\geq 0}$ is k-automatic if and only if there exists a k-DFAO M such that $a_n = \tau(\delta(q_0, (n)_k))$ for all $n \geq 0$. Moreover, we may choose M such that $\delta(q_0, 0) = q_0$.*

Proof. See the proof of Theorem 5.2.1. in [Sil07]. □

Example 3.1.10. A famous automatic sequence is the Thue-Morse sequence. Let $(t_n)_{n\geq 0}$ denote the sequence, defined by

$$t_n = \begin{cases} 0 & \text{if the number of 1's in the base 2-expansion of } n \text{ is even;} \\ 1 & \text{if the number of 1's in the base 2-expansion of } n \text{ is odd;} \end{cases}.$$

We can make a 2-DFAO with 2 states $\{q_0, q_1\}$ which generates the Thue-Morse sequence.



Here q_0 is the state with output $t_n = 0$ and q_1 has $t_n = 1$ as output. Clearly, we start with output zero and whenever we get a 1 the parity of the number of 1's changes, and whenever we get a zero, the parity remains the same. The automaton above clearly represents this behaviour.

3.2 NUMBER THEORETICAL APPLICATIONS

In this section we will focus on automatic sequences and how to determine which sequences can or cannot be p-automatic for a prime p. We will obtain many tools throughout this section which will play a major role in many of the proofs presented in Chapter 5. We start with a famous theorem which truly exemplifies the connection between automata theory and number theory.

Theorem 3.2.1 (Christol). *Let p be a prime and let $\sum_{i=0}^{\infty} b_i t^i \in \mathbb{F}_p[\![t]\!]$ be a formal power series. Then this power series is algebraic over $\mathbb{F}_p(t)$ if and only if the coefficient sequence $(b_i)_{i\geq 0}$ is p-automatic.*

Proof. See the proof of Theorem 12.2.5. in [AS03]. □

This theorem has a very practical corollary.

Corollary 3.2.2. *Let $\sum_{i=0}^{\infty} b_i t^i \in \mathbb{Z}[\![t]\!]$ be a formal power series. If it is algebraic over $\mathbb{Q}(t)$, then for every prime p the reduced coefficient sequence $(b_n \mod p)_{n\geq 0}$ is p-automatic.*

Proof. Let us write $f(t) := \sum_{i=0}^{\infty} b_i t^i$ for the formal power series. Assume f is algebraic over $\mathbb{Q}(t)$. Then there exists a polynomial $P(X)$ of degree at least 1 with coefficients in $\mathbb{Q}(t)$ such that $P(f) = 0$. Let us write $P(X) = a_n(t)X^n + \ldots + a_0(t)$, where $a_i(t) \in \mathbb{Q}(t)$, such that for all primes there is at least one a_i with $v_q(a_i) = 0$. Now we can write each $a_i(t) = \tilde{a}_i(t)/\alpha_i(t)$, where $\tilde{a}_i(t), \alpha_i(t) \in \mathbb{Z}[t]$ and for each i we have $(\tilde{a}_i(t)$ is coprime to $\alpha_i(t)$ in $\mathbb{Z}[t]$.

Define $\alpha(t)$ as the least common multiple of all $\alpha_i(t)$, and define $\tilde{P}(X) := \alpha(t)P(X)$. It follows that $\tilde{P}(f(t)) = \alpha(t)P(f(t)) = \alpha \cdot 0 = 0$. So we get

$$\tilde{P}(X) = a'_n(t)X^n + \ldots + a'_0(t),$$

where $a'_i(t)$ is a multiple of $\tilde{a}_i(t)$. By definition of $\tilde{a}_i(t)$ it must follow that $a'_i(t) \in \mathbb{Z}[t]$. Note that by taking the least common multiple the $a'_i(t)$ are not all divisible by some non-unit in $\mathbb{Z}[t]$. Hence we can define $\overline{a}_i(t) := a'_i(t) \mod p$ in $\mathbb{F}_p(t)$ and henceforth we get $\overline{P}(X) = \overline{a}_n(t)X^n + \ldots \overline{a}_0(t)$. Similarly, we define $\overline{b}_i := b_i \mod p$ in $\mathbb{F}_p$ which also gives us $\overline{f}(t) := \sum_{i=0}^{\infty} \overline{b}_i t^i \in \mathbb{F}_p[\![t]\!]$.

Since $\tilde{P}(f(t)) = 0$ in $\mathbb{Z}[t]$, we also know that $\tilde{P}(f(t)) \mod p \equiv 0$ in $\mathbb{F}_p[t]$. This is equivalent to saying that $\overline{P}(\overline{f}(t)) = 0$ in $\mathbb{F}_p$. We need that $\overline{P}$ is not identically zero. To get a contradiction, assume however that $\overline{P}$ is identically zero. This happens if and only if $\overline{a}_i(t) = 0$ for all $i = 0, \ldots, n$. This is equivalent to $a'_i(t) = 0 \mod p$. By construction all $a'_i(t)$ are coprime over $\mathbb{Z}[t]$, in particular they cannot all be divisible by p. Hence, this gives a contradiction. □

As the statements in Chapter 5 often include the notion of transcendence, we need tools to prove that a specific sequence is not automatic for a certain (prime) number. The following theorem is a great means to this end.

Theorem 3.2.3 (Cobham)**.** *Let p and q be multiplicatively independent integers (i.e. $\log p / \log q \notin \mathbb{Q}$), at least 2. If the sequence $(a_n)_{n\geq 0}$ is both p-automatic and q-automatic, then $(a_n)_{n\geq 0}$ is eventually periodic, i.e. there exists an integer $N \geq 0$, such that the sequence $(a_n)_{n\geq N}$ is periodic.*

Proof. See the proof of Theorem 11.2.2. in [AS03]. In fact this is a corollary of the original Cobham's Theorem, given as Theorem 11.2.1. in [AS03]. □

To apply the aforementioned theorems we often need to modify the given sequence to make it fit in the framework. We will provide several theorems and propositions which will be useful tools when proving that certain sequences are not p-automatic for a prime p.

Theorem 3.2.4. *Let $(a_n)_{n\geq 0}$ be an eventually periodic sequence, then $(a_n)_{\geq 0}$ is k-automatic for every $k \in \mathbb{Z}_{\geq 1}$*

Proof. See the proof of Theorem 5.4.2. in [AS03]. □

Theorem 3.2.5. *Let $(a_n)_{n\geq 0}$ be a k-automatic sequence. Then for all nonnegative integers b and c, the subsequence $(a_{bn+c})_{n\geq 0}$ is also k-automatic.*

Proof. See the proof of Theorem 6.8.1. in [AS03]. □

Proposition 3.2.6. *Let $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ be two k-automatic sequences both with values in the output alphabet Δ. Let $f : \Delta \times \Delta \to \Delta$ be any binary operation. Then the sequence $(f(a_n, b_n))_{n\geq 0}$ is k-automatic. In particular, if $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ have entries in a ring, this holds for the sum $(a_n + b_n)_{n\geq 0}$ and the product $(a_n \cdot b_n)_{n\geq 0}$.*

Proof. This is a special case of Corollary 5.4.5. in [AS03]. It follows if one just equates all output alphabets. Taking the pointwise sum and pointwise product are binary operations, hence it holds for these cases. □

Proposition 3.2.7. *Let $(a_n)_{n\geq 0}$ be a k-automatic sequences with entries in the ring R, and let $f : R \to R$ be a unary operation. Then the sequence $(f(a_n))_{n\geq 0}$ is k-automatic. In particular, the sequence $(ca_n)_{n\geq 0}$ is k-automatic for $c \in R$ and if a_n is invertible in R for all $n \geq 0$, then the sequence $(a_n^{-1})_{n\geq 0}$ is k-automatic.*

Proof. Let $M = (Q, \Sigma, \delta, q_0, R, \tau)$ be the k-DFAO corresponding to $(a_n)_{n\geq 0}$. We define $\tau' : Q \to R$ defined by $\tau'(q_i) := f(\tau(q_i))$. Consider $M = (Q, \Sigma, \delta, q_0, R, \tau')$. Then this is an k-DFAO and moreover, $\tau'(\delta(q_0, (n)_k)) = f(\tau(\delta(q_0, (n)_k))) = f(a_n)$. Therefore, the sequence $(f(a_n))_{n\geq 0}$ is k-automatic. Multiplying by a scalar and taking the inverse (if defined) clearly are unary operations. □

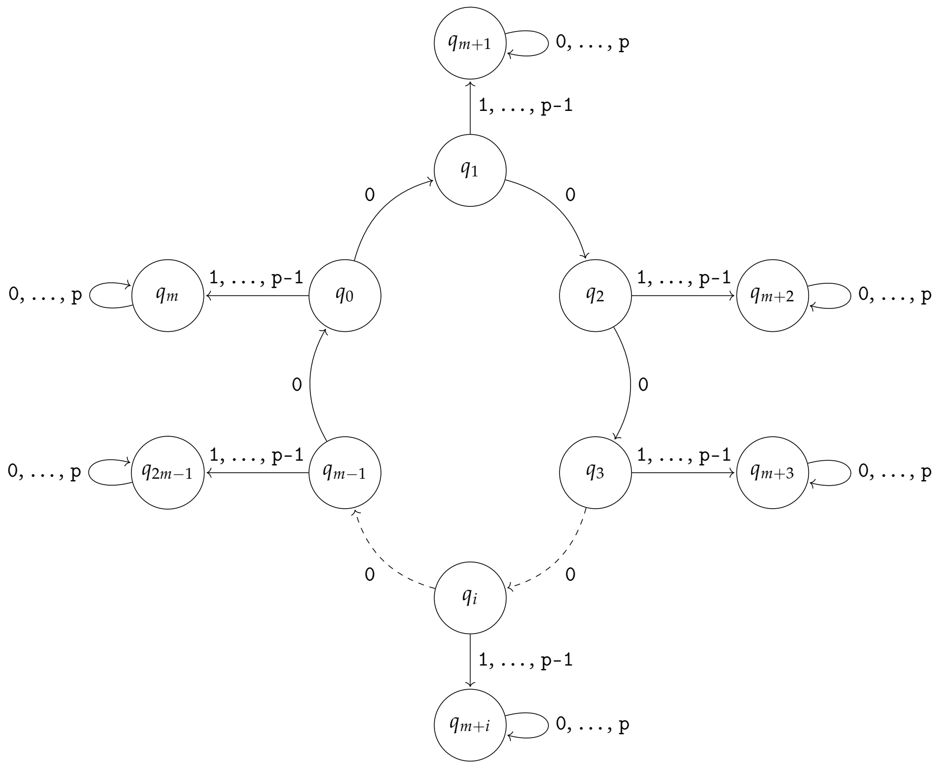
The propositions and theorem mentioned before give very general manipulations. We will now focus on sequences which include a valuation function, e.g. $a_n = a^{v_p(n)}$.

Proposition 3.2.8. *Let p be a prime and m a positive integer. If $(a_n)_{n\geq 0}$ is a function of the equivalence class of $v_p(n) \mod m$, then the sequence $(a_n)_{n\geq 0}$ is p-automatic.*

Proof. Let $\Delta = \{a_i \mid i \geq 0\}$ be the output alphabet. Because a_n only depends on $v_p(n) \mod m$, it can only attain a finite number of outputs, which implies that Δ is finite. This means there exists some function $f : \mathbb{Z}/m\mathbb{Z} \to \Delta$, such that $f(v_p(n) \mod m) = a_n$ for all $n \geq 0$. To prove the proposition we define a p-DFAO $M = (Q, \Sigma_p, \delta, q_0, \Delta, \tau)$, where we take $Q = \{q_0, \dots, q_{2m-1}\}$. Also, we define $\tau : Q \to \Delta$ by $\tau(q_i) = f(i \mod m)$. We define $\delta : Q \times \Sigma_p \to Q$, by

$$\delta(q_i, k) = \begin{cases} q_i & \text{if } i \in \{m, \dots 2m-1\}; \\ q_{i+m} & \text{if } i \in \{0, \dots m-1\} \text{ and } k \neq 0; \\ q_{i+1} & \text{if } i \in \{0, \dots m-2\} \text{ and } k = 0; \\ q_0 & \text{if } i = m-1 \text{ and } k = 0. \end{cases}$$

We can represent this automaton with the following graph, where the dashed arrows illustrate that this continues analogously for all $i \in \{4, \dots, m-2\}$:



□

This proposition gives us the opportunity to obtain the following two propositions which will both be critical to prove significant results in Chapter 5.

Proposition 3.2.9. *Let p and q be distinct primes. Suppose $a \in \mathbb{Z}_+$, $a \not\equiv 0, 1 \mod q$. Also, suppose $\alpha, \beta \in \mathbb{Z}$, with $\alpha \neq 0$ such that $v_p(\alpha) \leq v_p(\beta)$. Let the sequence $(a_n)_{n\geq 0}$ be a sequence with entries in $\mathbb{Z}/q\mathbb{Z}$ be defined by $a_n = a^{v_p(\alpha n+\beta)} \mod q$. Then the sequence $(a_n)_{n\geq 0}$ is not q-automatic.*

Proof. Let d be the multiplicative order of $a \mod q$ in $\mathbb{F}_q$, which exists as $a \not\equiv 0 \mod q$, and d is strictly greater than 1 as $a \not\equiv 1 \mod q$. Then the sequence $b_n = a^{v_p(n)}$ is a function of the equivalence class $v_p(n) \mod d$. We apply Proposition 3.2.8 to see that

b_n is p-automatic. Then $a_n = b_{\alpha n+\beta}$ is also p-automatic by Proposition 3.2.5. Assume by contradiction that a_n is q-automatic. As distinct primes are multiplicatively independent, we apply Theorem 3.2.3 to see that a_n must be eventually periodic.

Let k be the period and $N > 0$ such that $a_{kn+m} = a_m$ for all $m > N$. This means that $a^{v_p(\alpha m+\beta)} \equiv a^{v_p(\alpha(kn+m)+\beta)} \mod q$, which is equivalent to $v_p(\alpha m + \beta) \equiv v_p(\alpha(kn + m) + \beta) \mod d$. Define $\alpha' := \alpha \cdot |\alpha|_p$ and similarly $\beta' := \beta \cdot |\alpha|_p$. Clearly, α' is coprime to p (we use that α is nonzero). Because $v_p(\alpha) \leq v_p(\beta)$ we know $|\alpha|_p \geq |\beta|_p$, hence β' is still an integer. By arguments analogous to earlier ones, we have $v_p(\alpha' m + \beta') \equiv v_p(\alpha'(kn + m) + \beta') \mod d$. Choose $l := v_p(k)$ such that $k' = k/p^l$ and k' is coprime to p. As $\alpha' \neq 0 \mod p$ the following equation is solvable in m:

$$\alpha' m \equiv -\beta' + p^l \mod p^{l+2}.$$

We can choose $m > N$ as the sequence $(a_n)_{n\geq N}$ is periodic. Hence, we get $v_p(\alpha' m + \beta') = l$. Moreover, we can also solve the following equation in n:

$$\alpha' k' n \equiv p - 1 \mod p^{l+2}.$$

Let us multiply this equation with p^l and add it to the previous equation.

$$\alpha'(m + kn) \equiv -\beta' + p^{l+1} \mod p^{l+2}.$$

Therefore, $v_p(\alpha'(m + kn) + \beta') = l + 1$. If we combine our results we obtain $l \equiv l + 1 \mod d$. However, $d > 1$ is in contradiction with this identity. □

Proposition 3.2.10. *Let $a \in \mathbb{Z}_+$ and let p and q be primes with $q > p^{ap^a}$. If p is odd, also assume that $q - 1 \not\equiv 0 \mod p$. If $p = 2$, instead assume that $q \equiv 7 \mod 8$. Let the sequence $(a_n)_{n\geq 0}$ with entries in $\mathbb{Z}/q\mathbb{Z}$ be defined by $a_n = p^{ap^{v_p(n)}} \mod q$. Then this sequence $(a_n)_{n\geq 0}$ is not q-automatic.*

Proof. Because $q > p^{ap^a}$ the primes q and p are distinct. Hence, $p^a \not\equiv 0 \mod q$. We can define d to be the multiplicative order of $p^a \mod q$ in $\mathbb{F}_q$. As $q > p^{ap^a}$, we know that $d > p^a$. The sequence a_n is a function of the equivalence class of $p^{v_p(n)} \mod d$.
Assume p is odd. Then p^a and $q - 1$ are coprime, and as $d \mid \#\mathbb{F}_q^\times = q - 1$, we have that p^a and d are also coprime. Let e be the multiplicative order of $p^a \mod d$ in $\mathbb{Z}/d\mathbb{Z}$, note that $e \neq 1$. Hence, $a_n = a_m$ if and only if $p^{v_p(n)} \equiv p^{v_p(m)} \mod d$, which is equivalent to $v_p(n) \equiv v_p(m) \mod e$. By Proposition 3.2.8 this means a_n is p-automatic.

Secondly, assume $p = 2$. Then $q \equiv 7 \mod 8$, so 2 is a quadratic residue modulo q. This means that $d \mid (q - 1)/2$, which means d is odd and in particular coprime to $p = 2$. Let e be the multiplicative order of $p \mod d$ in $\mathbb{Z}/d\mathbb{Z}$, and as before $e \neq 1$. Similarly to the previous case we get equivalences $a_n = a_m$ if and only if $v_p(n) \equiv v_p(m) \mod e$. In particular by Proposition 3.2.8 a_n is again p-automatic.

Assume the contrary: a_n is q-automatic. Using Cobham's theorem we see that a_n must be eventually periodic. Let k be its ultimate period and $N > 0$ such that $a_{kn+m} = a_m$ for all $m > N$ and $n \geq 0$. In particular we get $v_p(kn + m) \equiv v_p(m) \mod e$. We get a contradiction by analogous arguments as we have seen in the proof of Proposition 3.2.9 with $\alpha = 1$ and $\beta = 0$. □

4

THE DYNAMICAL ZETA FUNCTION IN CHARACTERISTIC ZERO

In this chapter we will examine the dynamical zeta function of maps on varieties over a field K of characteristic zero. Understanding the characteristic zero case allows us to gain important insight into what to expect in positive characteristic. The most examined object on which we will consider self-maps is the projective line $\mathbb{P}^1_K$.

The first section is dedicated to Theorem 4.1.13 and its proof, which tells us that the dynamical zeta function of a rational self-map of degree at least two is rational as well.

In the second section we will exhibit some examples of self-maps on the projective line $\mathbb{P}^1_K$, or on its open subsets: the multiplicative group $\mathbb{G}_m$ and the additive group $\mathbb{G}_a$. This underlying algebraic structure of the maps allows us to give the exact dynamical zeta function. To avoid duplicating certain results, in the second section we will provide results over general fields, to be used in chapters 6 and 5 over a field of positive characteristic.

4.1 RATIONALITY OF THE DYNAMICAL ZETA FUNCTION

This section is based on an article [Lee15] by Junghun Lee. All propositions, lemmas and theorems which are (partially) his are referenced, although some proofs might deviate from the ones in the paper.

Throughout this section K will be a field of characteristic zero and $X = \mathbb{P}^1_K(\overline{K})$. We will consider $f : X \to X$, a rational map. We will always count points over the algebraic closure, hence we will just write $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ and denote the dynamical zeta function as $\zeta_f(T)$.

Because we can consider $\mathbb{P}^1_K(\overline{K})$ as the set $\overline{K} \cup \{\infty\}$, we can view f as a map on this set. So in fact $f : \mathbb{P}^1_K(\overline{K}) \to \overline{K} \cup \{\infty\}$ means that f is a regular map, but we do allow poles. For any $P \in \mathbb{P}^1_K(\overline{K})$ we have the local ring at P, denoted $\mathcal{O}_{P,\mathbb{P}^1_K}$. Let $\mathfrak{m}_P$ be the unique maximal ideal and κ the residue field. We can see f as an element of $\mathcal{O}_{P,\mathbb{P}^1_K}$ for all P which are not a pole of f.

Definition 4.1.1. Let $f \in \overline{K}(t)$ with $f = f_1/f_2$ such that $f_1, f_2 \in \overline{K}[t]$, and f_1 and f_2 have no common factors. Define the **degree** of f as

$$\deg(f) = \max\{\deg(f_1), \deg(f_2)\},$$

where $\deg(f_1)$ and $\deg(f_2)$ are the usual degrees of polynomials.

Definition 4.1.2. Let $f \in \mathcal{O}_{P,\mathbb{P}^1_K}$. Then for some $g \in \overline{K}(t)$ we have $f = g$ on an open $V \subset \mathbb{P}^1_K$. The **degree** of f is equal to the degree of g. Notation: $\deg(f)$.

This appears to depend on the choice of V, however, let V be the largest non-empty open on which f coincides with a rational function g. For any non-empty open U on which f coincides with some rational function h, we have that $f = g = h$ on $U \cap V \neq \emptyset$. In particular, the degree is invariant under the choice of V.

Definition 4.1.3. Let $P \in \mathbb{P}^1_K(\overline{K})$ and $f \in \mathcal{O}_{P,\mathbb{P}^1_K}$. The **multiplicity** at P of f is

$$m_P(f) := \max_{i \geq 0}\{i \mid f(z) - z \in \mathfrak{m}_P^i\}.$$

Note that $m_P(f) \geq 1$ if and only if P is a fixed point of f. Moreover, whether $f(z) - z \in \mathfrak{m}_p^i$ or not, does not depend on coordinates, hence the multiplicity of f at P is invariant under a change of coordinates.

Proposition 4.1.4. *If $P \in \mathbb{P}^1_K$, then the completion of $\mathcal{O}_{P,\mathbb{P}^1_K}$ with respect to the $\mathfrak{m}_p$-adic topology is equal to the ring of formal power series:*

$$\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K} = K[\![\pi_P]\!],$$

where π_P is a uniformizer of the maximal ideal $\mathfrak{m}_P$.

Proof. We denote the maximal ideal of $\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K}$ by $\widehat{\mathfrak{m}}_P$ and the residue field by $\widehat{\kappa}$. Because $\mathbb{P}^1_K$ is nonsingular, $\mathcal{O}_{P,\mathbb{P}^1_K}$ is a regular local ring for all $P \in \mathbb{P}^1_K$. Hence, $\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K}$ is a regular local ring(Theorem 5.4.A in [Har77]). We apply a corollary of Cohen's structure theorem (Corollary p. 307 in [ZS60]) to say that $\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K} = \widehat{\kappa}[\![x_1, \dots, x_n]\!]$, where $\{x_1, \dots, x_n\}$ is a system of regular parameters, i.e. a system of generators of the maximal ideal $\widehat{\mathfrak{m}}_p$. But we have $\widehat{\mathfrak{m}}_P = \mathfrak{m}_P\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K}$(Theorem 5.4.A in [Har77]). Hence, only one generator is needed, namely the uniformizer π_P. We acquire $\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K} = \widehat{\kappa}[\![\pi_P]\!]$. Observe that $K \subset \widehat{\mathcal{O}}_{P,\mathbb{P}^1_K}$, as constants are regular functions and a ring injects naturally into its completion. Now consider the evaluation map $\phi : \widehat{\mathcal{O}}_{P,\mathbb{P}^1_K} \to K$, $f \mapsto f(P)$. This is a group homomorphism with $\ker(\phi) = \widehat{\mathfrak{m}}_P$ and therefore $\operatorname{im}(\phi) \simeq \widehat{\mathcal{O}}_{P,\mathbb{P}^1_K}/\widehat{\mathfrak{m}}_P = \widehat{\kappa}$. Note that $\operatorname{im}(\phi)$ both contains and is contained in K. Ergo $\widehat{\kappa} = K$. This concludes the proof: $\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K} = K[\![\pi_P]\!]$. □

Remark. The elements of $\mathcal{O}_{P,\mathbb{P}^1_K}$ are pairs (f, U) under an equivalence relation. Here f is a regular function on U, which is an open subset of $\mathbb{P}^1_K$ containing P. Two pairs (f, U) and (g, V) are equivalent if and only if $f = g$ on $U \cap V$. Usually we just write f, but for the following corollary, we do need the pair.

Corollary 4.1.5 (Proposition 2.3. in [Lee15]). *Let $(f, U) \in \mathcal{O}_{P,\mathbb{P}^1_K}$ and let x be the local coordinate on U. If $P_x = \alpha$ with $\alpha \in \overline{K}$, then*

$$f(z) = \sum_{i=0}^{\infty} a_n (x - \alpha)^n \in \widehat{\mathcal{O}}_{P,\mathbb{P}^1_K},$$

with $a_i \in \overline{K}$.

Proof. Because $\mathcal{O}_{P,\mathbb{P}^1_K}$ naturally injects into its completion (Theorem 5.4.A in [Har77]), we can consider f as an element of $\widehat{\mathcal{O}}_{P,\mathbb{P}^1_K} = \overline{K}[\![\pi_P]\!]$. First observe that indeed $x - \alpha \in \mathfrak{m}_P$. We know $\mathfrak{m}_p$ is generated by one element, which must divide $(x-\alpha)$ too. Obviously, $\overline{K} \not\subset \mathfrak{m}_P$, therefore $\mathfrak{m}_P$ is not generated by a scalar. So $(x-\alpha)$ is a uniformizer. It follows that f can be written as a formal power series in $(x-\alpha)$ with coefficients in $\overline{K}$. □

Definition 4.1.6. Let $P \in \mathbb{P}^1_K$ and $(f,U) \in \mathcal{O}_{P,\mathbb{P}^1_K}$. Let $\{a_i\}_{i=0}^{\infty}$ be as in Corollary 4.1.5. Define

- $\lambda(f;P) := a_1$;
- $\mu(f;P) := \min_{i\geq 2}\{i \mid a_i \neq 0\}$.

The definition of $\lambda(f;P)$ depends on the choice of the local coordinate on U. In the case that P is a fixed point of f, we call $\lambda(f;P)$ the **multiplier** of f at P.

