Arithmetic Dynamics of Rational Maps

by
Michelle Manes
A. B., University of California at Berkeley, 1991
Sc. M., Brown University, 2004

Submitted in partial fulfillment of the requirements
for the Degree of Doctor of Philosophy in the
Department of Mathematics at Brown University

Providence, Rhode Island
May, 2007

Contents

Chapter 1

Introduction

In this thesis, we tackle arithmetic questions arising from discrete dynamical systems. The techniques used draw on classical complex dynamics, algebraic number theory, and algebraic geometry.

Nice stuff about history, maybe.

1.1 Discrete dynamical Systems

A discrete dynamical system is simply a set X with a self-map $\phi : X \to X$, allowing for iteration. For a non-negative integer n, denote by ϕ^n the nth iterate of ϕ under composition, with ϕ^0 taken to be the identity map. In classical complex dynamics, the set X is the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. More generally for this thesis, let K be a field with algebraic closure $\overline{K}$. Let $\phi : \mathbb{P}^1_{\overline{K}} \to \mathbb{P}^1_{\overline{K}}$ be a morphism defined over K; then we may write $\phi(z) \in K(z)$ as a rational map.

$$\phi(z) = F(z)/G(z), \quad F, G \in K[z], \quad \operatorname{Res}(F, G) \neq 0, \quad \deg \phi = \max\{\deg F, \deg G\}.$$

The (forward) orbit of a point $\alpha \in \mathbb{P}^1$ under ϕ is simply the set of iterates of α,

$$\mathcal{O}_\phi\{\phi^n(\alpha) : n \geq 0\}.$$

A fundamental question in dynamics is to classify points according to their orbits. Some types of points are of particular interest. A point $\alpha \in \mathbb{P}^1$ is *periodic* if there exists an integer $n > 0$ such that $\phi^n(\alpha) = \alpha$, and α is *preperiodic* if there exist integers $n > m \geq 0$ such that $\phi^n(\alpha) = \phi^m(\alpha)$.

$$\begin{aligned}
\operatorname{Fix}(\phi, \mathbb{P}^1) &= \{\text{the set of } \textit{fixed points}\} \\
&= \{\alpha \in \mathbb{P}^1 : \phi(\alpha) = \alpha\} \\
\operatorname{Per}(\phi, \mathbb{P}^1) &= \{\text{the set of } \textit{periodic points}\} \\
&= \{\alpha \in \mathbb{P}^1 : \phi^n(\alpha) = \alpha \text{ for some } n \geq 1\} \\
\operatorname{PrePer}(\phi, \mathbb{P}^1) &= \{\text{the set of } \textit{preperiodic points}\} \\
&= \{\alpha \in \mathbb{P}^1 : \phi^n(\alpha) = \phi^m(\alpha) \text{ for some } n > m \geq 0\} \\
&= \{\alpha \in \mathbb{P}^1 : \mathcal{O}_\phi(\alpha) \text{ is a finite set}\}
\end{aligned}$$

We say P has period n if $\phi^n(P) = P$, and it has *primitive* period n if $n > 0$ is the smallest such integer.

1.2 Arithmetic questions

One type of arithmetic question arising from discrete dynamical systems is the analysis of $\mathrm{PrePer}(\phi, K)$, the preperiodic points of a map $\phi(z) \in K(z)$ lying in the field K. Northcott proved in [17] that for a fixed morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ defined over a number field K, there are at most finitely many preperiodic points in $\mathbb{P}^N(K)$. Lying deeper is the uniform boundedness conjecture of Morton and Silverman (see [15]).

Conjecture 1. *Let $K/\mathbb{Q}$ be a number field of degree D, and let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over K. There is a constant $\kappa(D, N, d)$ such that*

$$\#\,\mathrm{PrePer}(\phi, K) \leq \kappa(D, N, d).$$

This conjecture implies, for example, uniform boundedness for torsion points on abelian varieties over number fields (see [5]). Even the special case $n = 1$ and $d = 4$ is enough to imply Merel's uniform boundedness of torsion points on elliptic curves proved in [9]. Torsion points on elliptic curves are exactly preperiodic points under the multiplication-by-2 map on the curve. Points on the elliptic curve map to $\mathbb{P}^1$ via their x-coordinate, and this multiplication-by-2 map induces a degree-four rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, with the x-coordinates of the torsion points mapping to preperiodic points of ϕ.