Note that we can also obtain $\lambda(f;P)$ by taking the formal derivative of f in P, because $f'(x) = a_1 \mod \mathfrak{m}_p$. This provides us with a useful computational definition of $\lambda(f;P)$. Moreover, we have

$$m_P(f) = \begin{cases} 1 & \text{if } \lambda(f;P) \neq 1; \\ \mu(f;P) & \text{if } \lambda(f;P) = 1. \end{cases}$$

Proposition 4.1.7 (Proposition 2.1.(2) in [Lee15]). *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$ and let $P \in \mathbb{P}^1_K$ be a fixed point. Then the following statements hold.*

1. *The multiplier $\lambda(f;P)$ is independent of the local coordinate x.*
2. *For any $k \in \mathbb{Z}_{\geq 0}$ we have $\lambda(f^{\circ k};P) = \lambda(f;P)^k$.*

Proof. (1.) The multiplier is defined on some open affine U with local coordinate x. First note that two pairs (f,U) and (g,V) are equivalent if $f = g$ on $U \cap V$. This means that on any intersection we need to get the same a_1, hence we can consider any open U, as all should result in the same power series on the intersection. We need to consider a change of coordinates. We will write $\lambda(f_x;\alpha)$ and $\lambda(f_y;\beta)$ where $P = (\alpha)_x$ and $P = (\beta)_y$ to emphasize the two different coordinate systems. We can write this as a linear coordinate change given by a map $\phi : \mathbb{P}^1_{K,y} \mapsto \mathbb{P}^1_{K,x}$, where the subscripts denote the coordinates. Therefore, we can write $f_y = \phi^{-1} \circ f_x \circ \phi$. We compute $\lambda(f_y;\beta)$:

$$\begin{aligned}
\lambda(f_y;\beta) &= \lambda(\phi^{-1} \circ f_x \circ \phi; \phi^{-1}(\alpha)) \\
&= (\phi^{-1} \circ f_x \circ \phi)'(\phi^{-1}(\alpha)) \\
&= (\phi^{-1})'(f_x(\phi(\phi^{-1}(\alpha)))) \cdot f_x'(\phi(\phi^{-1}(\alpha))) \cdot \phi'(\phi^{-1}(\alpha)) && \text{(chain rule)} \\
&= (\phi^{-1})'(f_x(\alpha)) \cdot f_x'(\alpha) \cdot \phi'(\phi^{-1}(\alpha)) && (\phi \circ \phi^{-1} = \mathrm{id}) \\
&= (\phi^{-1})'(f_x(\alpha)) \cdot f_x'(\alpha) \cdot \phi'(\phi^{-1}(f_x(\alpha))) && (\alpha = f_x(\alpha)) \\
&= (\phi \circ \phi^{-1})'(f_x(\alpha)) \cdot \lambda(f_x;\alpha) && \text{(chain rule)} \\
&= \lambda(f_x;\alpha).
\end{aligned}$$

Henceforth, we can truly write $\lambda(f;P)$.
(2.) We use that $f^{\circ i}(P) = P$ for all i. Let us compute $\lambda(f^{\circ k};P)$ using the chain rule for derivatives.

$$\lambda(f^{\circ k};P) = (f^{\circ k})'(\alpha) = \prod_{i=0}^{k-1} f'(f^{\circ i}(\alpha)) = \prod_{i=0}^{k-1} f'(\alpha) = \prod_{i=0}^{k-1} \lambda(f;\alpha) = \lambda(f;P)^k.$$

□

Remark. Note that the requirement that P is fixed is necessary for $\lambda(f;P)$ to be independent of the choice of coordinates. We define $f_x : \mathbb{P}^1_{K,x} \to \mathbb{P}^1_{K,x}$ by $f(x) = x^2+1$, and $f_x(\infty) = \infty$. We introduce the coordinate change $y = 1/x$. So $\phi : \mathbb{P}^1_{K,y} \to \mathbb{P}^1_{K,y}$ with $\phi(0) = \infty$, $\phi(\infty) = 0$ and $\phi(a) = 1/a$ for $a \in \overline{K}^{\times}$. We can see that $f_x(1) = 2 \neq 1$. So 1_x is not a fixed point. Note that $\phi^{-1}(1) = \{1\}$.

$$\begin{aligned}\frac{d(\phi^{-1}\circ f_x \circ \phi)}{dy}(1) &= \frac{d\left(\frac{1}{(\frac{1}{y})^2+1}\right)}{dy}(1)\\ &= \frac{2y(1+y^2)-2y\cdot y^2}{(1+y^2)^2}\Big|_{y=1}\\ &= \frac{2(1+1)-2}{2^2} = \frac{1}{2}.\end{aligned}$$

But we can also compute

$$\frac{df_x}{dx}(1) = 2x\Big|_{x=1} = 2.$$

Next we discuss the remark given in the introduction of [Lee15] in the form of a proposition.

Proposition 4.1.8. *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree zero or one over K, a field of characteristic 0. Then the dynamical zeta function $\zeta_f(T)$ is algebraic over $\mathbb{Q}$. Moreover, all zeros lie on the unit circle.*

Proof. If f is of degree 0, it must be constant. Let $f = c$ for some $c \in \mathbb{P}^1_K$. Then we know that $f^{\circ n} = c$. We can easily solve $f^{\circ n}(x) = x$, because we get exactly 1 solution: $x = c$. So $\mathcal{N}_n = 1$ for all $n \geq 1$. We compute the zeta function:

$$\zeta_f(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\mathcal{N}_n}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{1}{n} T^n\right) = \exp\left(\log\left(\frac{1}{1-T}\right)\right) = \frac{1}{1-T}.$$

Let f be of the form $f(x) = ax+b$ with $a, b \in K$ and $a \neq 0$. We first treat this case and then reduce all other cases to this one. The composition is easily determined:

$$f^{\circ n}(x) = a(a(\ldots a(ax+b)+b)\ldots+b)+b = a^n x + a^{n-1}b + \ldots + ab + b.$$

We will write this as $f^{\circ n}(x) = a^n x + c_n$. Next we solve $f^{\circ n}(x) = x$:

$$a^n x + c_n = x \qquad \Longleftrightarrow \qquad (a^n - 1)x = -c_n.$$

To see that ∞ is fixed, use the transformation $x = 1/y$. We obtain $1/f(1/y) = \frac{y}{a+by}$, which we consider in $y = 0$. We can see $y = 0$ is fixed. Hence, ∞ is fixed.
Here we need to make a distinction. If $a^n \neq 1$ then we have precisely two solutions: $x = \frac{-c_n}{1-a^n}$ and ∞. So $\mathcal{N}_n = 2$ for all such n. If this holds for all $n \geq 1$, we can compute $\zeta_f(T)$:

$$\zeta_f(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\mathcal{N}_n}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{2}{n} T^n\right) = \exp\left(2\log\left(\frac{1}{1-T}\right)\right) = \frac{1}{(1-T)^2}.$$

However, if $a^n = 1$, then we need the equation $0 = -c_n$ to hold. Now observe that $c_n = b(a^{n-1} + \ldots + 1)$. If $a = 1$, then $c_n = nb$. Here we need that $\mathrm{char}(K) \nmid n$ to say that $c_n = 0$ if and only if $b = 0$. If $b = 0$, we have the identity map and hence infinitely many solutions, so $\mathcal{N}_k = 0$. If $b \neq 0$ we have a translation, only ∞ is fixed. Hence, $\mathcal{N}_n = 1$ for all $n \geq 1$. We obtain the same result as in the constant case. If $a \neq 1$, then $0 = a^n - 1 = (a-1)(a^{n-1} + \ldots + 1)$ implies that $c_n = 0$. Hence, all points are solutions of the equation $f^{\circ n}(x) = x$. This means we have infinitely many fixed points, therefore $\mathcal{N}_n = 0$ for such n.
Let q be the smallest positive integer such that $a^q = 1$. Then

$$\mathcal{N}_n = \begin{cases} 2 & \text{if } q \mid n; \\ 0 & \text{if } q \nmid n. \end{cases}$$

We can determine the zeta function:

$$\begin{aligned}\zeta_f(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\mathcal{N}_n}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{1}{n} T^n - \sum_{\substack{n=1,\\ q\mid n}}^{\infty} \frac{1}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{1}{n} T^n - \frac{1}{q} \sum_{\ell=1}^{\infty} \frac{1}{\ell} (T^q)^\ell\right) \\ &= \exp\left(\log\left((1-T)^{-1}\right) - \frac{1}{q}\log\left((1-T^q)^{-1}\right)\right) = (1-T)^{-1} \cdot (1-T^q)^{\frac{1}{q}}.\end{aligned}$$

Lastly, we will discuss the case where $\mathrm{char}(K) = p \mid n$ and $a = 1$. We observe that $f(x) = x + b$, and hence $f^{\circ n}(x) = x + nb$. If $b = 0$ we find the identity map, hence there are infinitely many solutions. Hence, $\mathcal{N}_n = 0$ for all n. If $p \mid n$, then $f^{\circ n}(x) = x$, hence $\mathcal{N}_n = 0$ as there are infinitely many fixed points.

Let f be any rational map of degree 1. Then it is of the form $f(x) = \frac{ax+b}{cx+d}$, with $a, b, c, d \in K$ such that $ad - bc \neq 0$, otherwise the map would be of degree 0. Since f has at least one fixed point, we can assume it is ∞ by some change of coordinates. This means we can reduce each degree 1 case to the $ax + b$ case.
The fact that all zeros lie on the unit circle, follows easily from the expressions found. □

Proposition 4.1.9 (Corollary 2.2. in [Lee15]). *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$. Then the number of fixed points of $f^{\circ n}$ in $\mathbb{P}^1_k$ is exactly $d^n + 1$, counted with multiplicity.*

Proof. Because f is of degree d at least 2, it cannot be the identity map. Hence, there is at least one point not fixed. Using some change of coordinates we may assume ∞ is not fixed. Let us write $f = f_1/f_2$, where f_1, f_2 are polynomial maps with no common factors. Since ∞ is not a fixed point, we know that $\deg(f_1) \leq \deg(f_2)$, as the numerator cannot increase faster than the denominator. Therefore, $d = \deg(f_2)$. Observe that $\alpha \in \overline{K}$ is fixed if and only if

$$\frac{f_1(\alpha)}{f_2(\alpha)} = \alpha \iff f_1(\alpha) - \alpha f_2(\alpha) = 0.$$

We obtain $f_1(z) - zf_2(z)$, which is a polynomial over K. Because $\deg(f_1) \leq \deg(f_2) = d$, this polynomial is of degree $d+1$. Since $\overline{K}$ is algebraically closed, this polynomial has precisely $d+1$ zeros, counted with multiplicity. Since ∞ is not a fixed point, all fixed points lie in $\overline{K}$. This means that f has precisely $d+1$ fixed points counted with multiplicity.

As multiplicities of fixed points are preserved under a change of coordinates this result holds for any f. In particular under a change of coordinates we may assume ∞ is fixed. Hence, we can reverse the assumption on the degrees to $\deg(f_1) > \deg(f_2)$. We use this for the following claim, just for simplification of the proof.

Claim: If $f = f_1/f_2$ with $d := \deg(f_1) > \deg(f_2) = e$, then $f^{\circ n} = g_1/g_2$ with $\deg(g_1) = d^n > \deg(g_2)$.

We will prove our claim using induction. For $n = 1$ it is true by definition. Assume it is true for n and consider $f^{\circ(n+1)}$. We will write $f^{\circ n} = g_1/g_2$ as in the claim.

$$f^{\circ(n+1)} = f(f^{\circ n}) = \frac{f_1(g_1/g_2)}{f_2(g_1/g_2)} = \frac{g_2^{-d}\tilde{f}_1}{g_2^{-e}\tilde{f}_2} = \frac{\tilde{f}_1}{g_2^{d-e}\tilde{f}_2},$$

where $\tilde{f}_1 := g_2^d f_1(g_1/g_2)$ and $\tilde{f}_2 := g_2^e f_2(g_1/g_2)$. Note that both $\tilde{f}_1$ and $g_2^{d-e}\tilde{f}_2$ are polynomials. We need to check whether they have common factors. Let us write $f_1 = c_1 \prod_{i=1}^d (x - \alpha_i)$ and $f_2 = c_2 \prod_{i=1}^e (x - \beta_i)$. Then

$$\tilde{f}_1 = g_2^d c_1 \prod_{i=1}^d (g_1/g_2 - \alpha_i) = c_1 \prod_{i=1}^d (g_1 - \alpha_i g_2), \quad \text{and similarly} \quad \tilde{f}_2 = c_2 \prod_{i=1}^e (g_1 - \beta_i g_2).$$

If $\tilde{f}_1$ and $g_2^{d-e}\tilde{f}_2$ have an irreducible non-constant common component h, then $h \mid g_2$ or $h \mid \tilde{f}_2$ and $h \mid \tilde{f}_1$. If $h \mid g_2$ and $h \mid \tilde{f}_1$, then $h \mid g_1^d$. This is a contradiction with the assumption that g_1/g_2 is reduced. If $h \mid \tilde{f}_1$ and $h \mid \tilde{f}_2$, then h will divide some some factor: $h \mid g_1 - \alpha_i g_2$ and $h \mid g_1 - \beta_j g_2$. Hence, the difference is also divisible by h: $h \mid g_2(\alpha_i - \beta_j)$. As h is non-constant, $h \mid g_2$. However, this implies that $h \mid g_1$, which is again a contradiction. Hence, the polynomials have no common components.

We can conclude that $\deg(f^{\circ(n+1)}) = \max(\deg(\tilde{f}_1), \deg(g_2^{d-e}\tilde{f}_2))$. We observe that

$$\deg(\tilde{f}_1) = \deg\left(c_1 \prod_{i=1}^d (g_1 - \alpha_i g_2)\right) = d \cdot \deg(g_1 - \alpha_i g_2) = d \cdot \deg(g_1) = d^{n+1}.$$

Similarly, we find

$$\begin{aligned}\deg(g_2^{d-e}\tilde{f}_2) &= \deg(g_2^{d-e}) + \deg(\tilde{f}_2)\\ &= (d-e)\deg(g_2) + \deg(c_2 g_1^e) = (d-e)\deg(g_2) + ed^n.\end{aligned}$$

By the induction hypothesis $\deg(g_2) \leq d^n$. Hence, we see that $(d-e)\deg(g_2) + ed^n \leq (d-e)d^n + ed^{n+1} = d^{n+1}$. So indeed, $f^{\circ(n+1)}$ has degree d^{n+1}. The claim is proven.
We may assume f has at least one fixed point, hence we may assume it is the point at infinity. If we use the first part of the proposition and apply it to $f^{\circ n}$ we can use the claim to see that $f^{\circ n}$ has precisely $d^n + 1$ fixed points, counted with multiplicity. This concludes the proof. □

Lemma 4.1.10 (Lemma 3.2. in [Lee15]). *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$ and let α be a periodic point of f with minimal period n. Suppose that $\{f^{\circ k}(\alpha)\}_{k=0}^{n-1}$ is contained in K. Then $m_{f^{\circ k}(\alpha)}(f^{\circ n}) = m_\alpha(f^{\circ n})$ for all $k \in \{0, 1, \ldots, n-1\}$.*

Proof. We write $f(z)$ as a formal power series near $\alpha_k := f^{\circ k}(\alpha)$ using Proposition 4.1.5. For each α_k we get such a power series, denoted f_k.

$$f_k(z) = f(\alpha_k) + \lambda_k(z-\alpha_k) + a_{\mu_k}(z-\alpha_k)^{\mu_k} + \ldots$$

Note that for each α_k there is some U_k, formally $(f, U_k) \in \mathcal{O}_{P,\mathbb{P}^1_K}$. Because of the equivalence, the f_k will remain the same on the intersection $U := \cap_{k=0}^{n-1} U_k$. This set is open and contains P, hence we can consider each f_k on this open U. Note that $f^{\circ n}(\alpha_k) = \alpha_k$, because n is the minimal period of f. This means that $\alpha_k = \alpha_{k+nm}$ for all $m \geq 1$. Hence, $f_k(z) = f_{k+nm}(z)$ for all $m \geq 1$. Moreover, $\lambda_k = \lambda(f;\alpha_k) = \lambda(f;\alpha_{k+nm}) = \lambda_{k+nm}$ for all $m \geq 1$ and $\mu_k = \mu(f;\alpha_k) = \mu(f;\alpha_{k+nm}) = \mu_{k+nm}$ for all $m \geq 1$. Therefore, it makes sense to speak of f_k, α_k, λ_k and μ_k, where we restrict $k \in \mathbb{Z}/n\mathbb{Z}$. From now on k will denote an element in $\mathbb{Z}/n\mathbb{Z}$.
Next we obtain $f^{\circ n}$ using n different representations of f, namely those f_k with $k \in \mathbb{Z}/n\mathbb{Z}$. We can then find $f^{\circ n}$ near α_k by computing $f^{\circ n} = f_{k-1} \circ f_{k-2} \circ \ldots \circ f_{k+1} \circ f_k$. We define a partial composite $g_{k,i} := f_{k+i} \circ f_{k+i-1} \circ \ldots \circ f_{k+1} \circ f_k$, where $k, i \in \mathbb{Z}/n\mathbb{Z}$.
Claim:

$$\begin{aligned}g_{k,i} =& \alpha_{k+i+1} + \lambda_k \cdot \ldots \cdot \lambda_{k+i}(z-\alpha_k)\\ &+ \sum_{j=k}^{k+i} \lambda_k^{\mu_j} \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+i}(z-\alpha_k)^{\mu_j} + \ldots\end{aligned}$$

We let k fixed and prove this by induction on i. First for $i = 0$:

$$\begin{aligned}g_{k,0} = f_k &= f(\alpha_k) + \lambda_k(z-\alpha_k) + a_{\mu_k}(z-\alpha_k)^{\mu_k} + \ldots\\ &= a_{k+1} + \lambda_k(z-\alpha_k) + \sum_{j=k}^{k} a_{\mu_j}(z-\alpha_k)^{\mu_j} + \ldots\end{aligned}$$

We continue with the induction step. Assume the identity holds for i, and consider $g_{k,i+1}$:

$$\begin{aligned}
g_{k,i+1} &= f_{k+i+1} \circ f_{k+i} \circ \ldots \circ f_{k+1} \circ f_k \\
&= f_{k+i+1}(g_{k,i}) \\
&= f(\alpha_{k+i+1}) + \lambda_{k+i+1}(g_{k,i} - \alpha_{k+i+1}) + \alpha_{\mu_{k+i+1}}(g_{k,i} - \alpha_{k+i+1})^{\mu_{k+i+1}} + \ldots \\
&= \alpha_{k+i+2} + \lambda_{k+i+1}\Big(\lambda_k \cdot \ldots \cdot \lambda_{k+i}(z-\alpha_k) \\
&\quad + \sum_{j=k}^{k+i} \lambda_k^{\mu_j} \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+i}(z-\alpha_k)^{\mu_j} + \ldots\Big) \\
&\quad + \alpha_{\mu_{k+i+1}}\Big(\lambda_k \cdot \ldots \cdot \lambda_{k+i}(z-\alpha_k) \\
&\quad + \sum_{j=k}^{k+i} \lambda_k^{\mu_j} \cdot \ldots \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+i}(z-\alpha_k)^{\mu_j} + \ldots\Big)^{\mu_{k+i+1}} + \ldots \\
&= \alpha_{k+i+2} + \lambda_k \cdot \ldots \cdot \lambda_{k+i} \cdot \lambda_{k+i+1}(z-\alpha_k) \\
&\quad + \sum_{j=k}^{k+i} \lambda_k^{\mu_j} \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+i} \cdot \lambda_{k+i+1}(z-\alpha_k)^{\mu_j} \\
&\quad + \alpha_{\mu_{k+i+1}} \cdot \lambda_k^{\mu_{k+i+1}} \cdot \ldots \cdot \lambda_{k+i}^{\mu_{k+i+1}}(z-\alpha_k)^{\mu_{k+i+1}} + \ldots \\
&= \alpha_{k+i+2} + \lambda_k \cdot \ldots \cdot \lambda_{k+i+1}(z-\alpha_k) \\
&\quad + \sum_{j=k}^{k+i+1} \lambda_k^{\mu_j} \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+i+1}(z-\alpha_k)^{\mu_j} + \ldots
\end{aligned}$$

The claim is proven. Next, we consider $i = n-1 \in \mathbb{Z}/n\mathbb{Z}$.

$$\begin{aligned}
g_{k,n-1} =& \alpha_k + \lambda_k \cdot \ldots \cdot \lambda_{k+n-1}(z-\alpha_k) \\
&+ \sum_{j=k}^{k+n-1} \lambda_k^{\mu_j} \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+n-1}(z-\alpha_k)^{\mu_j} + \ldots
\end{aligned}$$

To see what the multiplicity of $f^{\circ n}$ at α_k is, we must consider $\mu_{n,k} := \min(\mu_j \mid \lambda_k^{\mu_j} \cdot \ldots \cdot \lambda_{j-1}^{\mu_j} \cdot a_{\mu_j} \cdot \lambda_{j+1} \cdot \ldots \cdot \lambda_{k+n-1} \neq 0) = \min(\mu_j)$. Note that this minimum is independent of k. This means that the multiplicity of α_k of $f^{\circ n}$ is independent of k. Hence, the multiplicity is equal for all k. □

Lemma 4.1.11 (Lemma 3.3. in [Lee15]). *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$ and $\alpha \in \mathbb{P}^1_K$ be a fixed point of f. Suppose that there exists a natural number q such that $\lambda(f;\alpha)^q = 1$ and $\lambda(f;\alpha)^l \neq 1$ for any $l \in \{1, 2, \ldots, q-1\}$. Then $\mu(f^{\circ q};\alpha) - 1$ is divisible by q. Moreover, for any natural number k, such that $\mathrm{char}(K) \nmid k$, we have $\mu(f^{\circ q};\alpha) = \mu(f^{\circ kq};\alpha)$.*

Proof. We know there is at least one fixed point and we can assume $\alpha = 0$. So $f(\alpha) = \alpha = 0$. Then we can use Corollary 4.1.5 to write f near α:

$$f(z) = \lambda z + a_\mu z^\mu + \ldots \ ,$$

where $\lambda := \lambda(f;\alpha)$ and $\mu := \mu(f;\alpha)$. We will consider $f^{\circ q}$. Because α is a fixed point of f and by the way q is defined, we have $\lambda(f^{\circ q};\alpha) = \lambda(f;\alpha)^q = 1$, and we write $\tilde{\mu} := \mu(f^{\circ q};\alpha)$. We can write $f^{\circ q}$ near α using Corollary 4.1.5.

$$f^{\circ q}(z) = z + b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots$$

We use these expressions for f and $f^{\circ q}$ to compute $f^{\circ(q+1)}$ near α in two different ways. We wish to obtain information on $\tilde{\mu}$ hence we will also include the term $a_{\tilde{\mu}} z^{\tilde{\mu}}$ in our expression for f. Note that $\tilde{\mu} \geq \mu$, as each term of the iterate f^n is either linear or of degree at least μ.

$$\begin{aligned}(f^{\circ q} \circ f)(z) =& f(z) + b_{\tilde{\mu}} f(z)^{\tilde{\mu}} + \ldots \\ =& (\lambda z + a_\mu z^\mu + \ldots + a_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots) + b_{\tilde{\mu}}(\lambda z + a_\mu z^\mu + \ldots + a_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots)^{\tilde{\mu}} + \ldots \\ =& \lambda z + a_\mu z^\mu + \ldots + a_{\tilde{\mu}} z^{\tilde{\mu}} + b_{\tilde{\mu}} \lambda^{\tilde{\mu}} z^{\tilde{\mu}} + \ldots \\ =& \lambda z + a_\mu z^\mu + \ldots + (a_{\tilde{\mu}} + b_{\tilde{\mu}} \lambda^{\tilde{\mu}}) z^{\tilde{\mu}} + \ldots\end{aligned}$$

Next we use another way to obtain $f^{\circ(q+1)}$.

$$\begin{aligned}(f \circ f^{\circ q})(z) =& \lambda f^{\circ q}(z) + a_\mu (f^{\circ q}(z))^\mu + \ldots + a_{\tilde{\mu}} (f^{\circ q}(z))^{\tilde{\mu}} + \ldots \\ =& \lambda(z + b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots) + a_\mu (z + b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots)^\mu + \ldots + a_{\tilde{\mu}}(z + b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots)^{\tilde{\mu}} + \ldots \\ =& \lambda z + \lambda b_{\tilde{\mu}} z^{\tilde{\mu}} + a_\mu z^\mu + a_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots \\ =& \lambda z + a_\mu z^\mu + (\lambda b_{\tilde{\mu}} + a_{\tilde{\mu}}) z^{\tilde{\mu}} + \ldots\end{aligned}$$

From this we obtain $a_{\tilde{\mu}} + b_{\tilde{\mu}} \lambda^{\tilde{\mu}} = \lambda b_{\tilde{\mu}} + a_{\tilde{\mu}}$. Hence, $b_{\tilde{\mu}}(\lambda - \lambda^{\tilde{\mu}}) = 0$. Since $b_{\tilde{\mu}} \neq 0$ per definition of $\tilde{\mu}$, we have $\lambda - \lambda^{\tilde{\mu}} = 0$. We also know that q is the multiplicative order of λ. If $q = 1$ it trivially divides $\tilde{\mu} - 1$. If $q \neq 1$, then $\lambda^{\tilde{\mu}-1} = 1$, so the order must divide the power: $q \mid \tilde{\mu} - 1$.
To prove the second part of the lemma, we write $f^{\circ kq} = (f^{\circ q})^k$ and use induction. Our claim is

$$f^{\circ kq} = z + k b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots$$

For $k = 1$ it is clear. Assume it is true for k, and $f^{\circ(k+1)q}$:

$$\begin{aligned}f^{\circ(k+1)q)}(z) &= f^{\circ q}(f^{\circ kq}(z)) = f^{\circ kq}(z) + b_{\tilde{\mu}} f^{\circ kq^{\tilde{\mu}}} \\ &= z + k b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots + b_{\tilde{\mu}}(z + k b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots)^{\tilde{\mu}} \\ &= z + k b_{\tilde{\mu}} z^{\tilde{\mu}} + b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots \\ &= z + (k+1) b_{\tilde{\mu}} z^{\tilde{\mu}} + \ldots\end{aligned}$$

The claim is proven. Because $\mathrm{char}(K) \nmid k$, we have that the coefficient $k b_{\tilde{\mu}} \neq 0$. Therefore, we see that $\mu(f^{\circ q};\alpha) = \mu(f^{\circ kq};\alpha)$ for any natural number k coprime to the characteristic. □

Remark. Note that we can see in the proof that the second part of the lemma holds for $k \in \mathbb{Z}_{\geq 1}$ if and only if $\mathrm{char}(K) \nmid k$. This means we know this lemma holds for all k if the field K is of characteristic zero, yet it most certainly does not for a field of positive characteristic.

Lemma 4.1.12 (Lemma 3.1. in [Lee15]). *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$. Then the cardinality of the set*

$$\mathcal{P} := \{P \in \mathbb{P}^1_K \mid \exists n \in \mathbb{Z}_{\geq 1}, \exists q \in \mathbb{Z}_{\geq 1} \text{ such that } f^{\circ n}(P) = P \text{ and } \lambda(f;P)^q = 1\}$$

is finite.

We call a point P **parabolic** if $\lambda(f;P)$ is a root of unity. Hence, the set $\mathcal{P}$ consists of all parabolic periodic points.

Proof. This proof is based on the Lefschetz principle, that translates statements over arbitrary fields of characteristic zero to statements over $\mathbb{C}$ (Section VI §6 in [Sil09]).
Let $f(x) = p(x)/r(x)$, with polynomials $p(x), r(x) \in \mathcal{O}_K[x]$, where $\mathcal{O}_K$ is the ring of integers of K. Let $p_0, \ldots, p_n$ be the coefficients of $p(x)$ and $r_0, \ldots, r_k$ the coefficients of $r(x)$. We define $A = \{p_0, \ldots, p_n, r_0, \ldots, r_k\} \cup (\mathcal{P} \setminus \{\infty\})$, and consider the field $L := \mathbb{Q}(A)$. This is a field of characteristic zero, as K has characteristic zero, and it is a countable extension of $\mathbb{Q}$. Therefore, we get an embedding $\iota : \mathbb{Q}(A) \to \mathbb{C}$ (Section VI §6 in [Sil09]). We can define $\hat{f}(x) \in \mathbb{C}(x)$ as $\hat{p}(x)/\hat{q}(x)$, where these are the polynomials with coefficients $\iota(p_i)$ and $\iota(r_i)$, respectively. Clearly, there is a 1-to-1 correspondence between $\mathcal{P}$ and

$$\mathcal{P}' := \{P \in \mathbb{P}^1_{\mathbb{C}} \mid \exists n \in \mathbb{Z}_{\geq 1}, \exists q \in \mathbb{Z}_{\geq 1} \text{ such that } \hat{f}^{\circ n}(P) = P \text{ and } \lambda(\hat{f};P)^q = 1\}.$$

The set $\mathcal{P}'$ is finite: see proof of Corollary 10.16 in [Mil06]. Hence, $\mathcal{P}$ is finite as well. □

Remark. This Lefschetz principle can be extended to fields of characteristic $p > 0$ for sufficiently large p, but it is not possible to make a general statement like we did here. Note in particular that over the algebraic closure of a finite field there will always exists an $q \in \mathbb{Z}_{\geq 1}$ such that $\lambda(f;P)^q = 1$.