Definition 1. *We say that two rational maps ϕ and ψ are* linearly conjugate *if there is some $h \in \mathrm{PGL}_2(\overline{K})$ such that $\phi^h = \psi$. They are* linearly conjugate over K *if there is some $h \in \mathrm{PGL}_2(K)$ such that $\phi^h = \psi$.*

If P is a point of primitive period n for ϕ, then $f^{-1}(P)$ has the same property for ϕ^f, and similarly for preperiodic points. It is also easily seen that $(\phi^n)^f = \left(\phi^f\right)^n$. So linearly conjugate maps have essentially the same dynamical behavior. However, if we are concerned with the arithmetic of the periodic points, we must be a bit more careful.

Let a rational map $\phi(z)$, a point P, and $f \in \mathrm{PGL}_2$ all be defined over K, with $\phi^n(P) = P$. Then both $\psi(z) = \phi^f(z)$ and $Q = f^{-1}(P)$ are defined over K, and $\psi^n(Q) = Q$. However, if f is defined instead over some finite extension of K, it is possible that ψ is still defined over K, but the periodic point Q is not.

Example. Let

$$\phi(z) = 2z + \frac{5}{z} \quad \text{and} \quad \psi(z) = \frac{z^2 - 3z}{3z - 1}.$$

Both rational maps are defined over $\mathbb{Q}$ and have rational fixed points at infinity. The finite fixed points of $\psi(z)$ are also rational; they are $z = -1$ and $z = 0$. The fixed points of $\phi(z)$, however, are

$\pm i\sqrt{5}$. One can check that

$$\phi^f(z) = \psi(z) \quad \text{where} \quad f(z) = \frac{i\sqrt{5}\,(z-1)}{1+z}.$$

1.3 Dynatomic polynomials

To tackle these arithmetic questions, we require algebraic descriptions of periodic and preperiodic points. For any $\phi(z) \in K(z)$, we create a homogeneous polynomial $\Phi_{n,\phi}(x,y) \in K[x,y]$ whose roots are precisely points of period n for ϕ. If we homogenize $\phi(z) = \phi(x,y) = [F(x,y) : G(x,y)]$ and write $\phi^n(x,y) = [F_n(x,y) : G_n(x,y)]$, then

$$\Phi_{n,\phi}(x,y) = yF_n(x,y) - xG_n(x,y).$$

If $P = [x : y]$ is a root of this polynomial, then by construction $\phi^n(P) = P$.

The polynomial Φ_n has as its roots all points of period n, including those of primitive period $k < n$ but satisfying $k \mid n$. We would like to examine points of primitive period n, so we define the nth *dynatomic polynomial* for ϕ by

$$\Phi^*_{n,\phi}(x,y) = \prod_{k|n} \left(\Phi_{k,\phi}(x,y)\right)^{\mu(n/k)} = \prod_{k|n} \left(yF_k(x,y) - xG_k(x,y)\right)^{\mu(n/k)}, \tag{1.1}$$

where μ is the Moebius mu function. (To ease notation, we will write simply Φ_n and Φ^*_n unless the distinction is needed.) It is not clear *a priori* that $\Phi^*_n(x,y)$ is a polynomial, but this is in fact the case. Morton and Silverman prove in [16] that $\Phi_{n,\phi}$ is an effective 0-cycle for $\phi : X \to X$, where X is a curve or ϕ is an automorphism of $\mathbb{P}^n$. In his thesis, Hutz [**?**] has extended this to X an irreducible, nonsingular projective variety of arbitrary dimension. The roots of $\Phi^*_n(x,y)$ are points of *formal* period n, which include all points of primitive period n.