Theorem 4.1.13 (Theorem 1.1. in [Lee15]). *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$ over K. Suppose that the characteristic of K is zero. Then the dynamical zeta function $\zeta_f(T)$ of f on $\mathbb{P}^1_K$ is rational over $\mathbb{Q}$. Moreover, all the zeros of $\zeta_f(T)$ are on the unit circle.*

Proof. As there must be at least one fixed point we can assume without of loss of generality that ∞ is a fixed point of f, so $m_\infty(f^{\circ n}) = 1$ for all $n \geq 1$. We want to count fixed points without multiplicity. If we were to count with multiplicity we would get $d^n + 1$ points (Proposition 4.1.9). Let us define the difference $\mathcal{M}_n := d^n + 1 - \mathcal{N}_n$. This gives us:

$$\begin{aligned}\log\left(\zeta_f(T)\right) &= \sum_{n=1}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{n=1}^{\infty} \frac{d^n + 1 - \mathcal{M}_n}{n} T^n \\ &= \sum_{n=1}^{\infty} \frac{d^n}{n} T^n + \sum_{n=1}^{\infty} \frac{1}{n} T^n - \sum_{n=1}^{\infty} \frac{\mathcal{M}_n}{n} T^n.\end{aligned}$$

We will determine the contributions to $\mathcal{M}_n$ for all periodic points. Note that we can disregard ∞ as it has multiplicity 1. Define

$$B_n := \{\alpha \in \mathbb{P}^1_K \mid \alpha \text{ periodic of exact period } k, \text{ with } k \mid n\} - \{\infty\}.$$

Then we can rewrite $\mathcal{M}_n$ in the following way:

$$\mathcal{M}_n = \sum_{\alpha \in B_n} (m_\alpha(f^{\circ n}) - 1) = \sum_{\alpha \in B_n \cap \mathcal{P}} (m_\alpha(f^{\circ n}) - 1) + \sum_{\alpha \in B_n - \mathcal{P}} (m_\alpha(f^{\circ n}) - 1).$$

Let $\alpha \in B_n$, $\alpha \neq \infty$. Assume $\alpha \notin \mathcal{P}$, then $\lambda(f^{\circ k}; \alpha)^n \neq 1$ for all $n \in \mathbb{Z}_{\geq 1}$ by definition of $\mathcal{P}$. Hence using (Proposition 4.1.7.(2)), $\lambda(f^{\circ nk}; \alpha) \neq 1$ for all $n \in \mathbb{Z}_{\geq 1}$. Therefore, the multiplicity $m_\alpha(f^{\circ n}) = 1$ for all $n \in \mathbb{Z}_{\geq 1}$. This means that for all non-parabolic periodic points, there is no contribution to $\mathcal{M}_n$:

$$\sum_{\alpha \in B_n - \mathcal{P}} (m_\alpha(f^{\circ n}) - 1) = 0.$$

We will take a closer look at $B_n \cap \mathcal{P}$. We first use the fact that the set $\mathcal{P}$ is finite (Lemma 4.1.12), hence $B_n \cap \mathcal{P}$ is finite. This gives us the possibility to partition $\mathcal{P}$ into N cycles C_i generated by some $\alpha_i \in \mathcal{P}$ with minimal period n_i, such that $C_i = \{f^{\circ n}(\alpha_i)\}_{m=1}^{n_i}$ and $\mathcal{P} = \coprod_{i=1}^{N} C_i$. As all $\alpha \in \mathcal{P}$ are periodic, these cycles are well-defined and invariant under f. We obtain a partition of $B_n \cap \mathcal{P}$ for all $n \geq 1$. Note that there is at most one cycle containing ∞ as it has period 1. Hence, we know for all other cycles $C_i \cap B_n = \{\alpha \in C_i \,:\, n_i \mid n\}$ have n_i elements. We can apply this to $\mathcal{M}_n$:

$$\mathcal{M}_n = \sum_{\alpha \in B_n \cap \mathcal{P}} (m_\alpha(f^{\circ n}) - 1) = \sum_{\substack{i=1, \\ n_i \mid n}}^{N} \sum_{\alpha \in C_i} (m_\alpha(f^{\circ n}) - 1) = \sum_{\substack{i=1, \\ n_i \mid n}}^{N} n_i \cdot m_{\alpha_i}(f^{\circ n} - 1).$$

Here we used Lemma 4.1.10, as B_n does not contain ∞. Henceforth, we will only consider $n_i \mid n$. Let q_i be the smallest positive integer such that $\lambda(f^{\circ n_i}; \alpha_i)^{q_i} = 1$ (by definition of $\mathcal{P}$ such a number must exist). Let r_i be the number such that $q_i r_i = \mu(f^{\circ n_i q_i}; \alpha_i) - 1$ (such a number exists due to Lemma 4.1.11). If $n_i q_i \mid n$, then $\lambda(f^{\circ n}; \alpha_i) = \lambda(f^{\circ n_i}; \alpha_i)^{n/n_i} = 1$. Similarly, if $n_i q_i \nmid n$, then $\lambda(f^{\circ n}; \alpha_i) = \lambda(f^{\circ n_i}; \alpha_i)^{n/n_i} \neq 1$. Hence, the multiplicity $m_{\alpha_i}(f^{\circ n}) = 1$, if $n_i q_i \nmid n$. Otherwise, i.e. if $n_i q_i \mid n$, the multiplicity $m_{\alpha_i}(f^{\circ n}) = \mu(f^{\circ n}; \alpha_i) = \mu(f^{\circ n_i q_i}; \alpha_i)$ by Lemma 4.1.11. Lastly, we have that $\mu(f^{\circ n_i q_i}; \alpha_i) = q_i r_i + 1$. This gives us:

$$\mathcal{M}_n = \sum_{\substack{i=1, \\ n_i \mid n}}^{N} n_i (m_{\alpha_i}(f^{\circ n}) - 1) = \sum_{\substack{i=1, \\ n_i q_i \mid n}}^{N} n_i q_i r_i.$$

We use this expression in the computation of the zeta function:

$$\begin{aligned}
\log\left(\zeta_f(T)\right) - \sum_{n=1}^{\infty} \frac{d^n}{n} T^n - \sum_{n=1}^{\infty} \frac{1}{n} T^n &= -\sum_{n=1}^{\infty} \frac{\mathcal{M}_n}{n} T^n = -\sum_{n=1}^{\infty} \frac{1}{n} \sum_{\substack{i=1, \\ n_i q_i \mid n}}^{N} n_i q_i r_i T^n \\
&= -\sum_{i=1}^{N} \sum_{\substack{n=1, \\ n_i q_i \mid n}}^{\infty} \frac{n_i q_i r_i}{n} T^n = -\sum_{i=1}^{N} \sum_{\ell=1}^{\infty} \frac{n_i q_i r_i}{n_i q_i \ell} T^{n_i q_i \ell} \\
&= -\sum_{i=1}^{N} r_i \sum_{\ell=1}^{\infty} \frac{1}{\ell} (T^{n_i q_i})^{\ell} = -\sum_{i=1}^{N} r_i \log\left((1 - T^{n_i q_i})^{-1}\right).
\end{aligned}$$

We can take the exp to see that

$$\zeta_f(T) = (1 - dT)^{-1} \cdot (1 - T)^{-1} \cdot \prod_{i=1}^{N} (1 - T^{n_i q_i})^{r_i}$$

As this is a finite product of rational functions, the zeta function is indeed rational over $\mathbb{Q}$ and all zeros lie on the unit circle. □

4.2 DYNAMICALLY AFFINE MAPS ON $\mathbb{P}^1_K$

To understand the dynamical zeta functions on $\mathbb{P}^1_K$ better, we will compute a few examples of a group-theoretical nature. In a one-dimensional setting we may consider dynamically affine rational maps. Depending on whether the characteristic of the field is zero or positive we can categorize these maps in three, respectively five families, namely in both cases: power maps, Chebyshev polynomials and Lattès maps. When the characteristic is positive, in addition there are two other families: additive polynomials and subadditive polynomials [Bri16]. We will give an overview of results for power maps, Chebyshev polynomials and Lattès maps, we may include some results for fields of arbitrary characteristic, but we will state this clearly.

To avoid duplicating calculations, we use the following proposition:

Proposition 4.2.1. *Let K be a field of characteristic zero and n a positive integer. Then the set of all nth roots of unity $\mu_n := \{x \in \overline{K} \mid x^n = 1\}$ has cardinality n.*

Proof. Define $f(x) = x^n - 1$ and note that $\mu_n = \{x \in \overline{K} \mid f(x) = 0\}$. As f has degree n it has exactly n zeroes, counted with multiplicity. Consider the derivative $f'(x) = nx^{n-1}$. Note that $f'(x) = 0$ if and only if $x = 0$, which is not a zero of f. Henceforth, all zeroes of f have multiplicity one and thus there are exactly n distinct zeroes of f. This means that $|\mu_n| = n$. □

As we are interested in maps on $\mathbb{P}^1_K$, it can occur that some points on $\mathbb{P}^1_K$ are completely fixed, for example a polynomial will not only fix ∞, any other element will never be send to ∞ as well. In a way we just want to ignore such elements. Let S be a set and $f : S \to S$. Let $F \subset S$ be a subset such that

- $F \subset \text{Fix}(f)$;
- $F \cap \cup_{k=0}^{\infty} f^{\circ k}(S - F) = \emptyset$.

Let $x \in S - F$, then $f^{\circ n}(x) \in \cup_{k=0}^{\infty} f^{\circ k}(S - F)$ and by assumption this implies $f^{\circ n}(x) \notin F$. Then $f^{\circ n} : S - F \to S - F$ is well defined for all $n \geq 1$. If the only such set is $F = \emptyset$, then f is called **primitive** on S.

Proposition 4.2.2. *Let S be a set and $f : S \to S$, and assume $\#\text{Fix}(f)$ is finite. For any subset $F \subset \text{Fix}(f) \subset S$ such that $F \cap \cup_{k=0}^{\infty} f^{\circ k}(S - F) = \emptyset$, the following holds:*

$$\zeta_{f,S}(T) = \zeta_{pt}^{\#F}(T) \cdot \zeta_{f,S-F}(T),$$

where $\zeta_{pt}(T) = \frac{1}{1-T}$, that is the dynamical zeta function of any map $g : \{P\} \to \{P\}$. Moreover, there exists a largest set $F_{\max}$ such that f is primitive on $S - F_{\max}$.

Proof. For any such set f can be considered on F and on $S - F$ separately. We can write $f_F : F \to F$ and $f_{S-F} : S - F \to S - F$. Observe that $\#\mathrm{Fix}(f^{\circ n}) = \#\mathrm{Fix}(f_F^{\circ n}) + \#\mathrm{Fix}(f_{S-F}^{\circ n}) = \#F + \#\mathrm{Fix}(f_{S-F}^{\circ n})$. We can use this to obtain the required identity on zeta functions:

$$\begin{aligned}\zeta_{f,S}(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{\#\mathrm{Fix}(f^{\circ n})}{n} T^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{\#F + \#\mathrm{Fix}(f_{S-F}^{\circ n})}{n} T^n\right)\\ &= \exp\left(\sum_{n=1}^{\infty} \frac{\#F}{n} T^n + \sum_{n=1}^{\infty} \frac{\#\mathrm{Fix}(f_{S-F}^{\circ n})}{n} T^n\right)\\ &= \exp\left(\#F \sum_{n=1}^{\infty} \frac{1}{n} T^n\right) \cdot \exp\left(\sum_{n=1}^{\infty} \frac{\#\mathrm{Fix}(f_{S-F}^{\circ n})}{n} T^n\right)\\ &= \zeta_{\mathrm{pt}}^{\#F} \cdot \zeta_{f,S-F}.\end{aligned}$$

To prove the second part of the proposition we will define $F_{\max} := \mathrm{Fix}(f) - \cup_{n=1}^{\infty} f^{\circ n}(S - \mathrm{Fix}(f))$. We prove that f is primitive on $S - F_{\max}$. Assume the contrary, so let $\emptyset \neq E \subset S - F_{\max}$ such that $E \subset \mathrm{Fix}(f)$ and $E \cap \cup_{k=0}^{\infty} f^{\circ k}(S - F_{\max} - E) = \emptyset$. Let $x \in E$, then $x \in \mathrm{Fix}(f) - F_{\max}$. Hence, $x \in \cup_{n=1}^{\infty} f^{\circ n}(S - \mathrm{Fix}(f))$. Because $F_{\max} \subset \mathrm{Fix}(f)$ and $E \subset \mathrm{Fix}(f)$, we have $F_{\max} \cup E \subset \mathrm{Fix}(f)$. This also means that $S - \mathrm{Fix}(f) \subset S - F_{\max} - E$. Therefore, $\cup_{n=1}^{\infty} f^{\circ n}(S - \mathrm{Fix}(f)) \subset \cup_{n=0}^{\infty} f^{\circ n}(S - F_{\max} - E)$. But $x \in \cup_{n=1}^{\infty} f^{\circ n}(S - \mathrm{Fix}(f))$ and $x \notin \cup_{n=0}^{\infty} f^{\circ n}(S - F_{\max} - E)$. Such x cannot exist, hence f is primitive on $S - F_{\max}$. The following then must hold:

$$\zeta_{f,S}(T) = \zeta_{\mathrm{pt}}^{\#F_{\max}} \cdot \zeta_{f,S-F_{\max}}.$$

We claim that $F_{\max}$ is the largest set such that f is primitive on the complement. If there is a set $G \subset \mathrm{Fix}(f)$ such that there exists $x \in G - F_{\max}$, then $x \in \cup_{n=1}^{\infty} f^{\circ n}(S - \mathrm{Fix}(f))$. Which means there exists an $y \in S - \mathrm{Fix}(f)$ and $n \geq 1$ such that $f^{\circ n}(y) = x$. Because $G \subset \mathrm{Fix}(f)$, we have that $S - \mathrm{Fix}(f) \subset S - G$. Hence, $y \in S - G$. So $x \in \cup_{n=0}^{\infty} f^{\circ n}(S - G)$. This means that $G \cap \cup_{n=0}^{\infty} f^{\circ n}(S - G) \neq \emptyset$. Hence, the function f is not primitive on $S - G$. Therefore, $F_{\max}$ is the largest set such that f is primitive on the complement. □

From now on we won't necessarily compute fixed points on $\mathbb{P}^1_K$, but we might only consider points on $\mathbb{P}^1_K \setminus \{\infty\}$ or $\mathbb{P}^1_K \setminus \{\infty, 0\}$.

4.2.1 *Power maps*

First let K have any characteristic. For any $m \in \mathbb{Z}_{\geq 1}$ the mth *power map* is defined by $f(x) = x^m$ on $\mathbb{P}^1_K$. It is clear that 0 and ∞ are always fixed for any m. Hence, we can simply consider f on the multiplicative group $\mathbb{G}_m/K = \mathbb{P}^1_K - \{0, \infty\}$. We observe that $f^{\circ n}(x) = x^{m^n}$. Hence, we solve $x^{m^n} = x$ for $x \in \mathbb{G}_m = K - \{0\}$. This is equivalent to $x^{m^n - 1} = 1$. Therefore, we can see that $\mathrm{Fix}(f^{\circ n}) = \mu_{m^n - 1}$.

Now we let K have characteristic zero, so we can use Proposition 4.2.1 to obtain $\mathcal{N}_n = m^n - 1$. From this we easily find the zeta function.

$$\begin{aligned}\log \zeta_{f,\mathbb{G}_{m,K,0}}(T) &= \sum_{n=1}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{n=1}^{\infty} \frac{m^n - 1}{n} T^n \\ &= \sum_{n=1}^{\infty} \frac{(mT)^n}{n} - \sum_{n=1}^{\infty} \frac{T^n}{n} = \log\left(\frac{1}{1-mT}\right) - \log\left(\frac{1}{1-T}\right).\end{aligned}$$

Hence, we have that

$$\zeta_{f,\mathbb{G}_{m,K,0}}(T) = \frac{1-T}{1-mT}. \tag{4.2.1.1}$$

4.2.2 *Chebyshev polynomials*

Another well-known example of rational maps with a group-theoretical origin is the family of Chebyshev polynomials. At first we will only assume that K is an arbitrary field, not necessarily of characteristic zero. We start with the multiplicative group $\mathbb{G}_m$. On $\mathbb{G}_m$ we have the non-trivial isomorphism $z \mapsto z^{-1}$. This gives rise to the following proposition.

Proposition 4.2.3. *Let $\mathbb{G}_m$ denote the multiplicative group and $\mathbb{G}_a$ the additive group of a field K. Then the map*

$$\begin{aligned}\phi :\ \mathbb{G}_m(\overline{K})/\{x \sim x^{-1}\} &\to \mathbb{G}_a(\overline{K}), \\ z &\mapsto z + z^{-1}\end{aligned}$$

is a bijection.

Proof. We start by showing that ϕ is well-defined. First note that if $x \in \mathbb{G}_m(\overline{K})$, then $x^{-1} \in \mathbb{G}_m(\overline{K})$. Moreover, we can consider $\mathbb{G}_m(\overline{K}) \subset \mathbb{G}_{a,0}(\overline{K})$, hence $a, a^{-1} \in \mathbb{G}_{a,0}(\overline{K})$. We have addition on $\mathbb{G}_{a,0}$, hence $a + a^{-1} \in \mathbb{G}_{a,0}(\overline{K})$. On the left-hand side we have $a \sim a^{-1}$, which proves that ϕ does not depend on the choice of representative: $\phi(a) = a + a^{-1} = a^{-1} + (a^{-1})^{-1} = \phi(a^{-1})$. We continue by proving that the map is surjective. Let $x \in \mathbb{G}_{a,0}(\overline{K})$. We want to solve $z + z^{-1} = x$ for $z \in \mathbb{G}_m(\overline{K})$. Because $z \neq 0$, the equation is equivalent to $z^2 - xz + 1 = 0$. This equation has solutions for $z \in \mathbb{G}_{a,0}(\overline{K})$ as we consider the algebraic closure. Note that $z = 0$ is not a solution. Therefore the equation has solutions for $z \in \mathbb{G}_m(\overline{K})$. The map is thus surjective.
To prove that the map is injective, we start with $w, z \in \mathbb{G}_m(\overline{K})$ such that $z + z^{-1} = w + w^{-1}$. Because we have both $z \neq 0$ and $w \neq 0$, the equation is equivalent to $z^2 w + w = zw^2 + z$, which is equivalent to $(zw - 1)(z - w) = 0$. This gives two possibilities: $z = w$ or $z = w^{-1}$. Because of the equivalence on $\mathbb{G}_m(\overline{K})$ we have that $w = w^{-1} \in \mathbb{G}_m(\overline{K})/\sim$, hence the map is injective. □

Note that the power map $x \mapsto x^d$ commutes with the isomorphism $x \mapsto x^{-1}$. The dth Chebyshev polynomial T_d satisfies an identity closely related to this property.

Definition 4.2.4. The d**th Chebyshev polynomial** is the polynomial in $\mathbb{Z}[w]$ that satisfies the following identity

$$T_d(z+z^{-1}) = z^d + z^{-d}$$

in the field $\mathbb{Q}(z)$.

The definition requires existence and uniqueness. The following proposition will provide all necessary properties.

Proposition 4.2.5. *For each integer $d \geq 0$ there exists a unique monic polynomial $T_d(w) \in \mathbb{Z}[w]$ of degree d satisfying*

$$T_d(z+z^{-1}) = z^d + z^{-d}$$

in the field $\mathbb{Q}(z)$. We call T_d the dth Chebyshev polynomial. Moreover, we have $T_d(T_e(w)) = T_{de}(w)$ for all $d, e \geq 0$.

Proof. See the proof of Proposition 6.6. in [Sil07]. □

For any field containing $\mathbb{Z}$ the dth Chebyshev polynomial naturally exists. For a field of positive characteristic we reduce the coefficients modulo the characteristic.

Proposition 4.2.6. *Let K be any field, and let d be a positive integer. Then the number of fixed points in $\mathbb{G}_a(\overline{K})$ is*

$$|\mathrm{Fix}(T_d^{\circ n})| = \frac{|\mu_{d^n+1}| + |\mu_{d^n-1}|}{2},$$

where μ_{d^n+1} and μ_{d^n-1} denote the sets of (d^n+1)-th and (d^n-1)-th roots of unity, respectively.

Proof. To compute $\mathrm{Fix}(T_d^{\circ n})$, we start by remarking that $T_d^{\circ n} = T_{d^n}$. We also use the bijection $z \mapsto z + z^{-1}$. Hence, by the surjectivity, solving $T_{d^n}(x) = x$ for $x \in \mathbb{G}_{a,0}$ is equivalent to solving $T_{d^n}(z+z^{-1}) = z + z^{-1}$, with $z \in \mathbb{G}_{m,0}$. By definition of the Chebyshev polynomial this is equivalent to $z^{d^n} + z^{-d^n} = z + z^{-1}$. Lastly, using the injectivity of ϕ we know that $z^{d^n} = z$ or $z^{d^n} = z^{-1}$. Note that $z \neq 0$, hence this is equivalent to z being a root of unity of order $d^n - 1$ or $d^n + 1$. We have the following.

$$\begin{aligned}\mathrm{Fix}(T_{d^n}) &= \{x \in \mathbb{G}_{a,0} \mid T_{d^n}(x) = x\} \\ &= \{z + z^{-1} \mid z \in \mathbb{G}_{m,0},\ T_{d^n}(z+z^{-1}) = z + z^{-1}\} \\ &= \{z + z^{-1} \mid z \in \mathbb{G}_{m,0},\ z \in \mu_{d^n-1} \cup \mu_{d^n+1}\}.\end{aligned}$$

Note that $z + z^{-1} = w + w^{-1}$ if and only if $w = z$ or $w = z^{-1}$ by injectivity of ϕ. Hence, most elements in the set occur twice, except for those $z + z^{-1}$ such that $z = z^{-1}$. In other words, the cardinality $|\mathrm{Fix}(T_{d^n})| = 1/2|\mu_{d^n+1} \cup \mu_{d^n-1}| + 1/2|\mu_{d^n+1} \cup \mu_{d^n-1} \cap \mu_2|$. We have that $\mu_{d^n+1} \cap \mu_{d^n-1} = \mu_{d^n+1} \cap \mu_2$. This leads us to the final result.

$$\begin{aligned}|\mathrm{Fix}(T_{d^n})| &= \frac{1}{2}\left(|\mu_{d^n+1}| + |\mu_{d^n-1}| - |\mu_{d^n+1} \cap \mu_{d^n-1}| + |\mu_{d^n+1} \cup \mu_{d^n-1} \cap \mu_2|\right) \\ &= \frac{1}{2}\left(|\mu_{d^n+1}| + |\mu_{d^n-1}|\right).\end{aligned}$$

□

Now let K have characteristic zero. We combine Proposition 4.2.1 and Proposition 4.2.6 to obtain the number of fixed points in $\mathbb{G}_{a,0}(\overline{K})$

$$\mathcal{N}_n = \frac{|\mu_{d^n+1}| + |\mu_{d^n-1}|}{2} = \frac{d^n + 1 + d^n - 1}{2} = d^n.$$

From this the zeta function follows easily:

$$\zeta_{T_d, \mathbb{G}_{a,K,0}}(T) = \exp \sum_{n=1}^{\infty} \frac{d^n}{n} T^n = \frac{1}{1 - dT}. \tag{4.2.2.1}$$

Remark. We count fixed points over $\mathbb{P}^1_K \setminus \{\infty\}$, and from an algebraic point of view the structure of Chebyshev polynomial it should be considered as a dynamically affine map coming from $\mathbb{G}_{m,0}$. This is clear as $\mathbb{P}^1_K \setminus \{\infty\}$ is the Zariski open from Definition 2.2.5 and Proposition 4.2.3 tells us how this map works.

4.2.3 *Lattès maps*

Lastly, we will investigate the family of Lattès maps.

Definition 4.2.7. Let K be any field. Let $\phi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$. We call ϕ a **Lattès map** if there exists an elliptic curve E over K, a morphism $\psi : E \to E$, and a finite separable covering $\pi : E \to \mathbb{P}^1_K$ such that the following diagram commutes.

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1_K & \xrightarrow{\phi} & \mathbb{P}^1_K \end{array} .$$

Let us introduce a family of Lattès maps. Let E/K be an elliptic curve with O_E the identity element in the group. The map $\sigma : E \to E$, defined by $P \mapsto -P$ is an automorphism of order 2 in $\mathrm{Aut}(E)$, i.e. $\sigma^2 = \mathrm{id}$. Hence, the quotient $E/\langle\sigma\rangle$ is isomorphic to $\mathbb{P}^1$(Proposition 6.37. in [Sil07]). We obtain a map $\pi : E \to \mathbb{P}^1$, such that $\pi(P) = \pi(\sigma(P))$ for all $P \in E$. This means that $\pi(P) = \pi(Q)$ if and only if $P = \pm Q$. Consider $m \in \mathbb{Z}_{\geq 2}$ and the map $[m] : E \to E$, which induces a Lattès map $L_m : \mathbb{P}^1 \to \mathbb{P}^1$ such that $L_m \circ \pi = \pi \circ [m]$. The map L_m depends on the chosen elliptic curve. However, we will see that the zeta function does not depend on E if K has characteristic zero and in the positive characteristic case it only depends on whether E is ordinary or supersingular.

Proposition 4.2.8. *Let K be a field, E/K an elliptic curve with identity element O_E and an integer $m \geq 2$. Let L_m be the corresponding Lattès map. Then*

$$|\mathrm{Fix}(L_m^{\circ n})| = \frac{|E_{m^n-1}| + |E_{m^n+1}|}{2}.$$

Proof. To find the fixed points, we start with rewriting $L_m^{\circ n}(x) = x$. As π is a covering, there exists $P \in E$ such that $\pi(P) = x$. From this we get $L_m^{\circ n}(\pi(P)) = \pi(P)$. Now we use the commuting property $L_m \circ \pi = \pi \circ [m]$ repeatedly:

$$L_m^{\circ n}(\pi(P)) = L_m^{\circ(n-1)}(\pi \circ [m])(P) = L_m^{\circ(n-2)}(\pi \circ [m]^{\circ 2}(P)) \ldots = \pi([m]^n(P)).$$

Combine this with the fact that $[m]^{\circ n} = [m^n]$, and we can find the fixed points set. We will denote the set of n-torsion points of $E(K)$ with E_n. We get:

$$\begin{aligned} \mathrm{Fix}(L_m^{\circ n}) &= \{x \in \mathbb{P}^1 \mid L_m^{\circ n}(x) = x\} \\ &= \{x \in \mathbb{P}^1 \mid \pi(P) = x = \pi([m^n]P) \text{ for some } P \in E\} \\ &= \pi(\{P \in E \mid \pi(P) = \pi([m^n]P)\}) \\ &= \pi(\{P \in E \mid P = [m^n]P \text{ or } P = -[m^n]P\}) \\ &= \pi(\{P \in E \mid [m^n - 1]P = O_E \text{ or } [m^n + 1]P = O_E\}) \\ &= \pi(\{P \in E \mid P \in E_{m^n-1} \text{ or } P \in E_{m^n+1}\}) \\ &= \pi(E_{m^n-1}) \cup \pi(E_{m^n+1}). \end{aligned}$$

To determine the cardinality of this set, we use the set-theoretic fact that

$$|\mathrm{Fix}(L_m^{\circ n})| = |\pi(E_{m^n-1})| + |\pi(E_{m^n+1})| - |\pi(E_{m^n-1}) \cap \pi(E_{m^n+1})|.$$

To use this we have the following claim:

Claim: $\pi(E_{m^n+1}) \cap \pi(E_{m^n-1}) = \pi(E_{m^n\pm1}) \cap \pi(E_2) = \pi(E_{m^n\pm1} \cap E_2)$. Moreover, $|\pi(E_{m^n\pm1} \cap E_2)| = |E_{m^n\pm1} \cap E_2|$, where the $\pm$ sign means for either choice of sign.

We start with $\pi(E_{m^n-1}) \cap \pi(E_{m^n+1})$. If $x \in \pi(E_{m^n-1}) \cap \pi(E_{m^n+1})$, then there exists some $P \in E_{m^n-1}$ and $Q \in E_{m^n+1}$, such that $\pi(P) = \pi(Q)$. By definition of π this implies that $P = \pm Q$.

- If $P = Q$, then $[m^n - 1]P = O_E = [m^n + 1]P$. This implies that $O_E = O_E - O_E = [m^n + 1]P - [m^n - 1]P = [2]P$. So $P \in E_2$.
- If $P = -Q$, then $[m^n - 1]P = O_E = [m^n + 1](-P)$. This implies $O_E = O_E + O_E = [m^n - 1]P + [m^n + 1](-P) = -2[P]$, and hence $P \in E_2$.