1.4 Quadratic polynomials

Let $\phi(z) \in K[z]$ be a quadratic polynomial, and assume that $\operatorname{char} K \neq 2$. Then $\phi(z)$ is linearly conjugate over K to some map $f_c(z) = z^2 + c$ with $c \in K$. To see this, write

$$\phi(z) = Az^2 + Bz + C, \quad A, B, C \in K.$$

Conjugating by $h(z) = (2z - B)/(2A) \in \mathrm{PGL}_2(K)$, we get

$$\phi^h(z) = z^2 + \underbrace{\left(AC - \frac{1}{4}B^2 + \frac{1}{2}B\right)}_{c \in K}.$$

Thus, studying the dynamics of quadratic polynomials — including the arithmetic dynamics of these maps — reduces to studying the dynamics of the one-parameter family $f_c(z) = z^2 + c$. This

is certainly the most-studied family of rational maps. The famous Mandelbrot set is a c-parameter plane for f_c, describing the fate of $\mathcal{O}_{f_c}(0)$.

We now summarize some of the arithmetic results known for the family f_c. In his thesis, Bousch [3] proved the following.

1. $\Phi^*_{n,f_c}(z) = \Phi^*_n(z,c) \in \mathbb{Z}[z,c]$, and this polynomial is irreducible for every n.

2. The affine curve $Y_1(n)$ given by $\Phi^*_n(z,c) = 0$ is smooth.

3. Let $X_1(n)$ be the normalization of the projective closure of $Y_1(n)$. Then

$$\text{genus } X_1(n) = 1 + \frac{n-3}{4}\kappa(n) - \frac{1}{4}\sum_{m|n} \phi\left(\frac{n}{m}\right) m\kappa(m)$$

   where $\kappa(n) = \sum_{k|n} \mu(n/k)2^k$ (this is essentially the z-degree of Φ^*_n) and ϕ is the Euler totient function.

Bousch's genus formula shows that $X_1(1)$, $X_1(2)$, and $X_1(3)$ are all rational. So there are one-parameter families of c-values giving maps f_c with rational fixed points, rational points of period 2, and rational points of period 3 respectively.

The genus of $X_1(4)$ is 2, and in [14] Morton shows that this curve is birational to the elliptic modular curve $X_1(16)$, and that it has no finite rational points. In other words, there are no quadratic polynomials defined over $\mathbb{Q}$ with a rational point of primitive period 4. $X_1(5)$ has genus 14. This curve is not modular, but in [7] Flynn, Poonen, and Shaefer show that there are no finite rational points. So there are no quadratic polynomials defined over $\mathbb{Q}$ with a rational point of primitive period 5.

In [18], Poonen conjectures that no quadratic polynomial ϕ defined over $\mathbb{Q}$ has rational points of primitive period $n > 3$. He shows that if this is true, then for such maps,

$$\#\operatorname{PrePer}(\phi, \mathbb{Q}) \leq 9.$$

The set $\operatorname{PrePer}(\phi, K)$ of preperiodic points of ϕ defined over K can be represented by a directed graph, with an arrow from P to $\phi(P)$, and Poonen provides a complete analysis of directed graphs that occur as $\operatorname{PrePer}(\phi, \mathbb{Q})$ for points of primitive period $n \leq 3$ and $\phi \in \mathbb{Q}[x]$ a quadratic polynomial.

1.5 Rational maps with automorphsims

Usually, $\phi^f \neq \phi$ as rational maps, but this is not always the case.

Example. Consider the map $\phi(z) = 2z + \frac{5}{z}$ from the example above, and let $h(z) = -z$. Then

$$\phi^h(z) = -\phi(-z) = \phi(z).$$

Definition 2. *We define the* stabilizer group *(or* automorphism group*) of ϕ to be*

$$\mathrm{Aut}(\phi) = \{f \in \mathrm{PGL}_2 \,|\, \phi^f = \phi\}.$$

One can prove the following three facts:

- If $h \in \mathrm{Aut}(\phi)$, then $f^{-1}hf \in \mathrm{Aut}(\phi^f)$, so linearly conjugate maps have the same stabilizer groups, at least as abstract groups. (The groups are conjugate in PGL_2.)
- $\mathrm{Aut}(\phi)$ must be a finite subgroup of PGL_2; furthermore, if two maps defined over a field K are linearly conjugate, then they must be linearly conjugate over K unless the maps have a nontrivial stabilizer group (see, for example, [20]).
- Most rational maps of degree $d \geq 2$ have no nontrivial automorphisms, in the following sense. Let Rat_d be the parameter space of rational maps of degree d. Rat_d is an affine open subscheme of $\mathbb{P}^{2d+1}_{\mathbb{Z}}$ (see [21] for details). One can show that $\{\phi \in \mathrm{Rat}_d \,|\, \mathrm{Aut}(\phi) \neq \mathrm{id}\}$ is a Zariski-closed subset of Rat_d ([22], exercise 4.38)..

Much of the work in this thesis began with (unsuccessful) attempts to extend Bousch's results to rational maps with a nontrivial PGL_2 automorphism. The results for these maps differ in some striking ways from the results for quadratic polynomials, and the proofs are complicated by the need to consider linear conjugacy over K rather than over $\overline{K}$.

1.6 Summary of results

As mentioned in the previous sections, the set of morphisms $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree d is parametrized by an affine open subset Rat_d of $\mathbb{P}^{2d+1}$, and there is a natural equivalence given by the conjugacy action of PGL_2 on these maps. It is natural, then, to consider the quotient space $M_d = \mathrm{Rat}_d/\mathrm{PGL}_2$. Generalizing work by Milnor in [11], Silverman proved in [21] that M_d exists as an affine integral scheme over $\mathbb{Z}$ and that M_2 is isomorphic to $\mathbb{A}^2_{\mathbb{Z}}$.

In Chapter 2, we consider the moduli space of rational maps of degree d with level-N structure; that is, the space $M_d(N)$ of rational maps of degree d together with a point of formal period N.

Theorem 1. *$M_2(N)$ is geometrically irreducible for every $N > 1$.*

The proof takes advantage of the fact that we have an explicit description of the space M_2. Using a normal form for quadratic rational maps, one may iterate to find polynomial descriptions of the $M_2(N)$ and then specialize and apply a result of Morton to prove irreducibility.

If we consider one-parameter families in M_2, their intersections with the surfaces $M_2(N)$ are algebraic curves. Bousch's result, combined with Bertini's theorem and the fact that the surfaces are irreducible, says that we should expect irreducibility of the period-N curves except possibly on a Zariski-closed subset of M_2.

The main result of Chapter 3, then, is potentially surprising. Let $M_d(N, \boldsymbol{\mu}_m)$ represent the moduli space of (equivalence classes of) rational functions of degree d having an automorphism of order m, together with a marked point of formal period N.

Proposition 1. *$M_2(2n, \boldsymbol{\mu}_2)$ is geometrically reducible for infinitely many n.*

In other words, the period-N curves lying over the family of rational maps of degree 2 with a nontrivial automorphism are reducible infinitely often. Similar results are known for the pure power functions z^d and for the Chebyshev polynomials. In both cases, the result is proved for only one specific function of each degree d. In this case, we have an entire curve in the moduli space M_2. In fact, proposition 1 is actually a corollary of a more general result.

Theorem 2. *Let p be prime. $M_d(pn, \boldsymbol{\mu}_p)$ is reducible for infinitely many n.*

The proof is constructive, providing a particular proper closed subvariety of $M_d(pn, \boldsymbol{\mu}_p)$. The difficulty of the proof lies in first defining the appropriate object, and then proving that the object is in fact a variety, which is not at all obvious from the definition.

The construction gives a geometric explanation for reducibility when a rational map ϕ has a nontrivial automorphism: If P is a point of formal period N, then $h(P)$ must be as well for $h \in \mathrm{Aut}(\phi)$. There are two possible cases if the order of h divides N: either P and $h(P)$ are on the same orbit, or the action of h interchanges the separate orbits of P and $h(P)$. The moduli space has at least two components, corresponding to these two possibilities.

In Chapter 4, we take up the search for rational maps with a rational N cycle — the question at the heart of Conjecture 1. This is equivalent to the search for rational points in the moduli space $M_2(N)$. In the case of maps with a nontrivial automorphism, the situation is complicated by the existence of nontrivial twists of the maps; that is, the existence of maps that are linearly conjugate over $\mathrm{PGL}_2(\overline{\mathbb{Q}})$, but not linearly conjugate over $\mathrm{PGL}_2(\mathbb{Q})$. It is necessary, then, to first establish a normal form akin to the $f_c = z^2 + c$ form for quadratic polynomials.