Consequently, $\pi(E_{m^n-1}) \cap \pi(E_{m^n+1}) \subset \pi(E_2)$. Moreover, we have

$$\pi(E_{m^n-1}) \cap \pi(E_{m^n+1}) \subset \pi(E_{m^n\pm1}) \cap \pi(E_2).$$

Assume $x \in \pi(E_{m^n\pm1}) \cap \pi(E_2)$, then there exist P, Q such that $\pi(P) = \pi(Q)$ and $P \in E_{m^n\pm1}$ and $Q \in E_2$. From this we find that $Q = -Q$, as it is of order two, and $P = \pm Q$. Together, we get that $P = Q$. Hence, $O_E = O_E \pm O_E = [m^n \pm 1]P \mp 2[P] = [m^n \mp 1]P$. So indeed

$$\pi(E_{m^n+1}) \cap \pi(E_{m^n-1}) = \pi(E_{m^n\pm1}) \cap \pi(E_2).$$

Furthermore, the fact that $P = Q$ implies that $x \in \pi(E_{m^n\pm1} \cap E_2)$. Because all 2-torsion points have exactly one image, we have $|\pi(E_2)| = |E_2|$ and similarly for any subset of E_2.

In particular we find $|\pi(E_{m^n\pm 1} \cap E_2)| = |E_{m^n\pm 1} \cap E_2|$. The claim is proven.
Determining $|\pi(E_{m^n-1})|$ and $|\pi(E_{m^n+1})|$ is completely analogous. Hence, we will write $m^n \pm 1$. We use that all points $P \in E$ have 2 pre-images, except for those $P \in E_2$. Hence, $|\pi(E_{m^n\pm 1})| = \frac{1}{2}|E_{m^n\pm 1}| + \frac{1}{2}|E_2 \cap E_{m^n\pm 1}|$. We can use this in the formula.

$$\begin{aligned}
|\mathrm{Fix}(L_m^{\circ n})| &= |\pi(E_{m^n-1})| + |\pi(E_{m^n+1})| - |\pi(E_{m^n-1}) \cap \pi(E_{m^n+1})| \\
&= \frac{1}{2}|E_{m^n-1}| + \frac{1}{2}|E_2 \cap E_{m^n-1}| + \frac{1}{2}|E_{m^n+1}| + \frac{1}{2}|E_2 \cap E_{m^n+1}| - |\pi(E_{m^n-1} \cap E_2)| \\
&= \frac{1}{2}|E_{m^n-1}| + \frac{1}{2}|E_{m^n+1}|.
\end{aligned}$$

□

Now let K have characteristic zero. To determine the size of the torsion groups we use the following proposition.

Proposition 4.2.9. *Let E be an elliptic curve over a field K and let $m \in \mathbb{Z}$ at least two. Then*

$$E_m(\overline{K}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. See the proof of Corollary III.6.4. in [Sil09]. □

Henceforth, we have $|E_n| = n^2$ and $\mathcal{N}_n = \frac{(m^n-1)^2+(m^n+1)^2}{2} = m^{2n} + 1$. The zeta function can be computed:

$$\begin{aligned}
\zeta_{L_m,\mathbb{P}^1_{K,0}}(T) &= \exp\left(\sum_{n=1}^{\infty} \frac{m^{2n}+1}{n} T^n\right) \\
&= \exp\left(\sum_{n=1}^{\infty} \frac{(m^2T)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n}\right) \qquad (4.2.3.1) \\
&= \frac{1}{(1-m^2T)(1-T)}.
\end{aligned}$$

5

THE DYNAMICAL ZETA FUNCTION IN POSITIVE CHARACTERISTIC

In this chapter we will explore the case where the characteristic of K is positive. The first section is focused on *dynamically affine maps* as introduced in Section 2.2. In particular it centers around the results proved by Andrew Bridy in [Bri12] and later in [Bri16].

The second section involves generalizing this result to abelian varieties, in particular to elliptic curves.

5.1 DYNAMICALLY AFFINE MAPS ON $\mathbb{P}^1_K$

As introduced in Section 2.2 a dynamically affine map involves some underlying algebraic structure. We will prove transcendence of the corresponding dynamical zeta function in the separable case. We first prove a general theorem, which is easily applicable to many cases, and then cover each family in short.

5.1.1 *General theorem for transcendence*

We start by stating the main theorem.

Theorem 5.1.1. *Let p be a prime and $m \in \mathbb{Z} \setminus \{-1, 0, 1\}$ and $b, c, d, e, \varepsilon \in \mathbb{Z}_{\geq 0}$ with $\varepsilon \in \{0, 1\}$ and $A \in \mathbb{Q}^\times$. Define the sequence $(a_n)_{n\geq 1}$ by*

$$a_n := A\left((m^n - 1)^b |m^n - 1|_p^c + \varepsilon(m^n + 1)^d |m^n + 1|_p^e\right).$$

If $p \nmid m$, then the power series $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ is transcendental over $\mathbb{Q}(T)$.
However, if $p \mid m$, then the power series $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ is algebraic over $\mathbb{Q}(T)$. In particular, when $A \in \mathbb{Z}$, it is rational.

To prove this theorem, we need two lemmas and some basic facts on p-adic norms. We start by summarizing all norm related facts in the following proposition.

Proposition 5.1.2. *Let p be a prime number and m an integer coprime to p. With μ_m we denote the set of all mth roots of unity in $\overline{\mathbb{F}_p}$. Then the following hold for all positive integers n.*

1. $|\mu_n| = n \cdot |n|_p$.

2. *Let $p \neq 2$ and let s be the smallest positive integer such that $m^s - 1 \equiv 0 \mod p$.*

$$|m^n - 1|_p = \begin{cases} |m^s - 1|_p \cdot |n|_p & \text{if } s \mid n; \\ 1 & \text{if } s \nmid n. \end{cases}$$

3. *If $p \neq 2$, then*

$$|m^n + 1|_p = \begin{cases} |m^{s/2} + 1|_p \cdot |n|_p & \text{if } \frac{2n}{s} \in 1 + 2\mathbb{Z}; \\ 1 & \text{otherwise.} \end{cases}.$$

4. *If $p \neq 2$ and $\frac{2n}{s} \in 1 + 2\mathbb{Z}$, where s is as before, then*

$$|m^s - 1|_p = |m^{s/2} + 1|_p.$$

5. *If $p = 2$ and m is odd, then*

$$|m^n - 1|_2 = \begin{cases} 2|m-1|_2 \cdot |m+1|_2 \cdot |n|_2 & \text{if } 2 \mid n; \\ |m-1|_2 & \text{if } 2 \nmid n. \end{cases}.$$

6. *If $p = 2$ and m is an odd integer, then*

$$|m^{2n} + 1|_2 = 1/2.$$

Proof. (1.) Write $n = p^k u$, where $k \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}$ such that $p \nmid u$. Then we consider $x \in \mu_n$.

$$x^n = 1 \iff x^{p^k u} - 1 = 0 \iff (x^u)^{p^k} - 1^{p^k} = 0 \iff (x^u - 1)^{p^k} = 0 \iff x^u - 1 = 0.$$

Hence, $\mu_n = \mu_u$. Consider the polynomial $f(x) = x^u - 1$, the derivative is $f'(x) = ux^{u-1}$. Since $f(x)$ and $f'(x)$ have no common zeros, all zeros have multiplicity one. Because $\overline{\mathbb{F}_p}$ is algebraically closed, $f(x)$ has exactly u unique zeros. So $|\mu_n| = |\mu_u| = u = n \cdot |n|_p$.
(2.) Because s is the multiplicative order of m in $\mathbb{F}_p^\times$, if $s \nmid n$ then $m^n \not\equiv 1 \mod p$. Therefore, we find that $|m^n - 1|_p = 1$ if $s \nmid n$. Now consider the case where $s \mid n$. Note that $s \mid p - 1$ which is the order of the multiplicative group. This implies that s and p are coprime. Write $n = sp^k u$, where $k \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}$ such that $p \nmid u$. Also, write $m^s - 1 = ap^i$, where $p \nmid a \in \mathbb{Z}$ and $i \in \mathbb{Z}_{\geq 1}$. Then we have

$$\begin{aligned} m^n - 1 = m^{sp^k u} - 1 &= (ap^i + 1)^{p^k u} - 1 \\ &= -1 + \sum_{j=0}^{p^k u} \binom{p^k u}{j} (ap^i)^j \\ &= \sum_{j=1}^{p^k u} \binom{p^k u}{j} (ap^i)^j \\ &= p^k u \cdot ap^i + \text{higher } p\text{-order terms.} \end{aligned}$$

From this we see that $\text{ord}_p(m^n - 1) = \text{ord}_p(p^k u \cdot ap^i) = i + k = \text{ord}_p(m^s - 1) + \text{ord}_p(n)$. Indeed we find $|m^n - 1|_p = |m^s - 1|_p \cdot |n|_p$.
(3.) Unlike the previous case $m^n \equiv -1 \mod p$ does not necessarily have a solution for n. If it does not, we find $|m^n + 1|_p = 1$ for all n. Assume such a solution exists and define t to be the smallest positive solution to $m^t \equiv -1 \mod p$. Obviously, we have $m^{2t} \equiv 1 \mod p$, hence $s \mid 2t$. Because $p \neq 2$ we have that $s \neq t$. If $s < t$, then $-1 \equiv m^t \equiv m^{t-s}m^s = m^{t-s}$. Since $t - s > 0$ this contradicts the minimality of t. Therefore $s > t$. We know $sk = 2t$ for some $k > 0$ and hence $tk < sk = 2t$, which means $k = 1$. So we see that $s = 2t$. Therefore, if $s/2 \notin \mathbb{Z}$ we have $|m^n + 1|_p = 1$ for all n. Note that $s/2 \notin \mathbb{Z}$ implies $2n/s \notin 1 + 2\mathbb{Z}$. Clearly, this means $|m^n + 1|_p = 1$ if $s/2 \notin \mathbb{Z}$. Now assume $2 \mid s$ and write $t = s/2$. Then $m^n + 1 \equiv 0 \mod p$ implies $s \mid 2n$, so $t \mid n$. Also, if n/t is even, then $m^n \equiv 1 \mod p$. This means that if $2n/s \in 2\mathbb{Z}$, then $|m^n + 1|_p = 1$. If n/t is odd, so $2n/s \in 1 + 2\mathbb{Z}$, then we see $|m^n + 1|_p < 1$. We will now prove the formula given in the proposition. Write $n = tp^\ell v$, where $2, p \nmid v \in \mathbb{Z}$ and $\ell \in \mathbb{Z}_{\geq 0}$, and $m^t + 1 = bp^j$

$$\begin{aligned} m^n + 1 = m^{tp^\ell v} + 1 &= (bp^j - 1)^{p^\ell v} + 1 \\ &= 1 + \sum_{i=0}^{p^\ell v} \binom{p^\ell v}{i} (bp^j)^i \\ &= \sum_{i=1}^{p^\ell v} \binom{p^\ell v}{i} (bp^j)^i \\ &= p^\ell v \cdot bp^j + \text{higher } p\text{-order terms.} \end{aligned}$$

This implies that $\text{ord}_p(m^n + 1) = \text{ord}_p(p^\ell v \cdot bp^j) = \ell + j = \text{ord}_p(m^t + 1) + \text{ord}_p(n)$. This leads us to the formula in the case that $2n/s \in 1 + 2\mathbb{Z}$: $|m^n + 1|_p = |m^{s/2} + 1|_p \cdot |n|_p$.
(4.) Write $m^{s/2} + 1 = p^k u$, where $k > 0$ and $p \nmid u \in \mathbb{Z}$. Then we square $m^{s/2} = p^k u - 1$ and obtain $m^s = p^{2k}u^2 - 2p^k u + 1$. From this we can deduce that $|m^s - 1|_p = |p^k u(p^k u - 2)|_p = |p^k u|_p$, because $p \nmid 2$. Hence, we see that indeed $|m^{s/2} + 1|_p = |m^s - 1|_p$.
(5.) First we write $n = k \cdot 2^\ell$, where $2 \nmid k$ and $\ell \geq 0$. Note that $m^n - 1 = (m^{2^\ell})^k - 1 = (m^{2^\ell} - 1)((m^{2^\ell})^{k-1} + \ldots + m^{2^\ell})$. Because k is odd, we have that $k - 1$ is even. Note that $m^{2^\ell} \equiv 1 \mod 2$ as m is odd and that $m^{2^\ell})^{k-1} + \ldots + m^{2^\ell} \equiv k \cdot 1 \mod 2 = 1 \mod 2$. Hence, $v_2(m^n - 1) = v_2(m^{2^\ell} - 1)$. If $\ell = 0$, and hence $2 \nmid 2$, then this already proves the first case. If $\ell > 0$, that means 2^ℓ is divisible by 2, and as the square of an odd prime is 1 mod 4, we get that $m^{2^\ell} - 1 = (m^{2^{\ell-1}} + 1) \cdot (m^{2^{\ell-2}} + 1) \cdot \ldots \cdot (m^2 + 1)(m + 1)(m - 1)$. As m is odd, we know that $m^{2^i} \equiv 1 \mod 4$ for all $i \geq 1$. Hence, $m^{2^i} + 1 \equiv 2 \mod 4$. We see that each such factor has exactly one factor 2. There are exactly $\ell - 1$ such factors. This yields: $v_2(m^{2^\ell} - 1) = \ell - 1 + v_2(m + 1) + v_2(m - 1)$. If we combine this with the first part, we see that $v_2(m^n - 1) = v_2(n) - 1 + v_2(m + 1) + v_2(m - 1)$. This result is easily translated to the result on norms.
(6.) As m is odd, its square is $1 \mod 4$. Hence, $m^{2n} + 1 \equiv 2 \mod 4$. Hence, $|m^{2n} + 1|_2 = 2^{-1}$. □

Now we give the lemma which incorporates all automata theory related notions.

Lemma 5.1.3. *Let p be a prime and $m, b, c, d, e, \varepsilon \in \mathbb{Z}_{\geq 0}$ with m coprime to p, $c \neq 0$ and $\varepsilon \in \{0,1\}$. If $p = 2$, assume moreover that $\operatorname{rad}(m) \nmid \operatorname{rad}(2^c - 1)$. Define the sequence $(a_n)_{n\geq 1}$ by*

$$a_n := (m^n - 1)^b |m^n - 1|_p^c + \varepsilon (m^n + 1)^d |m^n + 1|_p^e.$$

Then there exists a prime q such that $(a_n \mod q)_{n\geq 1}$ is not q-automatic.

Proof. First for $p \neq 2$. Choose a prime q such that $q \equiv -1 \mod p$ and $q > \max\{m, (m^{p-1} - 1)^b, p^c\}$. By Dirichlet's theorem on primes (Theorem 13.2 in [Neu92]), such a prime must exist. Now q is fixed. Assume the sequence $(a_n \mod q)_{n\geq 1}$ is q-automatic. The subsequence $a_{(p-1)((q-1)n+1)} \mod q$ is q-automatic by Proposition 3.2.5. We obtain the sequence defined by

$$\begin{aligned} b_n &:= (m^{(p-1)((q-1)n+1)} - 1)^b |m^{(p-1)((q-1)n+1)} - 1|_p^c \\ &\quad + \varepsilon (m^{(p-1)((q-1)n+1)} + 1)^d |m^{(p-1)((q-1)n+1)} + 1|_p^e \mod q. \end{aligned}$$

Obviously, as $q > m$, we know that $m \not\equiv 0 \mod q$ and hence m is invertible. Moreover, $m^{q-1} \equiv 1$. Hence, we get

$$b_n = (m^{p-1} - 1)^b |m^{(p-1)((q-1)n+1)} - 1|_p^c + \varepsilon (m^{p-1)} + 1)^d |m^{(p-1)((q-1)n+1)} + 1|_p^e \mod q.$$

Also, as m is coprime to p, we know that $m^{p-1} \equiv 1 \mod p$, and hence $|m^{(p-1)((q-1)n+1)} + 1|_p^e = 1$. We get

$$b_n = (m^{p-1} - 1)^b |m^{(p-1)((q-1)n+1)} - 1|_p^c + \varepsilon (m^{p-1} + 1)^d \mod q.$$

Because $\varepsilon (m^{p-1} + 1)^d$ is just a constant (possibly zero), subtracting this is a unary operation, hence by Proposition 3.2.7 the sequence $c_n := (m^{p-1} - 1)^b |m^{(p-1)((q-1)n+1)} - 1|_p^c \mod q$ is q-automatic. Now let us write $c_n := (m^{p-1} - 1)^b p^{-cv_p(m^{(p-1)((q-1)n+1)} - 1)} \mod q$. By our choice of q we have that $q > (m^{p-1} - 1)^b$, and in particular we get that $(m^{p-1} - 1)^b$ is invertible modulo q. Hence, we can multiply $(c_n)_{n\geq 1}$ by the inverse of this constant, which is a unary operation, and then invert every element, and then by Proposition 3.2.7 the sequence $d_n := p^{cv_p(m^{(p-1)((q-1)n+1)} - 1)} \mod q$ is also q-automatic, note that as $q \neq p$ we can just invert p in $\mathbb{F}_q$. We use Proposition 5.1.2(2) to see that $v_p(m^{(p-1)((q-1)n+1)} - 1) = v_p(m^{p-1} - 1) + v_p((q-1)n + 1)$. We get that $d_n := p^{cv_p(m^{p-1} - 1)} p^{cv_p((q-1)n+1)} \mod q$. However, we know that $p^c \in \mathbb{Z}$ and $p^c \not\equiv 0, 1 \mod q$ and $v_p(q-1) = 0$ as $q \equiv -1 \not\equiv 1 \mod p$ as $p \neq 2$. Note that $v_p(q-1) = 0 \geq v_p(1)$, hence we can use Proposition 3.2.9 to conclude that $(d_n)_{n\geq 1}$ is not q-automatic. We found a contradiction.

Now let $p = 2$. Then consider q prime such that $q \mid m$ and $q \nmid 2^c - 1$, such a prime must exist by the assumption that $\operatorname{rad}(m) \nmid \operatorname{rad}(2^c - 1)$. Note that $q \mid m$ implies that $q \neq 2$. Let us fix this q. Again assume that $(a_n)_{n\geq 1} \mod q$ is q-automatic. Then the subsequence $a_{2n} \mod q$ is also q-automatic. We get

$$\begin{aligned} b_n &:= (m^{2n}-1)^b|m^{2n}-1|_2^c + \varepsilon(m^{2n}+1)^d|m^{2n}+1|_2^e \mod q \\ &= (m^{2n}-1)^b 2^{-cv_2(m^{2n}-1)} + \varepsilon(m^{2n}+1)^d 2^{-e} \mod q \\ &= (-1)^b 2^{-cv_2(m^{2n}-1)} + \varepsilon 2^{-e} \mod q \end{aligned}$$

We can subtract the (possibly zero) constant $\varepsilon 2^{-e}$, which is a unary operation, hence by Proposition 3.2.7 the sequence $c_n := (-1)^b 2^{-cv_2(m^{2n}-1)} \mod q$ is also q-automatic. Clearly, we have that $(-1)^b$ is invertible in $\mathbb{F}_q$. We can construct another sequence by multiplying with its inverse and taking the inverse of each element in the sequence. We get $d_n = 2^{cv_2(m^{2n}-1)} \mod q$, which is also q-automatic by Proposition 3.2.7. Now use Proposition 5.1.2(5) to obtain $d_n = 2^{c(v_2(m-1)+v_2(m+1))}2^{cv_2(n)} \mod q$. As $q \neq 2$, we know that $2^{c(v_2(m-1)+v_2(m+1))}$ is invertible in $\mathbb{F}_q$. Hence, we can multiply the sequence with its inverse to obtain another q-automatic sequence by Proposition 3.2.7, namely: $e_n := 2^{cv_2(n)} \mod q$. We assumed that $q \nmid 2^c - 1$. Hence, $2^c \neq 0, 1 \mod q$. Now by Proposition 3.2.9 this sequence is not q-automatic. We have a contradiction. □

The second lemma tells us the connection between the dynamical zeta function and the automata theory.

Lemma 5.1.4. *If* $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ *is algebraic over* $\mathbb{Q}(T)$*, where* $a_n \in \mathbb{Z}$ *for all* $n \geq 1$*. Then* $(a_n \mod q)_{n\geq 1}$ *is a* q*-automatic sequence for any prime* q*.*

Proof. By assumption $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ is algebraic over $\mathbb{Q}(T)$.

Write $F(T) := \exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$. So let $P(x) \in \mathbb{Q}(T)[x]$ be such that $P(F(T)) = 0$. Then we can write $P(x,T) = \sum_{i=0}^n p_i(T)x^i$ for some $n \in \mathbb{N}$ and $p_i(T) \in \mathbb{Q}(T)$.

$$\begin{aligned} \frac{d(P(F(T)))}{dT} = 0 &\iff \sum_{i=0}^n \frac{d(p_i(T)(F(T))^i)}{dT} = 0 \\ &\iff \sum_{i=0}^n \frac{dp_i(T)}{dT}(F(T))^i + p_i(T)\frac{d(F(T)^i)}{dT} = 0 \\ &\iff \sum_{i=0}^n p_i'(T)(F(T))^i + \sum_{i=0}^n p_i(T)iF'(T)(F(T))^{i-1} = 0 \\ &\iff \sum_{i=0}^n p_i'(T)(F(T))^i = -\left(\sum_{i=0}^n p_i(T)i(F(T))^{i-1}\right)F'(T) \\ &\iff F'(T) = \frac{-\sum_{i=0}^n p_i'(T)(F(T))^i}{\sum_{i=0}^n p_i(T)i(F(T))^{i-1}}. \end{aligned}$$

Because $p_i(T) \in \mathbb{Q}(T)$, that means $p_i'(T) \in \mathbb{Q}(T)$. Moreover, as $F(T)$ is algebraic, we know that $-\sum_{i=0}^n p_i'(T)(F(T))^i$ and $\sum_{i=0}^n p_i(T)i(F(T))^{i-1}$ are algebraic. The quotient of algebraic elements is algebraic (algebraic elements form a field), hence $F'(T)$ is algebraic over $\mathbb{Q}(T)$. Observe the following

$$F'(T) = \frac{d\left(\exp\left(\sum_{k=1} \frac{a_k}{k} T^k\right)\right)}{dT} = \frac{d\left(\sum_{k=1} \frac{a_k}{k} T^k\right)}{dT} \cdot \exp\left(\sum_{k=1} \frac{a_k}{k} T^k\right)$$
$$= \sum_{k=1} \frac{a_k}{k} \frac{d(T^k)}{dT} \cdot F(T) = \sum_{k=1} a_k T^{k-1} \cdot F(T).$$

We can see that $\sum_{k=1} a_k T^{k-1} = F'(T)/F(T)$, which is algebraic, as it is the quotient of algebraic elements. Note that $a_n \in \mathbb{Z}$ for all $n \geq 1$, hence $\sum_{k=0}^{\infty} a_{k+1} T^k \in \mathbb{Z}[\![T]\!]$. Apply Corollary 3.2.2 to conclude that $(a_k)_{\geq 1}$ is a q-automatic sequence for all primes q. □

These two lemmas already represent the main ingredients of the proof of Theorem 5.1.1, and hence the proof follows easily:

Proof of Theorem 5.1.1. First let $p \nmid m$. Assume by contradiction that $\exp\left(\sum_{n\geq 1} \frac{a_n}{n} T^n\right)$ is algebraic over $\mathbb{Q}(T)$. Define $b_n := A^{-1} a_n$, which is defined over $\mathbb{Z}$ for all n. Hence, we see that

$$\exp\left(\sum_{n\geq 1} \frac{A^{-1} b_n}{n} T^n\right) = \left(\exp\left(\sum_{n\geq 1} \frac{b_n}{n} T^n\right)\right)^{A^{-1}}$$

is algebraic over $\mathbb{Q}(T)$. Taking a rational power A of an algebraic function preserves being algebraic over $\mathbb{Q}(T)$. Therefore, we know that $\exp\left(\sum_{n\geq 1} \frac{b_n}{n} T^n\right)$ must be algebraic over $\mathbb{Q}(T)$. Then we use Lemma. 5.1.4 to see that $(b_n \mod q)_{n\geq 1}$ is q-automatic for any prime q. In our case that means that $b_n = (m^n - 1)^b |m^n - 1|_p^c + \varepsilon(m^n + 1)^d |m^n + 1|_p^e \mod q$ is q-automatic for any prime q. However, this is in contradiction with Lemma 5.1.3.
Now let $p \mid m$. Then $a_n = A(m^n - 1)^b + \epsilon(m^n + 1)^d$. This can be rewritten using the binomial identity to some polynomial in m^n with integral coefficients times A: $a_n = A(b_k(m^n)^k + \ldots + b_0)$. We use this in our computation of the dynamical zeta function.

$$\sum_{n=1}^{\infty} \frac{A(b_k(m^n)^k + \ldots + b_0)}{n} T^n = A\left(\sum_{n=1}^{\infty} \frac{b_k(m^{nk}}{n} T^n + \ldots + \sum_{n=1}^{\infty} \frac{b_0}{n} T^n\right)$$
$$= A\left(\sum_{n=1}^{\infty} \frac{b_k((m^k T)^n}{n} + \ldots + \sum_{n=1}^{\infty} \frac{b_0 T^n}{n}\right)$$
$$= A\left(b_k \log\left(\frac{1}{1 - m^k T}\right) + \ldots + b_0 \log\left(\frac{1}{1-T}\right)\right)$$

We take the exp:

$$\exp\left(\sum_{n=1}^{\infty} \frac{a_n}{n} T^n\right) = \left(\prod_{i=1}^{k} \left(\frac{1}{1 - m^i T}\right)^{b_i}\right)^A.$$

This is a finite product of rational functions to a fractional power, hence the formal power series are in fact algebraic. When $A \in \mathbb{Z}$, it is clearly rational. □

5.1.2 *Power maps*

To compute the zeta function for power maps we do something similar to Subsection 4.2.1. Let $f(x) = x^m$ for some $m \in \mathbb{Z}_{\geq 1}$. Again we will study this map on $\mathbb{G}_{m,p}$, the multiplicative group of the field $\overline{\mathbb{F}}_p$. The n-fold composition is $f^{\circ n}(x) = x^{m^n}$. Similarly to before we need to solve $x^{m^n} = x$ for $x \in \mathbb{G}_{m,p}$. This is equivalent to solving $x^{m^n-1} = 1$ for $x \in \mathbb{G}_{m,p}$. Again we can conclude that $\text{Fix}(f^{\circ n}) = \mu_{m^n-1}$. Using Proposition 5.1.2(1), we obtain the following.

$$\mathcal{N}_n = (m^n - 1) \cdot |m^n - 1|_p$$

If $p \mid m$, then $\mathcal{N}_n = m^n - 1$ for all $n \geq 1$. Hence, we get exactly the same result as in Subsection 4.2.1: $\zeta_{f,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{1-T}{1-mT}$.
If $p \nmid m$, then we can clearly see that this formula fits into the requirements ($A = 1$, $b = 1$, $c = 1$, $d = 0$, $e = 0$, $\varepsilon = 0$) of Theorem 5.1.1 and hence the zeta function becomes transcendental over $\mathbb{Q}(T)$.

5.1.3 *Chebyshev polynomials*

Using Proposition 4.2.6, we know that: $|\text{Fix}(T_d^{\circ n})| = \frac{|\mu_{d^n+1}|+|\mu_{d^n-1}|}{2}$. Here we can use the formula from Proposition 5.1.2(1), so $|\mu_k| = k \cdot |k|_p$, where $|k|_p$ can be found using Proposition 5.1.2(2,3). We denote the additive group of $\overline{\mathbb{F}}_p$ be $\mathbb{G}_{a,p}$. We get

$$\mathcal{N}_n = \frac{(d^n+1)|d^n+1|_p + (d^n-1)|d^n-1|_p}{2}.$$

If $p \mid m$, then $\mathcal{N}_n = \frac{(d^n+1)}{2} + \frac{(d^n-1)}{2} = d^n$ for all $n \geq 1$. Therefore, we get the same result as in Subsection 4.2.2: $\zeta_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T)\frac{1}{1-dT}$.
If $p \nmid m$, then we can again use Theorem 5.1.1 with ($A = 1/2$, $b = 1$, $c = 1$, $d = 1$, $e = 1$, $\varepsilon = 1$) to see that the zeta function becomes transcendental over $\mathbb{Q}(T)$.