Lemma 1. *Let K be a field with $\mathrm{char}(K) \neq 2, 3$ and let ϕ be a rational map of degree 2 defined over K. Then $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$ if and only if ϕ is linearly conjugate over K to some map of the form*

$$\phi_{k,b}(z) = kz + \frac{b}{z} \tag{1.2}$$

with $k \in K \smallsetminus \{0, -1/2\}$ and $b \in K^*$. Furthermore, two such maps $\phi_{k,b}$ and $\phi_{k',b'}$ are linearly conjugate over K if and only if $k = k'$ and $b/b' \in (K^*)^2$.

We are then able to adapt the methods of Morton in [14] and of Flynn, Poonen, and Schaefer in [7] to prove the following.

Theorem 3. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be morphism of degree 2 defined over $\mathbb{Q}$, and suppose that $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$. Then*

(a) ϕ has at least one rational fixed point.

(b) There is a one-parameter family of maps such that ϕ has exactly three rational fixed points. No such map has exactly two rational fixed points.

(c) There is another one-parameter family of maps such that ϕ has a rational point of primitive period 2.

(d) No such rational maps have a rational point of primitive period 3*.*

(e) There is a one-parameter family of maps such that ϕ has a rational point of period 4*. These maps have exactly four such rational points.*

(f) No such rational maps have more than four rational points of primitive period 4*.*

Finally, we provide evidence that no such maps have rational points of primitive period 5 or 6. Summarizing, we have a conjecture similar to the one proposed for the polynomial family $f_c(z) = z^2 + c$ in [7].

Conjecture 2. *If $\phi(z) \in \mathbb{Q}(z)$ is a degree-2 rational map with $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$, then ϕ has no rational point of exact period $N > 4$.*

These results are in contrast with the case of quadratic polynomials, where it is known that there exists a one-parameter family of maps having rational points of period 3, and there are no $\mathbb{Q}$-rational points of primitive period 4 (see [14]) or 5 (see [7]). Evidence suggests that a quadratic polynomial defined over $\mathbb{Q}$ cannot have a rational periodic point of primitive period $N > 3$. The proofs for the case of rational maps with automorphisms are complicated by the need to consider quadratic twists of the maps; quadratic polynomials do not have such twists.

In Section 4.3, we provide a complete analysis of directed graphs that occur as $\mathrm{PrePer}(\phi, \mathbb{Q})$ for degree 2 rational maps with automorphisms. We prove the following theorem.

Theorem 4. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be morphism of degree 2 defined over $\mathbb{Q}$, and suppose that $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$. Then*

$$\#\{P \in \mathbb{Q} | P \textit{ is preperiodic and lands on a cycle of length at most four}\} \leq 12.$$

The complete list of possible directed graphs can be found in Figure 4.1 on page 72. This work is inspired by Poonen's paper [18], in which he provides a complete analysis of directed graphs that occur as $\mathrm{PrePer}(f, \mathbb{Q})$ for points of primitive period $n \leq 3$ and $f \in \mathbb{Q}[x]$ a quadratic polynomial. Specifically, he shows that if a quadratic polynomial f has no rational points of primitive period greater than 3, then (counting the fixed point at infinity) $\#\,\mathrm{PrePer}(f, \mathbb{Q}) \leq 9$.

As Poonen explains in [18], these directed graphs can be thought of as the analogs of possible torsion subgroups for elliptic curves over $\mathbb{Q}$ as classified in Mazur's theorem [8]. Let $\phi(z)$ be a rational map of degree two with $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$ (up to linear conjugacy) and let G be a specific graph of rational preperiodic points. Pairs $(\phi(z), G)$ are parameterized by points on an algebraic curve, just as elliptic curves with given level structure correspond to points on modular curves. Deciding whether a given graph is possible, then, reduces to finding rational points on these algebraic curves.

The particular curves whose rational points we need to determine have genus 0, 1, or 3. The genus 0 and 1 curves have rational points at infinity, so they are respectively $\mathbb{P}^1$ and elliptic curves. The elliptic curves all have small conductor and rank 0, so we are able to list their rational points completely. In the case of the genus 3 curve, it covers an elliptic curve, which unfortunately has

rank 1, so this does not allow us to list completely the (necessarily finitely many) rational points on the curve. However, it also covers a genus 2 curve. We are able to find all of the rational points on the genus 2 curve, and then we use that result to find all of the rational points on the original genus 3 curve.