5.1.4 *Lattès maps*

We start our computation using the result from Proposition 4.2.8: $|\text{Fix}(L_m^{\circ n})| = \frac{|E_{m^n-1}|+|E_{m^n+1}|}{2}$. Now we need to determine $|E_N|$ for a general N. Let us write $N = p^k \cdot u$, where $p \nmid u \in \mathbb{Z}$. Because E_N is an abelian torsion group it is the direct product of its coprime torsion groups. In particular, the fact that p^k and u are coprime implies $E_N \simeq E_{p^k} \times E_u$. Because u is coprime to p we know that $|E_u| = u^2$ (Corollary III.6.4.(b) in [Sil09]). The other factor depends on whether E is supersingular ($h = 2$) or ordinary ($h = 1$). Namely, $E_{p^k} \simeq \{0\}$ when E is supersingular, and $E_{p^k} \simeq \mathbb{Z}/p^k\mathbb{Z}$ when E is ordinary (Theorem V.3.1.(v,b) in [Sil09]). We obtain $|E_N| = u^2$ when E is supersingular and $|E_N| = u^2p^k$ when E is ordinary. We can write this in a general formula: $|E_N| = N^2 \cdot |N|_p^h$. We can use this formula for both $N = m^n + 1$ and $N = m^n - 1$. We can assemble the formula:

$$\begin{aligned}|\mathrm{Fix}(L_m^{\circ n})| &= \frac{1}{2}|E_{m^n-1}| + \frac{1}{2}|E_{m^n+1}| \\ &= \frac{1}{2}(m^n-1)^2|m^n-1|_p^h + \frac{1}{2}(m^n+1)^2|m^n+1|_p^h.\end{aligned}$$

If $p \mid m$, then $\mathcal{N}_n = \frac{(m^n-1)^2+(m^n-1)^2}{2} = m^{2n}+1$. The zeta function is again equal to the one we find in Subsection 4.2.3:

$$\zeta_{L_m,\mathbb{P}^1_{\mathbb{F}_p}}(T) = \frac{1}{(1-m^2T)(1-T)}.$$

If $p \nmid m$, we use Theorem 5.1.1 with ($A = 1/2$, $b = 2$, $c = h$, $d = 2$, $e = h$, $\varepsilon = 1$) to again conclude that the zeta function is transcendental over $\mathbb{Q}(T)$.

5.1.5 *Additive and subadditive polynomials*

We start with two definitions.

Definition 5.1.5. Let k be a field. A polynomial $f(x) \in k[x]$ is called **additive** over $\mathbb{G}_a$ if $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{G}_a$.

And the other family of polynomials.

Definition 5.1.6. Let k be a field. A polynomial $f(x) \in k[x]$ is called **subadditive** over $\mathbb{G}_a$ if $f(\omega_d x) = \omega_d f(x)$ for a d-th root of unity, such that $\mathrm{char}(k) \nmid d$.

Unlike the previous three families, these families do not contain any non-trivial examples over fields of characteristic zero. Moreover, these two families can be handled as one. We can just consider the endomorphism ring of $\mathbb{G}_a$. We know that this contains all multiplications $x \mapsto cx$, and also the Frobenius map. We get $\mathrm{End}(\mathbb{G}_a) \simeq \overline{k}\langle\phi\rangle$, where ϕ is the Frobenius, so $\phi c = c^p \phi$ for $c \in \overline{k}$. These results can be found in [Wat79] on p. 65. As we work in the algebraic closure of k, the Frobenius is not commutative, and hence the endomorphism algebra is not commutative. The Frobenius and its n-fold compositions are the only purely inseparable maps on $\mathbb{G}_a$. The inseparable degree of a map f is thus the number of times it contains the Frobenius. Let $f \in \mathrm{End}(\mathbb{G}_a)$, then $\#\ker(f) = \deg_s(f) = \deg(f) \cdot p^{-v_\phi(f)}$. Let f be a (sub)additive polynomial of degree $d \geq 2$ on $\mathbb{G}_a$. As it is a polynomial, we have $\deg(f^{\circ n}) = \deg(f)^n$. Moreover, subtracting the identity ($x \mapsto 1x$, so represented by 1 in $k\langle\phi\rangle$) does not impact the degree, as $d > 1$.

$$|\mathrm{Fix}(f^{\circ n})| = \#\ker(f^{\circ n} - 1) = \deg(f^{\circ n} - 1)p^{v_\phi(f^{\circ n}-1)} = d^n p^{v_\phi(f^{\circ n}-1)}.$$

If $f \in k\langle\phi\rangle$, then surely $v_\phi(f^{\circ n} - 1) = 0$. Hence, we get $\mathcal{N}_n = d^n$. So it is easy to see that we get $\zeta_{f,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \frac{1}{1-dT}$. If $f \notin k\langle\phi\rangle$. Then there is an s, such that $f^s - 1 \in \phi k\langle\phi\rangle$ (the multiplicative order in the residue field, so s is coprime to p). We need a lemma to rewrite the formula into the proper form.

Lemma 5.1.7 (Lemma 6.3. in [Bri16]). *Let k be an algebraically closed field of characteristic p, and let $k\langle\phi\rangle$ be the noncommutative polynomial ring, with multiplication rule $\phi c = c^p\phi$. Let $x \in k\langle\phi\rangle$ be such that $x - 1 \in \phi k\langle\phi\rangle$. Then*

$$v_\phi(x^n - 1) = v_\phi(x-1)p^{v_p(n)}.$$

Proof. First we assume $v_p(n) = 0$. In that case we get

$$x^n - 1 = (1 + (x-1))^n - 1 = \sum_{i=0}^{n} \binom{n}{i}(x-1)^i - 1 \equiv \binom{n}{1}(x-1) \mod \phi^2 k\langle\phi\rangle.$$

As $v_p(n) = 0$, we also have that $v_\phi(n) = 0$. Therefore, we get $v_\phi(x^n - 1) = v_\phi(x-1)p^0$. This allows us to reduce to the case where $n = p^k$, as we can take out all coprime factors. We will prove this for $k \geq 1$. So let $n = p^k$. Then $x^{p^k} - 1 = (x-1)^{p^k}$ because the characteristic is p (generalized high school student's dream). It is clear that we get $v_\phi((x-1)^{p^k}) = p^k v_\phi(x-1)$. □

We then get $\mathcal{N}_{sn} = d^{sn} p^{v_\phi(f^s-1)p^{v_p(n)}}$. Unfortunately, this does not match the form of Theorem 5.1.1. We can still use Lemma 5.1.4 to see that $\mathcal{N}_n \mod q$ is q-automatic for all primes q. Hence, the subsequence $\mathcal{N}_{s(q-1)n} \mod q$ is also q-automatic by Proposition 3.2.5. Moreover, we assume $q \not\equiv 1 \mod p$ if p is odd, and $q \equiv 7 \mod 8$ if $p = 2$. By Dirichlet's theorem (Theorem 13.2 in [Neu92]) there are still an infinite number of such primes q. For q sufficiently large we obtain another q-automatic sequence.

$$\begin{aligned} b_n &= d^{s(q-1)n} p^{v_\phi(f^s-1)p^{v_p(n(q-1))}} \mod q \\ &= 1 p^{v_\phi(f^s-1)p^{v_p(n)}p^{v_p(q-1)}} \mod q \\ &= p^{(v_\phi(f^s-1)p^{v_p(q-1)})p^{v_p(n)}} \mod q \end{aligned}$$

So we demand $q > d$. Now define $a := v_\phi(f^s - 1)p^{v_p(q-1)}$ and assume $q > p^{ap^a}$. By Proposition 3.2.10 this sequence is not q-automatic. This is a contradiction, hence the zeta function $\zeta_{f,\mathbb{G}_{a,\mathbb{F}_p}}(T)$ is transcendental over $\mathbb{Q}(T)$.

5.2 ABELIAN VARIETIES

We want to use the structure of proofs we saw in the previous section and apply them to different maps on different varieties, namely on isogenies on abelian varieties. We will provide a short introduction to abelian varieties following [MvdG].

Definition 5.2.1. A **group variety** over a field K is a K-variety X together with K-morphisms $m : X \times X \to X$ (group law), $i : X \to X$ (inverse) and a K-rational point $e \in X(K)$ (identity element), such that

i. $m \circ (m \times \mathrm{id}_X) = m \circ (\mathrm{id}_X \times m) : X \times X \times X \to X$;

ii. $m \circ (e \times \mathrm{id}_X) = j_1 : X \times \mathrm{Spec}(K) \times X \to X$ and $m \circ (\mathrm{id}_X \times e) = j_2 : X \times \mathrm{Spec}(K) \to X$, where $j_1 : \mathrm{Spec}(k) \times X \xrightarrow{\sim} X$ and $j_2 : X \times \mathrm{Spec}(K) \xrightarrow{\sim} X$ are the canonical isomorphisms;

iii. $e \circ \pi = m \circ (\mathrm{id}_X \times i) \circ \Delta_{X/K} = m \circ (i \times \mathrm{id}_X) \circ \Delta_{X/K} : X \to X$, where $\pi : X \to \mathrm{Spec}(K)$ is the structure morphism.

If X is a group variety, then the set $X(K)$ of K-rational points naturally inherits the structure of a group. As a variety (or morphism or point) over K is a variety (or morphism or point) over $\overline{K}$ as well, we see that $X(\overline{K})$ is a group is as well, this is very relevant to us, as we are interested in this group structure. We continue with abelian varieties:

Definition 5.2.2. An **abelian variety** is a group variety which, as a variety, is complete.

A famous example of an abelian variety is an elliptic curve. It turns out that demanding completeness makes abelian varieties into a very special class of varieties, most notable its group structure is very useful. Let us now show that the name is well chosen:

Proposition 5.2.3. *Let X be an abelian variety over a field K, then $X(\overline{K})$ has an abelian group structure.*

Proof. See the proof of Corollary 1.14(ii) in [MvdG]. □

Definition 5.2.4. Let $f : X \to Y$ be a homomorphism of abelian varieties. Then f is called an **isogeny** if f is surjective and $\dim(X) = \dim(Y)$.

So clearly, all isogenies $f : X \to X$ are endomorphisms. An endomorphism which is not an isogeny is not surjective. A group homomorphism f that is not surjective must have a proper subgroup as its image. However, we only consider maps of degree at least two, and hence all generic points need to have a pre-image. Therefore, the set of all endomorphisms of degree at least two is the same as the set of all isogenies of degree at least two.

Definition 5.2.5. Let $f : A \to B$ be an isogeny of abelian varieties over k.

- the **degree** of f is the degree of function field extensions $[k(A) : f^*k(B)]$;
- the **separable degree** of f is the separable degree of the function field extensions $[k(A) : f^*k(B)]_s$;
- the **inseparable degree** of f is the inseparable degree of the function field extensions $[k(A) : f^*k(B)]_i$.

It turns out that these notions are very useful to gain a better understanding of how to approach our generalization for abelian varieties.

Lemma 5.2.6. *Let $f : A \to A$ be an endomorphism of degree at least 2. Then the order of the kernel equals the separable degree* $\deg_s(f)$.

Proof. This result can be found in [Shi98] on p. 4. □

5.2.1 *Multiplication-by-m maps on abelian varieties*

We can generalize the results of the previous section to abelian varieties for the familiar multiplication-by-m map:

Theorem 5.2.7. *Let A be an abelian variety over a field K of characteristic $p > 0$, and let $[m] : A \to A$ be the multiplication-by-m map, with $|m| > 1$. If $p \nmid m$, then $\zeta_{[m],A}(T)$ is transcendental over $\mathbb{Q}(T)$. However, if $p \mid m$, then $\zeta_{[m],A}(T)$ is rational over $\mathbb{Q}(T)$.*

To prove this we need an expression for the number of fixed points. We first introduce a new notion and then give a useful lemma.

Definition 5.2.8. Let A be an abelian variety of dimension g over K, a field of characteristic $p > 0$. Then the p**-rank** of A is

$$r := v_p(|A[p](\overline{K})|).$$

Lemma 5.2.9. *Let A be an abelian variety of dimension g over a field K of characteristic $p > 0$, and let $[m] : A \to A$ be the multiplication-by-m map, defined by $P \mapsto \sum_{i=1}^{m} P$, with $m \in \mathbb{Z}$, not divisible by p. Then $\#\ker([m]) = m^{2g} p^{(r-2g)v_p(m)}$, where r is the p-rank of A.*

Proof. Write $m = p^k \cdot u$, with $k \in \mathbb{Z}_{\geq 0}$ and $u \in \mathbb{Z}$, such that $p \nmid u$. This means $[m] = [p^k][u]$. As the separable degree is multiplicative (follows from a tower of field extensions), we find $\deg_s([m]) = \deg_s([p^k]) \cdot \deg_s([u])$. Because $p \nmid u$, the map $[u]$ is separable (Proposition 5.9. in [MvdG]), therefore $\deg_s([u]) = \deg(u) = u^{2g}$ (Proposition 2.9. in [MvdG]). We are left with $\deg_s([p^k])$. Define r to be the p-rank of A. As $\ker(p^k) \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$ (Proposition 5.22. in [MvdG]), we know that $\deg_s([p^k]) = p^{kr}$. We get:

$$\deg_s([m]) = u^{2g} p^{kr} = m^{2g} p^{(r-2g)v_p(m)}.$$

□

We can now prove the theorem with this lemma.

Proof of Theorem 5.2.7. By Lemma 5.2.6 we know that $\#\mathrm{Fix}([\ell]) = \deg_s([\ell m])$. We can also apply Lemma 5.2.9 and see that $\#\mathrm{Fix}([\ell]) = \ell^{2g} p^{(r-2g)v_p(\ell)}$. When we take $\ell = m^n - 1$, we see that

$$\mathcal{N}_n = (m^n - 1)^{2g} p^{(r-2g)v_p(m^n-1)}.$$

Then we can apply 5.1.1 to this for $(A = 1, b = 2g, c = r - 2g, \epsilon = 0, d = 1, e = 1)$ and obtain that $\zeta_{[m],A}(T)$ is transcendental over $\mathbb{Q}(T)$, when $p \nmid m$ and it is rational if $p \mid m$. □

5.2.2 *Endomorphisms on elliptic curves*

We wish to generalize our results to a wider range of endomorphisms on abelian varieties. We will present several lemmas which correspond to steps or lemmas of Theorem 5.1.1. It turns out that we can apply this theory to elliptic curves.

Lemma 5.2.10. *Let $\alpha : A \to A$ be an endomorphism of degree at least 2. Then the vector space generated by α and all its kth compositions $\alpha^{\circ k}$ denoted $\mathbb{Q}(\alpha)$ is a $\mathbb{Q}$-subalgebra, and $\mathbb{Q}(\alpha)$ is a finite field extension of $\mathbb{Q}$. Moreover, we have that $\deg(\beta) = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta)^{2g/d}$, for all $\beta \in \mathbb{Q}(\alpha)$, where $g = \dim(A)$ and d is the degree of the field extension $\mathbb{Q}(\alpha)/\mathbb{Q}$.*

Proof. It is clear that $1 \in \mathbb{Q} \subset \mathbb{Q}(\alpha)$ and by definition we generate it as a vector space. Any isogeny has a characteristic polynomial of degree $2g$. When we fill in the isogeny itself, the polynomial is zero. This can be found in [Shi98] on p. 4,5. Moreover, the polynomial is defined over $\mathbb{Z}$, hence α can be considered an algebraic element over $\mathbb{Q}$. That means $\mathbb{Q}(\alpha)$ can be seen as a field extension of $\mathbb{Q}$ of finite degree.

As $K = \mathbb{Q}(\alpha)$ is a $\mathbb{Q}$-subalgebra of $\mathrm{End}^0(A)$, and it is a field. We can use that $\deg(\beta) = \mathrm{Nm}_{K/\mathbb{Q}}(\beta)^{2g/d}$, where d is the degree of the field extension, so $d = [K : \mathbb{Q}]$, and $g = \dim(A)$. The proof of this claim can be found in [Mil08] as the proof of Proposition 10.23. □

Lemma 5.2.11. *Let $K := \mathbb{Q}(\alpha)$ be a finite separable extension of $\mathbb{Q}$, and L its normal closure. If $\alpha \in \mathcal{O}_K$, then there exists an integer $N \in \mathbb{Z}$ such that for each prime $q > N$ the sequence $(a_n)_{n\geq 1}$ defined by $a_n := N_{K/\mathbb{Q}}(\alpha^n - 1) \mod q$ is periodic of (not necessarily exact) period $q^f - 1$, where f is the inertia degree of the prime ideals above q in $\mathcal{O}_L$.*

Proof. Let $\sigma_1, \ldots, \sigma_k$ be the distinct $\mathbb{Q}$-embeddings of K into a normal closure L of K. Then the norm for $x \in K$ becomes

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{k} \sigma_i(x).$$

We are interested in the norm of $\alpha^n - 1$. We get the following:

$$N_{K/\mathbb{Q}}(\alpha^n - 1) = \prod_{i=1}^{k} \sigma_i(\alpha^n - 1) = \prod_{i=1}^{k} (\sigma_i(\alpha)^n - 1).$$

We know that $\sigma_i(\alpha) \in L$ for all σ_i. Moreover, as the set $\{\sigma_i(\alpha)\}_i$ is finite, we know there are only finitely many prime ideals $\mathfrak{q}$ in $\mathcal{O}_L$ such that $\sigma_i(\alpha) \in \mathfrak{q}$ for some i. Hence, there are only a finite number of primes $q \in \mathbb{Z}$ such that $\sigma_i(\alpha) \in \mathfrak{q}$ for some $\mathfrak{q} \mid q\mathcal{O}_L$. Hence, there exists an $N \in \mathbb{Z}$, such that for every prime number $q > N$ we have that $\sigma_i(\alpha) \notin \mathfrak{q}$ for every prime ideal $\mathfrak{q} \mid q\mathcal{O}_L$.

Note that over the number field L there are only finitely many primes that ramify. Hence, there exists an $M \in \mathbb{Z}_{\geq N}$ such that for every prime $q > M$ the prime q does not ramify over L. For any $q > M$ there is a factorization $q\mathcal{O}_L = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_\ell$, where $\mathfrak{q}_j \neq \mathfrak{q}_k$ for $j \neq k$ and each ideal $\mathfrak{q}_j$ is maximal. For each maximal ideal $\mathfrak{q}_j$ we know that $\mathcal{O}_L/\mathfrak{q}_j$ is a field and moreover it is a finite extension of $\mathbb{F}_q$ of degree f_j, the inertia degree. Note that $L/\mathbb{Q}$ is a Galois extension as it is a normal extension of a separable extension. Because we have a Galois extension we get $f_j = f$ for all $1 \leq j \leq \ell$ with $ef\ell = d'$, where e is the ramification degree ($e = 1$ in our case), ℓ the number of distinct prime ideals and lastly: $d' = [L : \mathbb{Q}]$, which is finite as the normal closure of an algebraic extension is also of finite degree.

Let us remark that $\#\mathcal{O}_L/\mathfrak{q}_i = q^f$, as it is a field extension of $\mathbb{F}_q$ of degree f. Note that we choose $q > M > N$, hence $\sigma_i(\alpha) \notin \mathfrak{q}_j$ for all $1 \leq j \leq \ell$ and $1 \leq i \leq k$. This means that $\sigma_i(\sigma)^{q^f-1} \equiv 1 \mod \mathfrak{q}_j$ as this is just the order of the multiplicative group. Note that we get

$\sigma_i(\alpha)^{q^f-1+a} \equiv \sigma_i(\alpha)^a \mod \mathfrak{q}_j$ for each $1 \leq j \leq \ell$, $1 \leq i \leq k$ and all $a \in \mathbb{Z}$. This also implies the following for all $1 \leq j \leq \ell$ and all $a \in \mathbb{Z}$.

$$\begin{aligned}\prod_{i=1}^{k}(\sigma_i(\alpha)^{q^f-1+a}-1) &\equiv \prod_{i=1}^{k}(\sigma_i(\alpha)^{q^f-1}\sigma_i(\alpha)^a-1) \mod \mathfrak{q}_j\\ &\equiv \prod_{i=1}^{k}(\sigma_i(\alpha)^a-1) \mod \mathfrak{q}_j.\end{aligned}$$

Note that as all $\mathfrak{q}_j$ are maximal they must be pairwise coprime. Hence, we can use the Chinese remainder theorem on the product $q\mathcal{O}_L = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_\ell$ to obtain that

$$\prod_{i=1}^{k}(\sigma_i(\alpha)^{q^f-1+a}-1) \equiv \prod_{i=1}^{k}(\sigma_i(\alpha)^a-1) \mod q\mathcal{O}_L.$$

We know that $\prod_{i=1}^{k}(\sigma_i(\alpha)^{q^f-1+a}-1) = N_{K/\mathbb{Q}}(\alpha^{q^f-1+a}-1)$ and $\prod_{i=1}^{k}(\sigma_i(\alpha)-1) = N_{K/\mathbb{Q}}(\alpha-1)$ for all $a \in \mathbb{Z}_{\geq 1}$. By assumption $\alpha \in \mathcal{O}_K$, hence $\alpha^{q^f-1+a}-1 \in \mathcal{O}_K$ and $\alpha - 1 \in \mathcal{O}_K$ for all $a \geq 1$. Because integral elements have integral norm (Corollary 2.21 in [Mil17]), we see that our identity must hold in $\mathbb{Z}$:

$$N_{K/\mathbb{Q}}(\alpha^{q^f-1+a}-1) \equiv N_{K/\mathbb{Q}}(\alpha^a-1) \mod q.$$

We clearly see that the sequence $(a_n)_{n\geq 1}$ with $a_n := N_{K/\mathbb{Q}}(\alpha^n-1) \mod q$ is periodic of (not necessarily exact) period q^f-1. □

Lemma 5.2.12. *Let A be an abelian variety over a field of characteristic p of dimension g, and $\alpha : A \to A$ a separable self-map. Assume one of the following conditions holds:*

1. $p-1 > 2g!$;
2. $p-1 > [\mathbb{Q}(\alpha) : \mathbb{Q}]!$.

Then there exist an infinite number of primes q such that $q^f - 1 \not\equiv 0 \mod p$, where f is the inertia degree of q in the normal closure of $\mathbb{Q}(\alpha)$.

Proof. We will prove that there exist and infinite number of primes q that split completely, so its inertia degree $f = 1$ and are not congruent to $1 \mod p$. It is clear that, then $q^f - 1 \not\equiv 0 \mod p$. We first prove it for assumption 2.

Denote the density of a subset A of all primes by $\delta(A)$. By Dirichlet's theorem on the density of primes (Theorem 13.2 in [Neu92]), we know that the density of primes of the form $a \mod p$, for a coprime to p, is $1/(p-1)$. Hence, the number of primes of the form $a \mod p$ for $a \not\equiv 0, 1$ must be $(p-2)/(p-1)$. Denote this set by A, so $\delta(A) = (p-2)/(p-1)$.

As α is algebraic (mentioned in proof of Lemma 5.2.10, we know the extension $\mathbb{Q}(\alpha)$ is welldefined and separable. Now let L be the normal closure of $\mathbb{Q}(\alpha)$. As it is defined by adjoining all other roots of the minimal polynomial of α, it is a separable extension. Because the extensions L/K and $K/\mathbb{Q}$ are separable, the extension $L/\mathbb{Q}$ is separable. This means the extension $L/\mathbb{Q}$ is both normal and separable, hence it is Galois.

Chebotarev's density theorem tells us that the density of primes that split completely in an Galois extension $L/\mathbb{Q}$ is precisely $1/[L:\mathbb{Q}]$ (Theorem 13.4 in [Neu92]). As $\mathbb{Q}(\alpha)$ is a separable extension, α has a minimal polynomial F of degree $d := [\mathbb{Q}(\alpha):\mathbb{Q}]$, and the normal closure is created by adjoining all $n-1$ other roots of F to $\mathbb{Q}(\alpha)$. For each root of F the extension can be of degree at most d. However, if it were of degree d, then all roots are included at once. Hence, if we need to extend $\mathbb{Q}(\alpha)$ for each root separately, we have extensions of degrees at most $d-1$, $d-2$, etc. So $[L:\mathbb{Q}] \leq d!$. Hence, the degree $[L:\mathbb{Q}(\alpha)]$ is at most $(d-1)!$. We see that $[L:\mathbb{Q}] \leq [\mathbb{Q}(\alpha):\mathbb{Q}]!$. Let us denote the set of primes that split completely in L by B, therefore: $\delta(B) = 1/d(d-1)$. We are interested in the density of $A \cap B$. Note that if $\delta(A) + \delta(B) > 1$, then $\delta(A \cap B) > 0$. In other words if

$$\frac{p-2}{p-1} + \frac{1}{d!} > 1 \iff \frac{1}{d!} > \frac{1}{p-1} \iff p-1 > d!.$$

We now prove that assumption 1. implies assumption 2. Because $\mathbb{Q}(\alpha)$ is a field, it is also a simple $\mathbb{Q}$-subalgebra on $\operatorname{End}^0(A)$, and it contains 1. Therefore the the degree $[\mathbb{Q}(\alpha):\mathbb{Q}] = d$ must divide $2g$, with $g = \dim(A)$. This follows from Proposition 2 on p. 36 of [Shi98] by noting that a field is it its own centre. This means that $d = [\mathbb{Q}(\alpha):\mathbb{Q}]$ is at most $2g$. We see that $p-1 > 2g! > d!$. □

Lemma 5.2.13. *Let E be an elliptic curve over a field K of characteristic $p > 0$ of height h, and let $\alpha : E \to E$ be a separable isogeny of degree at least 2. Define $K = \mathbb{Q}(\alpha) \subset \operatorname{End}^0(E)$ as before, then for all $\beta \in K \cap \operatorname{End}(E)$*

$$\deg_i(\beta) = p^{a v_{\mathfrak{p}}(\beta)},$$

Where a is an integer and

$$\mathfrak{p} = \begin{cases} (\pi) & \text{if } \pi \in K; \\ (p) & \text{if } \pi \notin K, \end{cases}$$

where π is the pth Frobenius on E. Moreover, if $\beta = \alpha^{k(p^2-1)} - 1$, then

$$v_{\mathfrak{p}}(\alpha^{k(p^2-1)} - 1) = v_{\mathfrak{p}}(\alpha^{p^2-1}) + b v_p(k),$$

with b an integer only depending on K.

Proof. If $\alpha \in \mathbb{Q}$, then $\pi \notin K = \mathbb{Q}$. This means $\beta = [m]$ for some $m \in \mathbb{Z}$, and therefore $\deg_i(\beta) = p^{h v_p(m)}$. This proves the lemma.

Now let $\alpha \notin \mathbb{Q}$ and assume $\pi \in K$, then $n = 2$, because $n \mid 2g = 2$ and $K \neq \mathbb{Q}$. We get that $\deg(\beta) = N_{K/\mathbb{Q}}(\beta)$ (Lemma 5.2.10). Note that $\beta = \gamma \circ \pi^n$ for some separable γ and integer n (Corollary 2.12. in [Sil09]). So $\deg_i(\beta) = \deg_i(\pi)^n = p^n$. We claim that (π) is a prime ideal in $\mathcal{O}_K$. Clearly, the ideal norm $N((\pi)) = p$, because $N_{K/\mathbb{Q}}(\pi) = \deg(\pi) = p$. When the norm of an ideal is prime, it clearly cannot be divisible by another ideal, hence it must be prime. We can see that $v_\pi(\beta) = n$, and hence

$$\deg_i(\beta) = \deg_i(\gamma \circ \pi^n) = \deg_i(\gamma)\deg_i(\pi)^n = \deg_i(\pi)^n = p^{v_\pi(n)}.$$

Lastly, we let $\alpha \notin \mathbb{Q}$ and $\pi \notin K$. We still have that $\beta = \gamma \circ \pi^n$ for some separable γ and integer n. However, as $\pi \notin K$, we must consider the smallest prime ideal that contains π. Because $N_{K/\mathbb{Q}}(\pi) = \deg(\pi) = p$, we know that $\pi \circ \hat{\pi} = p$ (the dual in Theorem 6.1 in [Sil09]). Hence, the smallest ideal which contains elements divisible by π must be (p), as $N((p)) = p^2$, and no ideal of degree p containing elements divisible by π can exist, as π itself is not contained in K. Therefore, we see that $\beta = \delta \circ p^k$, with

$$\deg_i(\beta) = \deg_i(\delta \circ p^k) = \deg_i(p)^n = p^{hk}$$

Here h is the height of E and we see that $\deg_i(\beta) = p^{hv_p(\beta)}$.
For the second part of the lemma we take $\beta = \alpha^{k(p^2-1)} - 1$. Note that $\#\mathfrak{p} = p^\epsilon - 1$, with $\epsilon = 1, 2$ as the field extension has degree 2. In either case, $\#\mathfrak{p} \mid p^2 - 1$. Because α is separable, it is clear that $\alpha \neq 0 \mod \mathfrak{p}$. Hence, we get $\alpha^{p^2-1} - 1 \in \mathfrak{p}$. Now we will write $\gamma = \alpha^{p^2-1}$ for easier notation. We prove $v_\mathfrak{p}(\gamma^k - 1) = v_\mathfrak{p}(\gamma - 1) + v_p(k)$, for $\gamma - 1 \in \mathfrak{p}$ and $\gamma \neq 1$. We prove this by induction on $v_p(k)$. Observe that $\gamma^k - 1 = (\gamma - 1)(\gamma^{k-1} + \ldots + 1)$, and hence $v_\mathfrak{p}(\gamma^k - 1) = v_\mathfrak{p}(\gamma - 1) + v_\mathfrak{p}(\gamma^{k-1} + \ldots + 1)$. We compute

$$\gamma^{k-1} + \ldots + 1 \equiv 1 + \ldots + 1 \mod \mathfrak{p} \equiv k \mod \mathfrak{p},$$

First suppose $v_p(k) = 0$, then clearly k is not zero over any ideal $\mathfrak{p}$ dividing (p) either. Now suppose $k = p$, then it just depends on $v_\mathfrak{p}(p)$ which is an integer:

$$v_\mathfrak{p}(\gamma^k - 1) = v_\mathfrak{p}(\gamma - 1) + bv_p(k),$$

with $b = 1$ or $b = v_\mathfrak{p}(p)$, an integer either way. Now let $k = p^i u$, for some integer i and $p \nmid u$. Then $\gamma^{p^i} - 1 \in \mathfrak{p}$ holds, hence we apply the proof for $v_p(u) = 0$ and see that

$$v_\mathfrak{p}(\gamma^k - 1) = v_\mathfrak{p}(\gamma^{p^i} - 1) + bv_p(u) = v_\mathfrak{p}(\gamma^{p^i} - 1).$$

Now we also note that $\gamma^{p^{i-1}} - 1 \in \mathfrak{p}$ for $i > 0$, hence we apply the proof for $v_p(p) = 1$:

$$v_\mathfrak{p}(\gamma^k - 1) = v_\mathfrak{p}(\gamma^{p^i} - 1) = v_\mathfrak{p}(\gamma^{p^{i-1}} - 1) + b.$$

With induction on i we get

$$v_\mathfrak{p}(\gamma^k - 1) = v_\mathfrak{p}(\gamma - 1) + bv_p(k).$$

□

Theorem 5.2.14. *Let E be an elliptic curve over a field K of characteristic $p > 3$, and let $\alpha : E \to E$ be an isogeny of degree at least 2. If α is separable, then $\zeta_{\alpha,E}(T)$ is transcendental over $\mathbb{Q}(T)$.*

Proof. We first remark that the fixed point set of $\alpha^{\circ n}$ is the same as the kernel of $\alpha^{\circ n} - 1$. Therefore, we want to find $|\ker(\alpha^n - 1)|$. By Lemma 5.2.6 we know that $|\ker(\alpha^n - 1)| =$

$\deg(\alpha^n - 1)/\deg_i(\alpha^n - 1)$. We start with the case where α is separable. So assume the zeta function is algebraic. Then by Lemma 5.1.4 the sequence

$$a_n := \deg(\alpha^n - 1)/\deg_i(\alpha^n - 1) \mod q = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^n - 1)^{2/d} p^{-av_{\mathfrak{p}}(\alpha^n - 1)} \mod q$$

is q-automatic for all primes q. Note that we used Lemmas 5.2.10 and 5.2.13 here. We will find a prime q such that this statement is false. First let let $q > N$ as in Lemma 5.2.11, such that $N_{K/\mathbb{Q}}(\alpha^n - 1) \mod q$ is periodic of period $q^f - 1$, where f is the inertia degree of the prime ideals above q in $\mathcal{O}_L$. We consider a subsequence, which must be q-automatic as well by Proposition 3.2.5:

$$b_n := a_{(p^2-1)((q^f-1)n+1)} = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{(p^2-1)((q^f-1)n+1)} - 1)^{2/d} p^{-av_{\mathfrak{p}}(\alpha^{(p^2-1)((q^f-1)n+1)}-1)} \mod q$$

As we choose $q > N$, the norm becomes periodic and we obtain:

$$b_n = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{p^2-1} - 1)^{2/d} p^{-av_{\mathfrak{p}}(\alpha^{(p^2-1)((q^f-1)n+1)}-1)} \mod q$$

Choose $q > N' := \max\{N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{p^2-1} - 1)^{2/d}, N\}$. Because $\deg(\alpha) > 2$ we must have $\alpha^{p^2-1} - 1 \neq 0$ and hence $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha^{p^2-1} - 1)^{2/d}$ is invertible in $\mathbb{F}_q^\times$. We multiply by its inverse and obtain another q-automatic sequence:

$$c_n := (N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(a^{p^2-1} - 1)^{2/d})^{-1} b_n = p^{-av_{\mathfrak{p}}(a^{(p^2-1)((q^f-1)n+1)}-1)} \mod q$$

Because $p > 3$, we know that $p - 1 > 2 = 2!$, and hence we may use Lemma 5.2.12: there exists an infinite number of primes such that $q^f - 1 \not\equiv 0 \mod p$. Certainly, there exist infinitely many such primes $q > N'$. So now let $q > N'$ also be such that $q^f - 1 \not\equiv 0 \mod p$. We use Lemma 5.2.13 to get

$$v_{\mathfrak{p}}(\alpha^{(p^2-1)((q^f-1)n+1)} - 1) = v_{\mathfrak{p}}(\alpha^{(p^2-1)} - 1) + bv_p(q^f - 1)n + 1).$$

We get

$$c_n = p^{-a(v_{\mathfrak{p}}(\alpha^{(p^2-1)}-1)+bv_p(q^f-1)n+1))} \mod q$$

As $q \neq p$, we can invert p and hence we can invert $p^{-av_{\mathfrak{p}}(\alpha^{(p^2-1)}-1)}$ to obtain another q-automatic sequence:

$$d_n := p^{av_{\mathfrak{p}}(\alpha^{(p^2-1)}-1)} c_n = p^{abv_p(q^f-1)n+1)} \mod q$$

Because $ab \in \mathbb{Z}$, we can assume $ab \in \mathbb{Z}_+$ as otherwise we just add multiples of $q - 1$. Moreover, we can choose $q > p^{ab}$ to ensure that $p^{ab} \neq 0, 1 \mod q$. Because we choose q such that $v_p(q^f - 1) = 0 \leq 0 = v_p(1)$, we can apply Proposition 3.2.9 and see that d_n cannot be q-automatic. This is a contradiction, hence the zeta function cannot be algebraic: it must be transcendental. □

Remark. To replace 'elliptic curve' with 'abelian variety' in Theorem 5.2.14 we need to find an equivalent to Lemma 5.2.13 for abelian varieties. Note that all other steps in the proof of Theorem 5.2.14 can be duplicated as Lemmas 5.1.4, 5.2.6, 5.2.10, 5.2.11, 5.2.12 are all stated in full generality, except for the fact that we need to increase the lower bound on p.

6

THE TAME DYNAMICAL ZETA FUNCTION IN POSITIVE CHARACTERISTIC

In the previous chapter we saw that over positive characteristic the dynamical zeta function can become transcendental for certain endomorphisms on $\mathbb{P}^1_K$ or abelian varieties. This suggests that a straightforward pattern in the number of fixed points of iterates cannot easily be deduced. However, one would like to have an alternative which contains at least part of the information in a way that we can use or compute it well. In this chapter we present an alternative to the (full) dynamical zeta function: the *tame dynamical zeta function* due to J. Byszewski and G. Cornelissen. This chapter will exhibit some computations and results on the tame dynamical zeta function of dynamically affine maps. We will also discuss the notion of lifting to characteristic zero.

6.1 INTRODUCTION TO THE TAME DYNAMICAL ZETA FUNCTION

In this section we provide the definition of the tame dynamical zeta function, give the main result and a proposition which will be most useful in doing computations.

Definition 6.1.1. Let X be a variety defined over a field K of characteristic $p > 0$, and let $f : X \to X$ be a map. Then the **tame dynamical zeta function** of f is defined as

$$\zeta^*_{f,X}(T) := \exp \sum_{\substack{n=1, \\ p \nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n,$$

where

$$\mathcal{N}_n = \begin{cases} |\mathrm{Fix}(f^{\circ n})| & \text{if } |\mathrm{Fix}(f^{\circ n})| \in \mathbb{N}; \\ 0 & \text{otherwise.} \end{cases}$$

It turns out that the tame dynamical zeta function of all maps for which we computed it, unlike the full dynamical zeta function, is algebraic:

Theorem 6.1.2. *Let K be a field of characteristic $p > 0$, and let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a morphism of degree at least 2. If f is a power map, Chebyshev polynomial, Lattès map induced by a multiplication-by-m map or a (sub)additive polynomial, then the tame dynamical zeta function $\zeta^*_{f,\mathbb{P}^1_K}(T)$ is algebraic over $\mathbb{Q}(T)$.*

We will prove this theorem in Section 6.3.1, after we have completed all computations. To simplify parts of those computations we will use Proposition 6.3.1 to only do the computations for $\mathbb{G}_a \subset \mathbb{P}^1$ or $\mathbb{G}_m \subset \mathbb{P}^1$. Also, we have the following proposition:

Proposition 6.1.3. *Let $k \in \mathbb{Z}_{\geq 1}$ and T a variable. Then the following holds:*

$$\sum_{\substack{n=1,\\ k\nmid n}}^{\infty} \frac{T^n}{n} = \log\left(\frac{(1-T^k)^{1/k}}{1-T}\right).$$

Proof. Let $k \in \mathbb{Z}_{\geq 1}$. We compute:

$$\begin{aligned}
\sum_{\substack{n=1,\\ k\nmid n}}^{\infty} \frac{T^n}{n} &= \sum_{n=1}^{\infty} \frac{T^n}{n} - \sum_{\substack{n=1,\\ k\mid n}}^{\infty} \frac{T^n}{n} \\
&= \sum_{n=1}^{\infty} \frac{T^n}{n} - \sum_{\ell=1}^{\infty} \frac{T^{k\ell}}{k\ell} && \text{(substitute } n = k\ell) \\
&= \sum_{n=1}^{\infty} \frac{T^n}{n} - \frac{1}{k}\sum_{\ell=1}^{\infty} \frac{(T^k)^\ell}{\ell} \\
&= \log\left(\frac{1}{1-T}\right) - \frac{1}{k}\log\left(\frac{1}{1-T^k}\right) && \text{(power series log)} \\
&= \log\left(\frac{(1-T^k)^{1/k}}{1-T}\right).
\end{aligned}$$

□

We will often use this where k is equal to the characteristic p. Also, we may use substitutions $T = aT'^{\ell}$, for some $a \in \mathbb{Q}$ and $\ell \in \mathbb{Z}$.

6.2 DYNAMICALLY AFFINE MAPS ON $\mathbb{P}^1_K$

We will now compute the tame dynamical zeta functions, rather than the regular dynamical zeta functions in the positive characteristic case. We will discuss all five families of dynamically affine maps: power maps, Chebyshev polynomials, Lattès maps, additive polynomials and subadditive polynomials. For the first three families we will use results from the previous chapter as several results were for arbitrary field, i.e. not necessarily of characteristic zero.

As several computations are quite lengthy, boxes are used to assist the reader in recognizing all significant results.

6.2.1 *Power maps*

As we have seen in Subsection 5.1.2, we obtain a formula for the number of fixed points:

$$\mathcal{N}_n = (m^n - 1) \cdot |m^n - 1|_p.$$

To determine the tame dynamical zeta function, we distinguish between a number of cases.

***Case 1**: $p \mid m$.*

Assume $p \mid m$. Then $p \nmid m^n - 1$ for all $n \geq 1$, which means that $|m^n - 1|_p = 1$. Therefore, we find $\mathcal{N}_n = m^n - 1$. We find:

$$\log \zeta^*_{x^m, \mathbb{G}_{m,\mathbb{F}_p}}(T) = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{m^n - 1}{n} T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(mT)^n}{n} - \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{T^n}{n}$$
$$= \log\left(\frac{(1-(mT)^p)^{1/p}}{1-mT}\right) - \log\left(\frac{(1-T^p)^{1/p}}{1-T}\right).$$

The tame dynamical zeta function is easily determined:

$$\zeta^*_{x^m, \mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{(1-(mT)^p)^{1/p}}{(1-T^p)^{1/p}} \cdot \frac{1-T}{1-mT}. \qquad (6.2.1.1)$$

***Case 2**: $p \neq 2$ and $p \nmid m$.*

Assume $p \nmid m$ and $p \neq 2$. In this case m is invertible in $\mathbb{F}_p$. Hence, m has a multiplicative order $s \in \mathbb{Z}$ in $\mathbb{F}_p$. We apply Proposition 5.1.2(1,2):

$$\mathcal{N}_n = (m^n - 1) \cdot |m^n - 1|_p = \begin{cases} (m^n - 1) \cdot |m^s - 1|_p \cdot |n|_p & \text{if } s \mid n; \\ m^n - 1 & \text{if } s \nmid n. \end{cases}$$

First notice that as $p \nmid n$, the norm $|n|_p = 1$ in all cases. Let us introduce the notation

$$A := |m^s - 1|_p.$$

Also, note that s and p are coprime, because s divides the order of $\mathbb{F}_p^\times$, which is $p - 1$. We get:

$$\begin{aligned}
\log \zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) &= \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{\substack{n=1,\\ p\nmid n, s\nmid n}}^{\infty} \frac{m^n-1}{n} T^n + \sum_{\substack{n=1,\\ p\nmid n, s\mid n}}^{\infty} \frac{(m^n-1)A}{n} T^n \\
&= \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{m^n-1}{n} T^n - \sum_{\substack{n=1,\\ p\nmid n, s\mid n}}^{\infty} \frac{m^n-1}{n} T^n + A \sum_{\substack{n=1,\\ p\nmid n, s\mid n}}^{\infty} \frac{m^n-1}{n} T^n \\
&= \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{m^n-1}{n} T^n + (A-1) \sum_{\substack{n=1,\\ p\nmid k}}^{\infty} \frac{m^{sk}-1}{sk} T^{sk} \\
&= \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(mT)^n}{n} - \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{T^n}{n} + \frac{A-1}{s} \left(\sum_{\substack{n=1,\\ p\nmid k}}^{\infty} \frac{(mT)^{sk}}{k} - \sum_{\substack{n=1,\\ p\nmid k}}^{\infty} \frac{T^{sk}}{k} \right) \\
&= \log\left(\frac{(1-(mT)^p)^{1/p}}{1-mT} \right) - \log\left(\frac{(1-T^p)^{1/p}}{1-T} \right) \\
&\quad + \frac{A-1}{s} \log\left(\frac{(1-(mT)^{ps})^{1/p}}{1-(mT)^s} \right) - \frac{A-1}{s} \log\left(\frac{(1-T^{ps})^{1/p}}{1-T^s} \right).
\end{aligned}$$

The tame dynamical zeta function then becomes:

$$\begin{aligned}
\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) =& \frac{1-T}{1-mT} \cdot \frac{(1-(mT)^p)^{1/p}}{(1-T^p)^{1/p}} \\
& \cdot \left(\frac{(1-(mT)^{ps})^{1/p}}{(1-T^{ps})^{1/p}} \cdot \frac{1-T^s}{1-(mT)^s} \right)^{(A-1)/s}.
\end{aligned} \tag{6.2.1.2}$$

Moreover, assume $m \equiv 1 \mod p$. In this case $s = 1$ and the tame dynamical zeta function simplifies further:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \left(\frac{(1-(mT)^p)^{1/p}}{(1-T^p)^{1/p}} \cdot \frac{1-T}{1-mT} \right)^A. \tag{6.2.1.3}$$

***Case 3**: $p = 2$ and $2 \nmid m$.*

Assume $p \nmid m$ and $p = 2$. We can still use Proposition 5.1.2(1) to obtain that $\mathcal{N}_n = (m^n-1)|m^n-1|_2$. Note that by assumption m is odd, hence $s = 1$. We define $A := |m-1|_2$ and $B := |m+1|_2$. Then we have $\mathcal{N}_n = 2AB(m^n-1)$ for all $p \nmid n$.

We compute the tame dynamical zeta function:

$$\begin{aligned}
\log \zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) =& \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{\substack{n=1,\\ 2\nmid n}}^{\infty} \frac{2AB(m^n-1)}{n} T^n \\
=& 2AB \log\left(\frac{(1-(mT)^2)^{1/2}}{1-mT} \right) - 2AB \log\left(\frac{(1-T^2)^{1/2}}{1-T} \right)
\end{aligned}$$

This gives us the tame dynamical zeta function:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \left(\frac{(1-(mT)^2)^{1/2}}{(1-T^2)^{1/2}}\frac{1-T}{1-mT}\right)^{2AB}. \tag{6.2.1.4}$$

Comparison to characteristic zero

In Section 4.2.1 we had Equation 4.2.1.1 that said for K of characteristic 0:

$$\zeta_{x^m,\mathbb{G}_{m,K,0}}(T) = \frac{1-T}{1-mT}.$$

In this subsection we saw a few different answers. Recall that s denotes the multiplicative order of m in $\mathbb{F}_p$ and $A := |m^s - 1|_p$, also $B = |m+1|_2$ in the last case. We will give identities in each case to show the relation between the tame dynamical zeta function in positive characteristic and the zeta function in characteristic zero.

- If $p \mid m$, then

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{(1-(mT)^p)^{1/p}}{(1-T^p)^{1/p}} \cdot \frac{1-T}{1-mT}.$$

  This can be rewritten:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{\zeta_{x^m,\mathbb{G}_{m,K,0}}(T)}{\zeta_{x^{m^p},\mathbb{G}_{m,K,0}}(T^p)^{1/p}}. \tag{6.2.1.5}$$

- If $p \neq 2$ and $p \nmid m$, then

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{1-T}{1-mT} \cdot \frac{(1-(mT)^p)^{1/p}}{(1-T^p)^{1/p}} \cdot \left(\frac{(1-(mT)^{ps})^{1/p}}{(1-T^{ps})^{1/p}}\right)^{(A-1)/s} \cdot \left(\frac{1-T^s}{1-(mT)^s}\right)^{(A-1)/s}.$$

  Again, we can write this using the zeta function in characteristic zero:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{\zeta_{x^m,\mathbb{G}_{m,K,0}}(T)}{\zeta_{x^{m^p},\mathbb{G}_{m,K,0}}(T^p)^{1/p}} \cdot \left(\frac{\zeta_{x^{m^s},\mathbb{G}_{m,K,0}}(T^s)}{\zeta_{x^{m^{ps}},\mathbb{G}_{m,K,0}}(T^{ps})^{1/p}}\right)^{(A-1)/s}. \tag{6.2.1.6}$$

- A special case of this is when $m \equiv 1 \mod p$, then

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \left(\frac{(1-(mT)^p)^{1/p}}{(1-T^p)^{1/p}} \cdot \frac{1-T}{1-mT}\right)^A.$$

As we did before, we will now rewrite this:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \left(\frac{\zeta_{x^m,\mathbb{G}_{m,K,0}}(T)}{\zeta_{x^{mp},\mathbb{G}_{m,K,0}}(T^p)^{1/p}} \right)^A . \tag{6.2.1.7}$$

- If $p = 2$ and m is odd, then

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \left(\frac{(1-(mT)^2)^{1/2}}{(1-T^2)^{1/2}} \frac{1-T}{1-mT} \right)^{2AB} .$$

And we repeat this process:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \left(\frac{\zeta_{x^m,\mathbb{G}_{m,K,0}}(T)}{\zeta_{x^{m^2},\mathbb{G}_{m,K,0}}(T^2)^{1/2}} \right)^{2AB} . \tag{6.2.1.8}$$

6.2.2 *Chebyshev polynomials*

As we have seen in Subsection 5.1.3, we have that: $|\mathrm{Fix}(T_d^{\circ n})| = \frac{|\mu_{d^n+1}|+|\mu_{d^n-1}|}{2}$. In this formula we again use the identity from Proposition 5.1.2(1), so $|\mu_k| = k \cdot |k|_p$.

***Case 1**: $p \mid d$.*

If $p \mid d$ we know that $|d^n - 1|_p = |d^n + 1|_p = 1$. This means we get a formula for the number of fixed points:

$$\mathcal{N}_n = \frac{d^n + 1 + d^n - 1}{2} = d^n.$$

With this identity we determine the log of the tame dynamical zeta function:

$$\log \zeta^*_{T^d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n}{n} T^n = \log \left(\frac{(1-(dT)^p)^{1/p}}{1-dT} \right).$$

This gives us the tame dynamical zeta function:

$$\zeta^*_{T^d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \frac{(1-(dT)^p)^{1/p}}{1-dT} . \tag{6.2.2.1}$$

***Case 2**: let p be odd, $p \nmid d$ and s odd.*

Since $d \in \mathbb{F}_p^\times$, let s be the multiplicative order of d in $\mathbb{F}_p$ and $A := |d^s - 1|_p$. Again, we have that:

$$|\mu_{d^n-1}| = (d^n - 1) \begin{cases} 1 & \text{if } s \mid n; \\ A \cdot |n|_p & \text{if } s \nmid n. \end{cases}$$

We define:

$$A_n = \begin{cases} A & \text{if } s \mid n; \\ 1 & \text{if } s \nmid n. \end{cases}$$

In this case s is odd, which means that $|d^n + 1|_p = 1$ for all n. When $p \nmid n$, we get a formula for the number of fixed points:

$$\mathcal{N}_n = \frac{(d^n - 1)A_n + d^n + 1}{2}.$$

In fact we obtain two summations which we will compute separately. We start with the first half which depends on A_n:

$$\begin{aligned}\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(d^n-1)A_n}{2n} T^n &= \sum_{\substack{n=1,\\ p\nmid n, s\mid n}}^{\infty} \frac{(d^n-1)A}{2n} T^n + \sum_{\substack{n=1,\\ p\nmid n, s\nmid n}}^{\infty} \frac{(d^n-1)}{2n} T^n \\ &= (A-1) \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{d^{ks}-1}{2ks} T^{ks} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(d^n-1)}{2n} T^n.\end{aligned}$$

These two sums need to be split in two again:

$$\begin{aligned}\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(d^n-1)A_n}{2n} T^n &= \frac{A-1}{2s}\left(\sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{(dT)^{ks}}{k} - \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{T^{ks}}{k}\right) + \frac{1}{2}\left(\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(dT)^n}{n} - \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{T^n}{n}\right) \\ &= \frac{A-1}{2s}\left(\log\left(\frac{(1-(dT)^{ps})^{1/p}}{1-(dT)^s}\right) - \log\left(\frac{(1-T^{ps})^{1/p}}{1-T^s}\right)\right) \\ &\quad + \frac{1}{2}\left(\log\left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\right) - \log\left(\frac{(1-T^p)^{1/p}}{1-T}\right)\right).\end{aligned}$$

Next we compute the second summation:

$$\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n+1}{2n} T^n = \frac{1}{2}\left(\log\left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\right) + \log\left(\frac{(1-T^p)^{1/p}}{1-T}\right)\right).$$

In this case the tame dynamical zeta function becomes:

$$\begin{aligned}\zeta^*_{T_d, \mathbb{G}_{a,\mathbb{F}_p}}(T) = &\left(\frac{(1-(dT)^{ps})^{1/p}}{1-(dT)^s}\frac{1-T^s}{(1-T^{ps})^{1/p}}\right)^{(A-1)/2s} \cdot \left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\frac{1-T}{(1-T^p)^{1/p}}\right)^{1/2} \\ &\left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\frac{(1-T^p)^{1/p}}{1-T}\right)^{1/2}.\end{aligned}$$

This can be written in a simpler formula:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{(1-(dT)^{ps})^{1/p}}{1-(dT)^s} \frac{1-T^s}{(1-T^{ps})^{1/p}} \right)^{(A-1)/2s} \cdot \frac{(1-(dT)^p)^{1/p}}{1-dT}. \quad (6.2.2.2)$$

If $d \equiv 1 \mod p$, then s must be 1 and the above can be simplified:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{(1-(dT)^p)^{1/p}}{1-dT} \right)^{(A+1)/2} \cdot \left(\frac{1-T}{(1-T^p)^{1/p}} \right)^{(A-1)/2}. \quad (6.2.2.3)$$

Case 3*: p is odd, $p \nmid d$ and s even.*

Because s is even, we can write $t = s/2$ and we know that $|d^t+1|_p = |d^s-1|_p = A$ by Proposition 5.1.2(4). Similar to before, we can find a useful identity:

$$|\mu_{d^n+1}| = (d^n+1) \begin{cases} 1 & \text{if } t \mid n \text{ or } \frac{n}{t} \in 2\mathbb{Z}; \\ A \cdot |n|_p & \text{if } \frac{n}{t} \in 1+2\mathbb{Z}. \end{cases}$$

Again, we define:

$$A_n = \begin{cases} A & \text{if } s \mid n; \\ 1 & \text{if } s \nmid n, \end{cases} \qquad \text{and} \qquad B_n = \begin{cases} A & \text{if } \frac{n}{t} \in 1+2\mathbb{Z}; \\ 1 & \text{otherwise.} \end{cases}$$

With this, we can write:

$$\mathcal{N}_n = \frac{(d^n-1)A_n + (d^n+1)B_n}{2}.$$

Again this renders two summations. However, we already computed the first half in the previous case. Hence, we only have to compute the second half:

$$\begin{aligned}
\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(d^n+1)B_n}{2n} T^n &= \sum_{\substack{n=1,\\ p\nmid n, t\mid n}}^{\infty} \frac{(d^n+1)B_n}{2n} T^n + \sum_{\substack{n=1,\\ p\nmid n, t\nmid n}}^{\infty} \frac{d^n+1}{2n} T^n \\
&= \sum_{\substack{n=1,\\ p\nmid n, t\mid n}}^{\infty} \frac{(d^n+1)(B_n-1)}{2n} T^n + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n+1}{2n} T^n \\
&= \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{(d^{kt}+1)(B_{kt}-1)}{2kt} T^{kt} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n+1}{2n} T^n \\
&= \sum_{\substack{k=1,\\ p\nmid k, 2\mid k}}^{\infty} \frac{(d^{kt}+1)(1-1)}{2kt} T^{kt} + \sum_{\substack{k=1,\\ p\nmid k, 2\nmid k}}^{\infty} \frac{(d^{kt}+1)(A-1)}{2kt} T^{kt} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n+1}{2n} T^n.
\end{aligned}$$

We can see that the first summation cancels and the last summation is one we computed already for case 2. Hence, we compute the second summation:

$$\begin{aligned}\sum_{\substack{k=1,\\ p\nmid k, 2\nmid k}}^{\infty} \frac{(d^{kt}+1)(A-1)}{2kt} T^{kt} &= \frac{A-1}{2t} \sum_{\substack{k=1,\\ p\nmid k, 2\nmid k}}^{\infty} \frac{d^{kt}+1}{k} T^{kt} = \frac{A-1}{2t} \left(\sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{d^{kt}+1}{k} T^{kt} - \sum_{\substack{\ell=1,\\ p\nmid \ell}}^{\infty} \frac{d^{2\ell t}+1}{2\ell} T^{2\ell} \right) \\ &= \frac{A-1}{2t} \log\left(\frac{(1-(dT)^{pt})^{1/p}}{1-(dT)^t} \frac{(1-T^{pt})^{1/p}}{1-T^t} \right) \\ &\quad - \frac{A-1}{4t} \log\left(\frac{(1-(dT)^{2pt})^{1/p}}{1-(dT)^{2t}} \frac{(1-T^{2pt})^{1/p}}{1-T^{2t}} \right).\end{aligned}$$

When we combine the results we obtain the tame dynamical zeta function:

$$\begin{aligned}\zeta^*_{T_d, \mathbb{G}_{a,\mathbb{F}_p}}(T) = &\left(\frac{(1-(dT)^{ps})^{1/p}}{1-(dT)^s} \frac{1-T^s}{(1-T^{ps})^{1/p}} \right)^{(A-1)/2s} \cdot \left(\frac{(1-(dT)^p)^{1/p}}{1-dT} \frac{1-T}{(1-T^p)^{1/p}} \right)^{1/2} \\ &\cdot \left(\frac{(1-(dT)^p)^{1/p}}{1-dT} \frac{(1-T^p)^{1/p}}{1-T} \right)^{1/2} \cdot \left(\frac{(1-(dT)^{pt})^{1/p}}{1-(dT)^t} \frac{(1-T^{pt})^{1/p}}{1-T^t} \right)^{(A-1)/2t} \\ &\cdot \left(\frac{1-(dT)^{2t}}{(1-(dT)^{2pt})^{1/p}} \frac{1-T^{2t}}{(1-T^{2pt})^{1/p}} \right)^{(A-1)/4t}.\end{aligned}$$

Using the fact that $s = 2t$, we can simplify the expression and regroup certain factors:

$$\begin{aligned}\zeta^*_{T_d, \mathbb{G}_{a,\mathbb{F}_p}}(T) = &\left(\frac{(1-(dT)^{pt})^{1/p}}{1-(dT)^t} \frac{(1-T^{pt})^{1/p}}{1-T^t} \frac{1-T^{2t}}{(1-T^{2pt})^{1/p}} \right)^{(A-1)/2t} \\ &\cdot \left(\frac{(1-(dT)^p)^{1/p}}{1-dT} \right).\end{aligned} \tag{6.2.2.4}$$

***Case 4**: $p = 2$ and d is odd.*

For $p = 2$ we still have $\mathcal{N}_n = \frac{1}{2}((d^n+1)|d^n+1|_2 + (d^n-1)|d^n-1|_2)$. Also, as d is an odd integer, we know that $s = 1$. Define $A := |d-1|_2$ and $B := |d+1|$. Then $|d^n-1|_2 = 2AB$ because $2 \nmid n$. Similarly, we get $|d^n+1|_2 = B$ for $2 \nmid n$. Let us write this in a formula:

$$\mathcal{N}_n = \frac{(d^n+1)B + (d^n-1)2AB}{2} = \frac{(2A+1)Bd^n}{2} + \frac{(1-2A)B}{2}.$$

The log of the tame dynamical zeta function becomes::

$$\begin{aligned}\log \zeta^*_{T^d,\mathbb{G}_{a,\mathbb{F}_p}}(T) &= \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(2A+1)Bd^n}{2n} T^n + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(1-2A)B}{2n} T^n \\ &= \frac{(2A+1)B}{2} \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(dT)^n}{n} + \frac{(1-2A)B}{2} \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{T^n}{n} \\ &= \frac{(2A+1)B}{2} \log\left(\frac{1-(dT)^p)^{1/p}}{1-dT}\right) + \frac{(1-2A)B}{2} \log\left(\frac{(1-T^p)^{1/p}}{1-T}\right).\end{aligned}$$

Moreover, we find the tame dynamical zeta function:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{1-(dT)^p)^{1/p}}{1-dT}\right)^{(2A+1)B/2} \cdot \left(\frac{(1-T^p)^{1/p}}{1-T}\right)^{(1-2A)B/2}. \quad (6.2.2.5)$$

Comparison to characteristic zero

In Subsection 4.2.2 we had Equation 4.2.2.1 that said, for a field K of characteristic 0:

$$\zeta_{T_d,\mathbb{G}_{a,K,0}}(T) = \exp \sum_{n=1}^{\infty} \frac{d^n}{n} T^n = \frac{1}{1-dT}.$$

In Subsection 6.2.2 we obtained results for distinct cases. Recall that s denotes the multiplicative order of d in $\mathbb{F}_p$, and $A := |d^s - 1|_p$, also $B = |d+1|_2$ in the last case. If s is even, then $t = s/2$. Unfortunately, unlike the power map case, here we cannot give an identity solely in terms of the zeta function in characteristic zero. We will give an identity that is as close as possible.

- If $p \mid d$, then

$$\zeta^*_{T^d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \frac{(1-(dT)^p)^{1/p}}{1-dT}.$$

  This can be rewritten:

$$\zeta^*_{T^d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \frac{\zeta_{T_d,\mathbb{G}_{a,K,0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K,0}}(T^p)^{1/p}}. \quad (6.2.2.6)$$

- If $p \neq 2$, $p \nmid d$ and s odd, then

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{(1-(dT)^{ps})^{1/p}}{1-(dT)^s} \frac{1-T^s}{(1-T^{ps})^{1/p}}\right)^{(A-1)/2s} \cdot \frac{(1-(dT)^p)^{1/p}}{1-dT}.$$

And we repeat this process:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{\zeta_{T_{d^s},\mathbb{G}_{a,K,0}}(T^s)}{\zeta_{T_{d^{ps}},\mathbb{G}_{a,K,0}}(T^{ps})^{1/p}} \frac{1-T^s}{(1-T^{ps})^{1/p}} \right)^{(A-1)/2s} \cdot \frac{\zeta_{T_d,\mathbb{G}_{a,K,0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K,0}}(T^p)^{1/p}}. \tag{6.2.2.7}$$

- A particular case of the above is when $d \equiv 1 \mod p$, we get:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{(1-(dT)^p)^{1/p}}{1-dT} \right)^{(A+1)/2} \cdot \left(\frac{1-T}{(1-T^p)^{1/p}} \right)^{(A-1)/2}.$$

As we did before, we will now rewrite this:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{\zeta_{T_d,\mathbb{G}_{a,K,0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K,0}}(T^p)^{1/p}} \right)^{(A+1)/2} \cdot \left(\frac{1-T}{(1-T^p)^{1/p}} \right)^{(A-1)/2}. \tag{6.2.2.8}$$

- If $p \neq 2$, $p \nmid d$ and s even, then

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{(1-(dT)^{pt})^{1/p}}{1-(dT)^t} \frac{(1-T^{pt})^{1/p}}{1-T^t} \frac{1-T^{2t}}{(1-T^{2pt})^{1/p}} \right)^{(A-1)/2t} \cdot \frac{(1-(dT)^p)^{1/p}}{1-dT}.$$

We rewrite this using the zeta function in characteristic zero:

$$\begin{aligned} \zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = & \left(\frac{\zeta_{T_{d^t},\mathbb{G}_{a,K,0}}(T^t)}{\zeta_{T_{d^{pt}},\mathbb{G}_{a,K,0}}(T^{pt})^{1/p}} \frac{(1-T^{pt})^{1/p}}{1-T^t} \frac{1-T^{2t}}{(1-T^{2pt})^{1/p}} \right)^{(A-1)/2t} \\ & \cdot \frac{\zeta_{T_d,\mathbb{G}_{a,K,0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K,0}}(T^p)^{1/p}}. \end{aligned} \tag{6.2.2.9}$$

- If $p = 2$ and d is odd, then

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{1-(dT)^p)^{1/p}}{1-dT} \right)^{(2A+1)B/2} \cdot \left(\frac{(1-T^p)^{1/p}}{1-T} \right)^{(1-2A)B/2}.$$

This can be rewritten:

$$\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{\zeta_{T_d,\mathbb{G}_{a,K,0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K,0}}(T^p)^{1/p}} \right)^{(2A+1)B/2} \cdot \left(\frac{(1-T^p)^{1/p}}{1-T} \right)^{(1-2A)B/2}. \tag{6.2.2.10}$$

6.2.3 *Lattès maps*

We use the result we obtained in Subsection 5.1.4:

$$
\begin{aligned}
|\mathrm{Fix}(L_m^{\circ n})| &= \frac{1}{2}|E_{m^n-1}| + \frac{1}{2}|E_{m^n+1}| \\
&= \frac{1}{2}(m^n-1)^2|m^n-1|_p^h + \frac{1}{2}(m^n+1)^2|m^n+1|_p^h.
\end{aligned}
$$

***Case 1**: $p \mid m$.*

When p and m are not coprime, we know that $|m^n-1|_p = |m^n+1|_p = 1$. This simplifies the formula for the number of fixed points to:

$$\mathcal{N}_n = \frac{1}{2}(m^n-1)^2 + \frac{1}{2}(m^n+1)^2 = m^{2n}+1.$$

Using this identity we can compute the log of the tame dynamical zeta function:

$$
\begin{aligned}
\log \zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) &= \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n}T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{m^{2n}+1}{n}T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^2T)^n}{n} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{T^n}{n} \\
&= \log\left(\frac{(1-(m^2T)^p)^{1/p}}{1-m^2T}\right) + \log\left(\frac{(1-T^p)^{1/p}}{1-T}\right).
\end{aligned}
$$

This gives the tame dynamical zeta function:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \frac{(1-(m^2T)^p)^{1/p}}{1-m^2T} \cdot \frac{(1-T^p)^{1/p}}{1-T}. \tag{6.2.3.1}$$

***Case 2**: let p be odd, $p \nmid m$ and s odd.*

As before we write $A := |m^s-1|_p$, where s is the multiplicative order of m in $\mathbb{F}_p$. We define:

$$A_n = \begin{cases} A^h & \text{if } s \mid n; \\ 1 & \text{if } s \nmid n. \end{cases}$$

As s is odd we know that $|m^n+1|_p = 1$. We again use Proposition 5.1.2 to see that $\mathcal{N}_n = (m^n-1)^2A_n/2 + (m^n+1)^2/2$ for n not divisible by p. This identity allows us to compute the log of the tame dynamical zeta function:

$$\log \zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n}T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^n-1)^2A_n}{2n}T^n + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^n+1)^2}{2n}T^n.$$

We compute these two sums separately, starting with the summation depending on A_n:

$$\begin{aligned}\sum_{\substack{n=1,\\ p\nmid n}}^{\infty}\frac{(m^n-1)^2A_n}{2n}T^n =&\sum_{\substack{n=1,\\ p\nmid n, s\mid n}}^{\infty}\frac{(m^n-1)^2A^h}{2n}T^n+\sum_{\substack{n=1,\\ p\nmid n, s\nmid n}}^{\infty}\frac{(m^n-1)^2}{2n}T^n\\ =&\sum_{\substack{k=1,\\ p\nmid k}}^{\infty}\frac{(m^{ks}-1)^2(A^h-1)}{2ks}T^{ks}+\sum_{\substack{n=1,\\ p\nmid n}}^{\infty}\frac{(m^n-1)^2}{2n}T^n\\ =&\frac{A^h-1}{2s}\sum_{\substack{k=1,\\ p\nmid k}}^{\infty}\frac{m^{2ks}-2m^{ks}+1}{k}T^{ks}+\frac{1}{2}\sum_{\substack{n=1,\\ p\nmid n}}^{\infty}\frac{m^{2n}-2m^n+1}{n}T^n\\ =&\frac{A^h-1}{2s}\log\left(\frac{(1-(m^2T)^{ps})^{1/p}}{1-(m^2T)^s}\left(\frac{(1-(mT)^{ps})^{1/p}}{1-(mT)^s}\right)^{-2}\frac{(1-T^{ps})^{1/p}}{1-T^s}\right)\\ &+\frac{1}{2}\log\left(\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\left(\frac{(1-(mT)^{p})^{1/p}}{1-mT}\right)^{-2}\frac{(1-T^{p})^{1/p}}{1-T}\right).\end{aligned}$$

Now we determine the second summation:

$$\begin{aligned}\sum_{\substack{n=1,\\ p\nmid n}}^{\infty}\frac{(m^n+1)^2}{2n}T^n =&\frac{1}{2}\sum_{\substack{n=1,\\ p\nmid n}}^{\infty}\frac{m^{2n}+2m^n+1}{n}T^n\\ =&\frac{1}{2}\log\left(\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\left(\frac{(1-(mT)^{p})^{1/p}}{1-mT}\right)^{2}\frac{(1-T^{p})^{1/p}}{1-T}\right).\end{aligned}$$

We can combine the results to find the tame dynamical zeta function:

$$\begin{aligned}\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T)=&\left(\frac{(1-(m^2T)^{ps})^{1/p}}{1-(m^2T)^s}\frac{(1-T^{ps})^{1/p}}{1-T^s}\right)^{(A^h-1)/2s}\cdot\left(\frac{1-(mT)^s}{(1-(mT)^{ps})^{1/p}}\right)^{(A^h-1)/s}\\ &\cdot\left(\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\frac{(1-T^{p})^{1/p}}{1-T}\right)^{1/2}\cdot\frac{1-mT}{(1-(mT)^p)^{1/p}}\\ &\cdot\left(\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\frac{(1-T^{p})^{1/p}}{1-T}\right)^{1/2}\cdot\frac{(1-(mT)^p)^{1/p}}{1-mT}.\end{aligned}$$

We obtain a simpler identity:

$$\begin{aligned}\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T)=&\left(\frac{(1-(m^2T)^{ps})^{1/p}}{1-(m^2T)^s}\left(\frac{1-(mT)^s}{(1-(mT)^{ps})^{1/p}}\right)^{2}\frac{(1-T^{ps})^{1/p}}{1-T^s}\right)^{(A^h-1)/2s}\\ &\cdot\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\frac{(1-T^{p})^{1/p}}{1-T}.\end{aligned} \tag{6.2.3.2}$$

Now we can assume $m\equiv 1 \mod p$ which means $s=1$. The above formula simplifies even further to another identity:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\frac{(1-(m^2T)^p)^{1/p}}{1-m^2T} \frac{(1-T^p)^{1/p}}{1-T} \right)^{(A^h+1)/2} \cdot \left(\frac{1-mT}{(1-(mT)^p)^{1/p}} \right)^{A^h-1}. \tag{6.2.3.3}$$

***Case 3**: let p be odd, $p \nmid m$ and s even.*

Because m and p are coprime, m is a root of unity in $\mathbb{F}_p$. Let s be the multiplicative order of m in $\mathbb{F}_p$ and write $A := |m^s - 1|_p$. We can use Proposition 5.1.2(4.) to also write $A := |m^t + 1|_p$, where $t = s/2$. For $p \nmid n$ we define:

$$A_n = \begin{cases} A^h & \text{if } s \mid n; \\ 1 & \text{if } s \nmid n, \end{cases} \quad \text{and} \quad B_n = \begin{cases} A^h & \text{if } \frac{n}{t} \in 1+2\mathbb{Z}; \\ 1 & \text{otherwise.} \end{cases}$$

Again we can start with computing the log of the tame dynamical zeta function:

$$\log \zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^n-1)^2 A_n + (m^n+1)^2 B_n}{2n} T^n.$$

The first summation has already been determined in the previous case. Hence, we only have to compute the second summation depending on B_n. Note that this computation is quite similar to case 3 of the Chebyshev polynomials.

$$\begin{aligned}
\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^n+1)^2 B_n}{2n} T^n &= \sum_{\substack{n=1,\\ p\nmid n, t\mid n}}^{\infty} \frac{(m^n+1)^2 B_n}{2n} T^n + \sum_{\substack{n=1,\\ p\nmid n, t\nmid n}}^{\infty} \frac{(m^n+1)^2}{2n} T^n \\
&= \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{(m^{kt}+1)^2 (B_{kt}-1)}{2kt} T^{kt} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^n+1)^2}{2n} T^n \\
&= \sum_{\substack{k=1,\\ p\nmid k, 2\mid k}}^{\infty} \frac{(m^{kt}+1)^2 (1-1)}{2kt} T^{kt} + \sum_{\substack{k=1,\\ p\nmid k, 2\nmid k}}^{\infty} \frac{(m^{kt}+1)^2 (A^h-1)}{2kt} T^{kt} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{(m^n+1)^2}{2n} T^n.
\end{aligned}$$

The first summation is zero and the last summation we already computed in the previous case. Therefore, we continue computing only the second summation:

$$\sum_{\substack{k=1,\\ p\nmid k, 2\nmid k}}^{\infty} \frac{(m^{kt}+1)^2(A^h-1)}{2kt} T^{kt} = \frac{A^h-1}{2t}\left(\sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{m^{2kt}+2m^{kt}+1}{k} T^{kt} + \sum_{\substack{\ell=1,\\ p\nmid \ell}}^{\infty} \frac{(m^{4\ell t}+2m^{2\ell t}+1}{2\ell} T^{2\ell t}\right)$$
$$= \frac{A^h-1}{2t}\log\left(\frac{(1-(m^2T)^{pt})^{1/p}}{1-(m^2T)^t}\cdot\left(\frac{(1-(mT)^{pt})^{1/p}}{1-(mT)^t}\right)^2 \frac{(1-T^{pt})^{1/p}}{1-T^t}\right)$$
$$+\frac{A^h-1}{4t}\log\left(\frac{(1-(m^2T)^{2pt})^{1/p}}{1-(m^2T)^{2t}}\cdot\left(\frac{(1-(mT)^{2pt})^{1/p}}{1-(mT)^{2t}}\right)^2 \frac{(1-T^{2pt})^{1/p}}{1-T^{2t}}\right).$$

We can combine this result with the part depending on A_n to get the complete tame dynamical zeta function:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\frac{(1-(m^2T)^{ps})^{1/p}}{1-(m^2T)^s}\left(\frac{(1-(mT)^{ps})^{1/p}}{1-(mT)^s}\right)^{-2}\frac{(1-T^{ps})^{1/p}}{1-T^s}\right)^{(A^h-1)/2s}$$
$$\cdot\left(\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\left(\frac{(1-(mT)^{p})^{1/p}}{1-mT}\right)^{-2}\frac{(1-T^{p})^{1/p}}{1-T}\right)^{1/2}$$
$$\cdot\left(\frac{(1-(m^2T)^{pt})^{1/p}}{1-(m^2T)^t}\left(\frac{(1-(mT)^{pt})^{1/p}}{1-(mT)^t}\right)^{2}\frac{(1-T^{pt})^{1/p}}{1-T^t}\right)^{(A^h-1)/2t}$$
$$\cdot\left(\frac{(1-(m^2T)^{2pt})^{1/p}}{1-(m^2T)^{2t}}\left(\frac{(1-(mT)^{2pt})^{1/p}}{1-(mT)^{2t}}\right)^{2}\frac{(1-T^{2pt})^{1/p}}{1-T^{2t}}\right)^{(A^h-1)/4t}$$
$$\cdot\left(\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\left(\frac{(1-(mT)^{p})^{1/p}}{1-mT}\right)^{2}\frac{(1-T^{p})^{1/p}}{1-T}\right)^{1/2}.$$

Fortunately, we can reduce this expression quite a bit using $s = 2t$:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\frac{(1-(m^2T)^{pt})^{1/p}}{1-(m^2T)^t}\left(\frac{(1-(mT)^{pt})^{1/p}}{1-(mT)^t}\right)^{2}\frac{(1-T^{pt})^{1/p}}{1-T^t}\right)^{(A^h-1)/2t}$$
$$\cdot\left(\frac{(1-(m^2T)^{2pt})^{1/p}}{1-(m^2T)^{2t}}\frac{(1-T^{2pt})^{1/p}}{1-T^{2t}}\right)^{(A^h-1)/2t}\cdot\frac{(1-(m^2T)^{p})^{1/p}}{1-m^2T}\frac{(1-T^{p})^{1/p}}{1-T}. \tag{6.2.3.4}$$

If $m \equiv -1 \mod p$, then $t = 1$ and the identity becomes:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\frac{(1-(m^2T)^p)^{1/p}}{1-(m^2T)} \cdot \frac{(1-T^p)^{1/p}}{1-T}\right)^{(A^h+1)/2} \cdot \left(\frac{(1-(mT)^p)^{1/p}}{1-mT}\right)^{A^h-1} \cdot \left(\frac{(1-(m^2T)^{2p})^{1/p}}{1-(m^2T)^2}\frac{(1-T^{2p})^{1/p}}{1-T^2}\right)^{(A^h-1)/2}. \tag{6.2.3.5}$$

Case 4: *Let $p = 2$ and m odd.*

For $p = 2$ we still have $\mathcal{N}_n = \frac{1}{2}(m^n-1)^2|m^n-1|_p^h + \frac{1}{2}(m^n+1)^2|m^n+1|_p^h$. As m is odd, we can introduce $A := |m-1|_2$ and $B := |m+1|_2$. This gives us a formula for $2 \nmid n$:

$$\begin{aligned}\mathcal{N}_n &= \frac{(m^n-1)^2(2AB)^h + (m^n+1)^2B^h}{2} \\ &= \frac{(2^hA^h+1)B^hm^{2n}}{2} + (1-2^hA^h)B^hm^n + \frac{(2^hA^h+1)B^h}{2}.\end{aligned}$$

We use this to find the log of the tame dynamical zeta function:

$$\begin{aligned}\log\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) =& \sum_{\substack{k=1,\\2\nmid k}}^{\infty}\frac{(2^hA^h+1)B^hm^{2n}}{2n}T^n + \sum_{\substack{k=1,\\2\nmid k}}^{\infty}\frac{(1-2^hA^h)B^hm^n}{n}T^n + \sum_{\substack{k=1,\\2\nmid k}}^{\infty}\frac{(2^hA^h+1)B^h}{2n}T^n \\ =& \frac{(2^hA^h+1)B^h}{2}\sum_{\substack{k=1,\\2\nmid k}}^{\infty}\frac{(m^2T)^n}{n} + (1-2^hA^h)B^h\sum_{\substack{k=1,\\2\nmid k}}^{\infty}\frac{(mT)^n}{n} + \frac{(2^hA^h+1)B^h}{2}\sum_{\substack{k=1,\\2\nmid k}}^{\infty}\frac{T^n}{n} \\ =& \frac{(2^hA^h+1)B^h}{2}\log\left(\frac{(1-(m^2T)^2)^{1/2}}{1-m^2T}\right) + (1-2^hA^h)B^h\log\left(\frac{(1-(mT)^2)^{1/2}}{1-mT}\right) \\ &+ \frac{(2^hA^h+1)B^h}{2}\log\left(\frac{(1-T^2)^{1/2}}{1-T}\right).\end{aligned}$$

The tame dynamical zeta function follows easily:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\frac{(1-(m^2T)^2)^{1/2}}{1-m^2T} \cdot \frac{(1-T^2)^{1/2}}{1-T}\right)^{(2^hA^h+1)B^h/2} \cdot \left(\frac{(1-(mT)^2)^{1/2}}{1-mT}\right)^{(1-2^hA^h)B^h}. \tag{6.2.3.6}$$

Comparison to characteristic zero

In Subsection 4.2.3 we had Equation 4.2.3.1, for a field K' of characteristic zero:

$$\zeta_{L_m,\mathbb{P}^1_{K',0}}(T) = \frac{1}{(1-m^2T)(1-T)}.$$

In Subsection 6.2.3 we distinguished between several cases again. We recall that s denotes the multiplicative order of m in $\mathbb{F}_p$, and $A := |m^s - 1|_p$, also $B := |m+1|_2$ when $p = 2$ and m is odd. If s is even, then $t = s/2$. As before, it is not possible to express the tame dynamical zeta function in positive characteristic completely in terms of the zeta function in characteristic zero. Instead, we provide an identity which emphasizes the connection as much as possible:

- If $p \mid m$, then

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \frac{(1-(m^2T)^p)^{1/p}}{1-m^2T} \cdot \frac{(1-T^p)^{1/p}}{1-T}.$$

  We substitute the zeta function in characteristic zero where possible:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K',0}}(T^p)^{1/p}}. \tag{6.2.3.7}$$

- If $p \neq 2$, $p \nmid m$ and s is odd, then

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{(1-(m^2T)^{ps})^{1/p}}{1-(m^2T)^s} \left(\frac{1-(mT)^s}{(1-(mT)^{ps})^{1/p}} \right)^2 \frac{(1-T^{ps})^{1/p}}{1-T^s} \right)^{(A^h-1)/2s} \cdot \frac{(1-(m^2T)^p)^{1/p}}{1-m^2T} \frac{(1-T^p)^{1/p}}{1-T}.$$

  As we did before, we will now rewrite this:

$$\zeta^*_{\mathbb{P}^1_{K',0},L_m}(T) = \left(\frac{\zeta_{L_{m^s},\mathbb{P}^1_{K',0}}(T^s)}{\zeta_{L_{m^{ps}},\mathbb{P}^1_{K',0}}(T^{ps})^{1/p}} \left(\frac{1-(mT)^s}{(1-(mT)^{ps})^{1/p}} \right)^2 \right)^{(A^h-1)/2s} \cdot \frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K,0}}(T^p)^{1/p}}. \tag{6.2.3.8}$$

- We get a special case if $m \equiv 1 \mod p$, then

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\frac{(1-(m^2T)^p)^{1/p}}{1-m^2T} \frac{(1-T^p)^{1/p}}{1-T} \right)^{(A^h+1)/2} \left(\frac{1-mT}{(1-(mT)^p)^{1/p}} \right)^{A^h-1}.$$

  And we repeat this process:

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K',0}}(T^p)^{1/p}} \right)^{(A^h+1)/2} \left(\frac{1-mT}{(1-(mT)^p)^{1/p}} \right)^{A^h-1}. \tag{6.2.3.9}$$

- If $p \neq 2$, $p \nmid m$ and s is even, then

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{(1-(m^2T)^{pt})^{1/p}}{1-(m^2T)^t} \left(\frac{(1-(mT)^{pt})^{1/p}}{1-(mT)^t} \right)^2 \frac{(1-T^{pt})^{1/p}}{1-T^t} \right)^{(A^h-1)/2t} \cdot \left(\frac{(1-(m^2T)^{2pt})^{1/p}}{1-(m^2T)^{2t}} \frac{(1-T^{2pt})^{1/p}}{1-T^{2t}} \right)^{(A^h-1)/2t} \cdot \frac{(1-(m^2T)^p)^{1/p}}{1-m^2T} \frac{(1-T^p)^{1/p}}{1-T}.$$

Again, we obtain a similar identity:

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K',0}}(T^p)^{1/p}} \right)^{(A^h-1)/2} \left(\frac{(1-(mT)^{pt})^{1/p}}{1-(mT)^t} \right)^{A^h-1} \cdot \left(\frac{\zeta_{L_{m^{2t}},\mathbb{P}^1_{K',0}}(T^{2t})}{\zeta_{L_{m^{2pt}},\mathbb{P}^1_{K',0}}(T^{2pt})^{1/p}} \right)^{(A^h-1)/2t} \cdot \frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K',0}}(T^p)^{1/p}}. \tag{6.2.3.10}$$

- A special case of this is when $m \equiv -1 \mod p$:

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{(1-(m^2T)^p)^{1/p}}{1-(m^2T)} \cdot \frac{(1-T^p)^{1/p}}{1-T} \right)^{(A^h+1)/2} \cdot \left(\frac{(1-(mT)^p)^{1/p}}{1-mT} \right)^{A^h-1} \cdot \left(\frac{(1-(m^2T)^{2p})^{1/p}}{1-(m^2T)^2} \frac{(1-T^{2p})^{1/p}}{1-T^2} \right)^{(A^h-1)/2}.$$

This gives us the following more compact formula:

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K',0}}(T^p)^{1/p}} \right)^{(A^h+1)/2} \cdot \left(\frac{(1-(mT)^p)^{1/p}}{1-mT} \right)^{A^h-1} \cdot \left(\frac{\zeta_{L_{m^2},\mathbb{P}^1_{K',0}}(T^2)}{\zeta_{L_{m^{2p}},\mathbb{P}^1_{K',0}}(T^{2p})^{1/p}} \right)^{(A^h-1)/2}. \tag{6.2.3.11}$$

- If $p = 2$ and m is odd, then

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{(1-(m^2T)^2)^{1/2}}{1-m^2T} \cdot \frac{(1-T^2)^{1/2}}{1-T} \right)^{(2^hA^h+1)B^h/2} \cdot \left(\frac{(1-(mT)^2)^{1/2}}{1-mT} \right)^{(1-2^hA^h)B^h}.$$

Lastly, we find the another identity:

$$\zeta^*_{\mathbb{P}^1_{K,p},L_m}(T) = \left(\frac{\zeta_{L_m,\mathbb{P}^1_{K',0}}(T)}{\zeta_{L_{m^p},\mathbb{P}^1_{K',0}}(T^p)^{1/p}} \right)^{(2^hA^h+1)B^h/2} \cdot \left(\frac{(1-(mT)^2)^{1/2}}{1-mT} \right)^{(1-2^hA^h)B^h}. \tag{6.2.3.12}$$

Relation between $\zeta_{L_m,\mathbb{P}^1_K}$ and the elliptic curve

It is clear that the fixed points of a Lattès map and the corresponding multiplication-by-m map are closely related, as $E_{m^n-1} = \mathrm{Fix}([m]^{\circ n}])$. Unfortunately, it appears impossible to find a endomorphism g to consider the m^n+1-torsion points as a fixed point set of g. We do see that for any field K:

$$\zeta_{L_m,\mathbb{P}^1_K}(T) = \zeta^{1/2}_{[m],E} \cdot \left(\exp\left(\sum_{n=1}^{\infty} \frac{|E_{m^n+1}|}{n} T^n\right)\right)^{1/2}.$$

When K is a field of characteristic $p > 0$, then a similar equality holds for the tame dynamical zeta function:

$$\zeta^*_{L_m,\mathbb{P}^1_{K,p}}(T) = \left(\zeta^*_{[m],E}\right)^{1/2} \cdot \left(\exp\left(\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{|E_{m^n+1}|}{n} T^n\right)\right)^{1/2}.$$

6.2.4 *Additive and subadditive polynomials*

We use the result found in Subsection 5.1.5: $\mathcal{N}_n = d^n p^{v_\phi(f)}$. Again, we will distinguish between a few cases.

***Case 1**: $p \mid f$*

In other words, let f be inseparable. Then it is clear that $f^n - 1$ is separable. We then get $\mathcal{N}_n = d^n$. The tame dynamical zeta function is easily determined.

With this identity we determine the log of the tame dynamical zeta function:

$$\log \zeta^*_{f,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n = \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n}{n} T^n = \log\left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\right).$$

This gives us the tame dynamical zeta function:

$$\zeta^*_{T^d,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \frac{(1-(dT)^p)^{1/p}}{1-dT}. \qquad (6.2.4.1)$$

***Case 2**: $p \nmid f$*

Let s be the multiplicative order of f in the residue field $k\langle\phi\rangle/\phi k\langle\phi\rangle$. Note that, as $s \mid p-1$, the multiplicative order s must be coprime to p. Then $f^n - 1 \notin \phi k\langle\phi\rangle$ if and only if $s \nmid n$. For n not divisible by p we get $v_p(n) = 0$, and hence:

$$\mathcal{N}_n = \begin{cases} d^n & \text{if } s \nmid n; \\ d^n p^{v_\phi(f^s-1)} & \text{if } s \mid n. \end{cases}$$

We define $A := p^{v_\phi(f^s-1)}$. We can compute the tame dynamical zeta function now:

$$\begin{aligned}
\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\mathcal{N}_n}{n} T^n &= \sum_{\substack{n=1,\\ p\nmid n, s|n}}^{\infty} \frac{d^n A}{n} T^n + \sum_{\substack{n=1,\\ p\nmid n, s\nmid n}}^{\infty} \frac{d^n}{n} T^n \\
&= \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{d^{sk} A}{sk} T^{sk} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n}{n} T^n - \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{d^{sk}}{sk} T^{sk} \\
&= \frac{A-1}{s} \sum_{\substack{k=1,\\ p\nmid k}}^{\infty} \frac{((dT)^s)^k}{k} + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{d^n}{n} T^n \\
&= \frac{A-1}{s} \log\left(\frac{(1-(dT)^{sp})^{1/p}}{1-(dT)^s}\right) + \log\left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\right).
\end{aligned}$$

This allows us to find the tame dynamical zeta function:

$$\zeta^*_{f,\mathbb{G}_{a,\mathbb{F}_p}}(T) = \left(\frac{(1-(dT)^{sp})^{1/p}}{1-(dT)^s}\right)^{(A-1)/s} \cdot \left(\frac{(1-(dT)^p)^{1/p}}{1-dT}\right). \qquad (6.2.4.2)$$

6.3 RESULTS REGARDING THE TAME DYNAMICAL ZETA FUNCTION

To place the computations of the previous section in some context we focus on two aspects. The first regards the fact that the tame dynamical zeta function is algebraic over $\mathbb{Q}(T)$ for the maps we investigated. The second focuses on the lifting of maps and how we can see the the relation between the tame dynamical zeta function in positive characteristic and its corresponding dynamical zeta function in characteristic zero.

6.3.1 *Proof of theorem on algebraicity*

In the previous section we gathered all computations. These allow us to prove the following:

Theorem (Theorem 6.1.2)**.** *Let K be a field of characteristic $p > 0$, and let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a morphism of degree at least 2. If f is a power map, Chebyshev polynomial, Lattès map induced by a multiplication-by-m map or a (sub)additive polynomial, then the tame dynamical zeta function $\zeta^*_{\mathbb{P}^1_K,f}(T)$ is algebraic over $\mathbb{Q}(T)$.*

We first adjust Proposition 4.2.2 for the tame dynamical zeta function to exclude a few points, e.g. zero and/or infinity.

Proposition 6.3.1. *Let S be a set and $f : S \to S$, such that #Fix(f) is finite. For any subset $F \subset$ Fix$(f) \subset S$ such that $F \cap \cup_{k=0}^{\infty}(S - F) = \emptyset$, the following holds:*

$$\zeta^*_{S,f}(T) = \left(\frac{(1-T^p)^{1/p}}{1-T}\right)^{\#F} \cdot \zeta_{S-F,f}(T).$$

Proof. The proof is completely analogous to the proof of Proposition 4.2.2. We can write $f_F : F \to F$ and $f_{S-F} : S - F \to S - F$. Observe that $\#\mathrm{Fix}(f^{\circ n}) = \#\mathrm{Fix}(f_F^{\circ n}) + \#\mathrm{Fix}(f_{S-F}^{\circ n}) = \#F + \#\mathrm{Fix}(f_{S-F}^{\circ n})$. We can use this to obtain the required identity on zeta functions:

$$\begin{aligned}
\zeta^*_{S,f}(T) &= \exp\left(\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\#\mathrm{Fix}(f^{\circ n})}{n} T^n\right) = \exp\left(\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\#F + \#\mathrm{Fix}(f_{S-F}^{\circ n})}{n} T^n\right) \\
&= \exp\left(\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\#F}{n} T^n + \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\#\mathrm{Fix}(f_{S-F}^{\circ n})}{n} T^n\right) \\
&= \exp\left(\#F \sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{1}{n} T^n\right) \cdot \exp\left(\sum_{\substack{n=1,\\ p\nmid n}}^{\infty} \frac{\#\mathrm{Fix}(f_{S-F}^{\circ n})}{n} T^n\right) \\
&= \left(\frac{(1-T^p)^{1/p}}{1-T}\right)^{\#F} \cdot \zeta^*_{S-F,f}(T).
\end{aligned}$$

□

We will now start the proof of Theorem 6.1.2.

Proof of Theorem 6.1.2. First let f be a power map, so $f(x) = x^m$ for some $m > 1$. It is clear that 0 and ∞ are fixed by f. Moreover, if $y \in f^{-1}\{0, \infty\}$, then $y \in \{0, \infty\}$. Hence, we apply Proposition 6.3.1:

$$\zeta^*_{\mathbb{P}^1_p, f}(T) = \left(\frac{(1-T^p)^{1/p}}{1-T}\right)^2 \cdot \zeta^*_{\mathbb{G}_{m,\mathbb{F}_p}, f}(T).$$

It is clear that the first factor is algebraic. The latter is algebraic when $p \mid m$ (Equation 6.2.1.1), when $p \neq 2$ and $p \nmid m$ (Equation 6.2.1.2) and when $p = 2$ and $p \nmid m$ (Equation 6.2.1.4). Now let f be a Chebyshev polynomial. This time we observe that ∞ is an isolated fixed point. With Proposition 6.3.1 we get:

$$\zeta^*_{\mathbb{P}^1_p, f}(T) = \frac{(1-T^p)^{1/p}}{1-T} \cdot \zeta^*_{\mathbb{G}_{a,\mathbb{F}_p}, f}(T). \qquad (6.3.1.1)$$

The first factor is clearly algebraic. The second factor is algebraic when $p \mid d$ (Equation 6.2.2.1), when $p \neq 2$, $p \nmid d$ and $2 \nmid s$ (Equation 6.2.2.2), when $p \neq 2$, $p \nmid d$ and $2 \mid s$ (Equation 6.2.2.4), and when $p = 2$ and $p \nmid m$ (Equation 6.2.2.5). Now let f be a Lattès map induced by the multiplication-by-m map $[m]$. The tame dynamical zeta function is algebraic when $p \mid d$ (Equation 6.2.3.1), when $p \neq 2$, $p \nmid d$ and $2 \nmid s$ (Equation 6.2.3.2), when $p \neq 2$, $p \nmid d$ and $2 \mid s$ (Equation 6.2.3.4), and when $p = 2$ and $p \nmid m$ (Equation 6.2.3.6). □

Remark. Our results show that the tame dynamical zeta function is algebraic, even when the full dynamical zeta turned out to be transcendental (Theorem 5.1.1). This suggests that the tame dynamical zeta function can be an alternative. No general results have been proven, hence it is unclear whether this would work for more general maps, e.g. $x \to x^2 + 1$. But as we do not even know if the full dynamical zeta function is transcendental in a general setting, offering an alternative might be premature.

6.3.2 *Lifting properties of the tame dynamical zeta function*

We first remark that (sub)additive polynomials do not occur as a dynamically affine map over fields of characteristic zero, hence they are not of interest in this section.

For power maps, Chebyshev polynomials and Lattès maps over positive characteristic there is a natural way to lift these to characteristic zero. For Chebyshev polynomials and power maps in characteristic zero, it is clear that these maps are defined over $\mathbb{Z}$, hence considering them over a field of positive characteristic is done by looking at the coefficients reduced modulo p.

As Chebyshev polynomials and power maps are uniquely determined by their degree, it is clear that we can uniquely lift any Chebyshev polynomial f of degree d over positive characteristic to a Chebyshev polynomial $\widetilde{f}$ over a field of characteristic zero of degree d (any field of characteristic zero contains a unique subring additively generated by the multiplicative identity isomorphic to $\mathbb{Z}$). Analogously, any power map over positive characteristic can be uniquely lifted to one over a field of characteristic zero.

For Lattès maps there is a lot to be considered when trying to lift such maps. Note that the (tame) dynamical zeta function over positive characteristic does not depend on the specific elliptic curve, but only on whether it is supersingular or ordinary. Over characteristic zero the dynamical zeta function does not depend on the elliptic curve nor its field of definition at all. Hence, to lift the Lattès map L_m, we first remark that any lift of an elliptic curve E over a field of positive characteristic to an elliptic curve $\widetilde{E}$ over any field of characteristic zero will suffice. Deuring's lifting theorem (Theorem 14 in §15 of Chapter 13 in [Lan73]) gives us a proper lift: an elliptic curve $\widetilde{E}$ over a field of characteristic zero which reduces to E. Also, the map $[m]$ is lifted to some map $\widetilde{[m]}$ over $\widetilde{E}$. As the group operation needs to be respected by the lift, we know that $\widetilde{[m]}$ is the multiplication-by-m map on $\widetilde{E}$. Taking the quotient under the relation $P \sim -P$ as described in Section 4.2.3 is defined for elliptitc curves over fields of arbitrary characteristic. We obtain a lift of L_m over positive characteristic given by $L_{\widetilde{m}} = \widetilde{L_m}$.

We are interested in how we can view the tame dynamical zeta function of a function f as a 'function' in the dynamical zeta function of its lift $\tilde{f}$. To make this precise, we introduce the following notion:

Definition 6.3.2. Let $f : X \to X$ be a power map, Chebyshev polynomial or Lattès map induced by a multiplication-by-m map, with X equal to $\mathbb{P}^1_{K,p}(\overline{K})$, $\mathbb{G}_{m,\mathbb{F}_p}(\overline{K})$ or $\mathbb{G}_{a,p}(\overline{K})$. Then we call $\widetilde{X}$ the **lift** of X and $\widetilde{f} : \widetilde{X} \to \widetilde{X}$ the **lift** of f, both defined by the construction above. Moreover, we call the tame dynamical zeta function $\zeta^*_{X,f}(T)$ **expressible over its lift** if

$$\zeta^*_{X,f}(T) = P(\zeta_{widetildef^{\circ i_1},\tilde{X}}(T^{j_1}), \dots, \zeta_{\widetilde{f}^{\circ i_\ell},\tilde{X}}(T^{j_\ell})),$$

where $P(x_1, \dots, x_\ell)$ is an algebraic function over $\mathbb{Q}(x_1, \dots, x_\ell)$ and $i_1, \dots, i_\ell, j_1, \dots, j_\ell \in \mathbb{Z}$.

In the last section we looked at whether a dynamically affine map is expressible over its lift, we summarize all results in the following theorem:

Theorem 6.3.3. *Let K be a field of characteristic $p > 0$, and let $f : X \to X$ be a power map, Chebyshev polynomial or Lattès map induced by a multiplication-by-m map, with X equal to $\mathbb{P}^1_{K,p}(\overline{K}), \mathbb{G}_{m,\mathbb{F}_p}(\overline{K})$ or $\mathbb{G}_{a,p}(\overline{K})$. Then $\zeta^*_{f,X}(T)$ is expressible over its lift if f is one of the following:*

i. Power map $x \to x^m$ on $\mathbb{G}_{m,\mathbb{F}_p}(\overline{K})$;

ii. Chebyshev polynomial T_d on $\mathbb{G}_{a,\mathbb{F}_p}(\overline{K})$, with $p \mid d$;

iii. Chebyshev polynomial T_d on $\mathbb{G}_{a,\mathbb{F}_p}(\overline{K})$, with $p = 2$, and $d \equiv 3 \mod 4$;

iv. Lattès map L_m on $\mathbb{P}^1_{K,p}(\overline{K})$, with $p \mid m$.

However, $\zeta^*_{f,X}(T)$ is not expressible over its lift if f is one of the following:

v. Chebyshev polynomial T_d on $\mathbb{G}_{a,\mathbb{F}_p}(\overline{K})$, with $p \nmid d$ and $p \neq 2$;

vi. Chebyshev polynomial T_d on $\mathbb{G}_{a,\mathbb{F}_p}(\overline{K})$, with $p = 2$, and $d \equiv 1 \mod 4$;

vii. Lattès map L_m on $\mathbb{P}^1_{K,p}(\overline{K})$, with $p \nmid m$.

Proof. We will prove this case by case, mainly referring to the equations we found in the previous section.
i. If f is a power map, then we can see that it is a (fractional) power of a rational function in $\zeta_{\widetilde{f},\mathbb{P}^1_{K',0}}$ when $p \mid m$ (Equation 6.2.1.5), when $p \neq 2$ and $p \nmid m$ (Equation 6.2.1.6) and when $p = 2$ and $p \nmid m$ (Equation 6.2.1.8).
ii. If $f = T_d : \mathbb{G}_{a,\mathbb{F}_p} \to \mathbb{G}_{a,\mathbb{F}_p}$ is a Chebyshev polynomial with $p \mid d$, then we can see that the statements holds in Equation 6.2.2.6.
iii. If $f = T_d : \mathbb{G}_{a,\mathbb{F}_p} \to \mathbb{G}_{a,\mathbb{F}_p}$ is a Chebyshev polynomial with $p = 2$ and $d \equiv 3 \mod 4$, then $A = |d-1|_2 = 1/2$. We set $A = 1/2$ in Equation 6.2.2.10:

$$\begin{aligned}\zeta^*_{T_d,\mathbb{G}_{a,\mathbb{F}_p}}(T) &= \left(\frac{\zeta_{T_d,\mathbb{G}_{a,K',0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K,0}}(T^p)^{1/p}}\right)^{(2\cdot 1/2+1)B/2} \cdot \left(\frac{(1-T^p)^{1/p}}{1-T}\right)^{(1-2\cdot 1/2)B/2} \\ &= \left(\frac{\zeta_{T_d,\mathbb{G}_{a,K',0}}(T)}{\zeta_{T_{d^p},\mathbb{G}_{a,K',0}}(T^p)^{1/p}}\right)^{B}.\end{aligned} \tag{6.3.2.1}$$

Hence, the statement holds.
iv. If $f = L_m : \mathbb{P}^1_{K,p} \to \mathbb{P}^1_{K,p}$ with $p \mid m$, then Equation 6.2.3.7 clearly confirms the statement.

v. If $f = T_d : \mathbb{G}_{a,\mathbb{F}_p} \to \mathbb{G}_{a,\mathbb{F}_p}$ is a Chebyshev polynomial with $p = 2$ and $p \nmid d$, then we can only partially express the tame dynamical zeta function in the required way, as we saw in Equations 6.2.2.6, 6.2.2.7 and 6.2.2.9. Note that the factor(s) we are left with has a rational factor in T, not in dT. As $A < 1$ and $B \neq 0$ it is clear that this last factor cannot disappear.

vi. If $f = T_d : \mathbb{G}_{a,\mathbb{F}_p} \to \mathbb{G}_{a,\mathbb{F}_p}$ is a Chebyshev polynomial with $p = 2$ and $d \equiv 1 \mod 4$, then $A = |d-1|_2 < 1/2$. This means that $1 - 2A \neq 0$ in Equation 6.2.2.10, and as $B \neq 0$ we know this last factor cannot disappear.

vii. If $f = L_m : \mathbb{P}^1_{K,p} \to \mathbb{P}^1_{K,p}$ is a Lattès map with $p \nmid m$, then we can partially express certain factors of the tame dynamical zeta function in the required way, as we saw in Equations 6.2.3.7, 6.2.3.8, 6.2.3.10 and 6.2.3.12. Note that we always have a factor left of the form

$$\left(\frac{(1-(mT)^{pt})^{1/p}}{1-(mT)^t}\right)^{A^h-1},$$

with a slight abuse of notation we set $t = 1$ for the cases no t occurred. Clearly, no such factor exists in

$$\zeta_{L_m,\mathbb{P}^1_{K',0}}(T) = \frac{1}{(1-m^2T)(1-T)}.$$

This factor can only disappear if $A^h - 1 = 0$, which cannot happen as $h = 1, 2$ and $A < 1$. □

Remark. Because the tame dynamical zeta function is algebraic (Theorem 6.1.2) one might expect that the behaviour is similar to that of the dynamical zeta function of its lift in characteristic zero. This suspicion is confirmed for power maps, but contradicted by the results for (most) separable Chebyshev polynomials and all separable Lattès maps. It is possible that there is another way of interpreting the functions, but it is not as straightforward as it was for power maps.

7

FUTURE RESEARCH QUESTIONS

In this thesis, we studied the behaviour of dynamical systems on varieties defined over a field K, of both characteristic zero and of positive characteristic. We have investigated this problem in roughly three ways: first we looked at results over a field K of characteristic zero and analyzed which steps of the proofs did or did not rely on the characteristic of the ground field; secondly we looked at the behaviour of certain specific maps on algebraic varieties over fields of positive characteristic; lastly, we investigated the possibility of an alternative: the tame dynamical zeta function. We now discuss some opportunities for further study.

7.1 PRODUCT OF RATIONAL FUNCTIONS

In Chapter 4 we saw that the dynamical zeta function of a rational map on $\mathbb{P}^1_K$, with K a field of characteristic zero, is a finite product of rational functions. We can ask ourselves the following question:

> **Q:** *Is there an expression of the zeta function of a rational map on $\mathbb{P}^1_K$, with K a field of arbitrary characteristic, as a (possibly infinite, but convergent) product of rational functions?*

When K has characteristic zero, we saw that the answer is yes (Theorem 4.1.13). Many steps were independent of the characteristic. The most notable that *did* depend on the characteristic was the following:

Lemma 7.1.1 (4.1.12)**.** *Let $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ be a rational map of degree $d \geq 2$, with K a field of characteristic zero. Then the cardinality of the set*

$$\mathcal{P} := \{P \in \mathbb{P}^1_K(\overline{K}) \mid \exists n \in \mathbb{Z}_{\geq 1}, \exists q \in \mathbb{Z}_{\geq 1} \text{ such that } f^{\circ n}(P) = P \text{ and } \lambda(f;P)^q = 1\}$$

is finite.

Over fields of positive characteristic this is generally untrue, e.g. if $\overline{K} = \overline{\mathbb{F}}_p$. As all nonzero elements are roots of unity, the condition of $\lambda(f;P)^q = 1$ for some q can be omitted. Then this set consists of all periodic points, which can easily be infinite. In the proof of Theorem 4.1.13 we saw that a partition of $\mathcal{P}$ corresponds to factors of the dynamical zeta function.

It would be interesting to partition $\mathcal{P}$ in a different way over a general field: perhaps an infinite number of finite subsets, which also corresponds with an infinite product (indeed, we do not expect rationality, as demonstrated in Chapter 5), which may give us more insight in the dynamical zeta function.

7.2 TRANSCENDENCE IN POSITIVE CHARACTERISTIC

Again, we can ask ourselves a compelling question:

> **Q:** *When is the dynamical zeta function of a separable endomorphism on an abelian variety transcendental?*

We obtained pleasing results for endomorphisms on elliptic curves in Theorem 5.2.14 and for multiplication-by-m maps on abelian varieties in Theorem 5.2.7. The only obstruction to finding a similar result for all endomorphisms of degree at least two on abelian varieties, was that it is unclear how to relate the inseparable degree of an isogeny $f^n - 1$ to the valuation $v_p(n)$. We need this to apply automata theory in the same way as Bridy.

Unlike for elliptic curves, higher dimensional abelian varieties may have endomorphism algebras where the inseparable isogenies do not form an ideal. For example: consider the abelian variety $E \times E'$, where E and E' are elliptic curves over a field of characteristic 2 and consider the maps $[2] \times \mathrm{id}$ and $\mathrm{id} \times [2]$; they are both inseparable, but the sum $[3] \times [3]$ is separable.

Perhaps there is a different way of finding out more about $\deg_i(f^n - 1)$. We could ask ourselves:

> **Q:** *Given that* $f - 1$ *is inseparable, can we write* $\deg_i(f^n - 1)$ *as an explicit function depending only on the variety* A*, the map* f *and* $v_p(n)$*?*

We expect the formula to depend on constants like the p-rank and dimension of the variety, but any constant depending on the variety or on f that is included in the formula will most likely not pose a problem for the structure of transcendence proofs.

It might be worth studying simple abelian varieties first as that would entail eliminating maps like the example mentioned. Later one could look at products of simple abelian varieties, where we might need to consider maps that operate on each simple abelian variety separately, and later consider even more complicated maps. Also, once we have a good understanding of what happens for abelian varieties, it is natural to consider algebraic groups next, as abelian varieties are a subcategory of algebraic groups.

7.3 TAME DYNAMICAL ZETA FUNCTION

Let us start with another question:

> **Q:** *When is the tame dynamical zeta function of a rational map* $f : \mathbb{P}^1_K \to \mathbb{P}^1_K$ *algebraic?*

We know that for dynamically affine maps the tame dynamical zeta function is indeed algebraic. However, we used that we could actually write down formulas for the number of fixed points. At the moment it is not obvious whether this would hold for general rational maps on $\mathbb{P}^1_K$. Also, we should consider expanding to other algebraic varieties, such as:

Q: *Is the tame dynamical zeta function of endomorphisms on abelian varieties algebraic?*

We already found several formulas; especially for multiplication-by-m maps it should not be difficult to check this. For general endomorphism it might turn out to be more complicated than for endomorphisms on elliptic curves because a norm function enters the formula.

One might also consider looking at a map f and its tame dynamical zeta function and the dynamical zeta function of its lifts $\widetilde{f}$ to characteristic zero. Note that there is not always a canonical choice of a lift. For power maps we observed that the tame dynamical zeta function can be written using the dynamical function of its lift: 6.2.1.6:

$$\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T) = \frac{\zeta_{x^m,\mathbb{G}_{m,K,0}}(T)}{\zeta_{x^{mp},\mathbb{G}_{m,K,0}}(T^p)^{1/p}} \cdot \left(\frac{\zeta_{x^{m^s},\mathbb{G}_{m,K,0}}(T^s)}{\zeta_{x^{m^{ps}},\mathbb{G}_{m,K,0}}(T^{ps})^{1/p}} \right)^{(A-1)/s},$$

We say that $\zeta^*_{x^m,\mathbb{G}_{m,\mathbb{F}_p}}(T)$ is *expressible over its lift* and we know that such a pattern cannot always be detected as easily (Theorem 6.3.3). We ask ourselves the question:

Q: *When is the tame dynamical zeta function expressible over its lift?*

Now it appears that we can always recognize the dynamical zeta function of the lift as a factor in the tame dynamical zeta function. Does this hold in general? It is compelling to first look at examples coming from algebraic groups, but simple maps such as $x \to x^2 + 1$, might also prove to be very insightful.

BIBLIOGRAPHY

[AM65] Michael Artin and Barry Mazur. On periodic points. *Ann. of Math. (2)*, 81:82–99, 1965.

[AS03] Jean-Paul Allouche and Jeffrey Shallit. *Automatic sequences*. Cambridge University Press, Cambridge, 2003. Theory, applications, generalizations.

[Bri12] Andrew Bridy. Transcendence of the Artin-Mazur zeta function for polynomial maps of $\mathbb{A}^1(\overline{\mathbb{F}}_p)$. *Acta Arith.*, 156(3):293–300, 2012.

[Bri16] Andrew Bridy. The Artin-Mazur zeta function of a dynamically affine rational map in positive characteristic. *J. Théor. Nombres Bordeaux*, 28(2):301–324, 2016.

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[Hin94] Aimo Hinkkanen. Zeta functions of rational functions are rational. *Ann. Acad. Sci. Fenn. Ser. A I Math.*, 19(1):3–10, 1994.

[Lan73] Serge Lang. *Elliptic functions*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Amsterdam, 1973. With an appendix by J. Tate.

[Lee15] Junghun Lee. The Artin-Mazur zeta functions of certain non-Archimedean dynamical systems. *ArXiv e-prints*, May 2015.

[Mil06] John Milnor. *Dynamics in one complex variable*, volume 160 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, third edition, 2006.

[Mil08] James S. Milne. Abelian varieties (v2.00), 2008. Available at `www.jmilne.org/math/`.

[Mil17] James S. Milne. Algebraic number theory (v3.07), 2017. Available at `www.jmilne.org/math/`.

[MvdG] Ben Moonen and Gerard van der Geer. Abelian varieties. Available at `www.math.ru.nl/~bmoonen/research.html#bookabvar`.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer-Verlag, Berlin, 1992.

[Shi98] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.

[Sil07] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979.

[ZS60] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. II*. The University Series in Higher Mathematics. D. Van Nostrand Co., Inc., Princeton, N. J.-Toronto-London-New York, 1960.