Poonen's result for quadratic polynomials together with Theorem **??** suggests the following specific version of the Morton and Silverman conjecture.

Conjecture 3. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism of degree 2 defined over $\mathbb{Q}$. Then*

$$\#\operatorname{PrePer}(\phi, \mathbb{Q}) \leq 12.$$

The bound of twelve seems reasonable given the data thus far, with the existence of the totally ramified fixed point at infinity reducing the total by three (a preimage P of the point at infinity, along with two preimages of P) in the case of quadratic polynomials. If the conjecture is true, the bound of 12 would be sharp, since two examples in Section 4.4 give maps with twelve rational preperiodic points.

Chapter 2

Modular curves and surfaces

2.1 Preliminaries

Let X be a variety and $\phi\colon X \to X$ be a morphism defined over some field K. Let

$$\mathrm{Per}_n(\phi) = \{\alpha \in X : \phi^n(\alpha) = \alpha\}$$

be the set of points of period n for ϕ. We define

$$\begin{aligned} \Delta(X) &= \{(x,x) : x \in X\} \subset X \times X && \text{the diagonal, and} \\ \Gamma(\phi^n) &= \{(x, \phi^n(x)) : x \in X\} \subset X \times X && \text{the graph of the morphism } \phi^n. \end{aligned}$$

We can then assign a multiplicity to each $\alpha \in \mathrm{Per}_n(\phi)$ by taking the intersection of the diagonal with $\Gamma(\phi^n)$ in $X \times X$. Following Morton and Silverman in [16], we define the cycle of n-periodic points

$$Z_n(\phi) = \sum_{P \in \mathbb{P}^1} a_P(n) P \stackrel{\text{def}}{=} \Delta \cdot \Gamma(\phi^n), \tag{2.1}$$

and the cycle of primitive n-periodic points

$$Z_n^*(\phi) = \sum_{P \in \mathbb{P}^1} a_P^*(n) P \stackrel{\text{def}}{=} \sum_{k|n} \mu\left(\frac{n}{k}\right) Z_k(\phi), \tag{2.2}$$

where μ is the Möbius mu function. In [16], the authors show that Z_n^* is an effective 0-cycle, and they give a precise description of the points $\alpha \in X$ with $a_n^*(\alpha) > 0$, for X a curve.

If $\alpha \in \mathrm{Per}_n(\phi)$ then ϕ^n induces a map from the cotangent space of X to itself,

$$(\phi^n)^* : \Omega_\alpha(X) \longrightarrow \Omega_\alpha(X).$$

When X is a curve, then the cotangent space has dimension one, so $(\phi^n)^*$ must be multiplication by a scalar, which we call the *multiplier* of the cycle associated to α. When $X = \mathbb{P}^1$, the scalar is exactly $(\phi^n)'(\alpha)$. In particular, for $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$, and for $\alpha \in \mathbb{P}^1$ a fixed point of ϕ — that is, for $\alpha \in \mathrm{Per}_1(\phi)$ — the multiplier of the fixed point is simply $\phi'(\alpha)$.

Note that ϕ will have $d+1$ fixed points, counted with proper multiplicity. When $X = \mathbb{P}^1$ and the fixed points of ϕ are all distinct, then we have an identity on the multipliers of these fixed points. Let $\lambda_1, \cdots, \lambda_{d+1}$ be the multipliers. Then

$$\sum_{i=1}^{d+1} 1/(1-\lambda_i) = 1. \tag{2.3}$$

The requirement that the fixed points are distinct means that none of the λ_i are 1. If the fixed points are not all distinct, a more complicated identity still holds (see [22], Exercise 1.18).

If we fix the variety $X = \mathbb{P}^1$, we may write the morphism $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ using homogeneous coordinates

$$\begin{aligned}\phi(x,y) &= [F_1(x,y) : G_1(x,y)] \\ &= [a_d x^d + a_{d-1}x^{d-1}y \cdots + a_1 x y^{d-1} + a_0 y^d : b_d x^d + b_{d-1}x^{d-1}y \cdots + b_1 x y^{d-1} + b_0 y^d],\end{aligned}$$

for some polynomials $F_1, G_1 \in K[x,y]$ with no common factors, and $\deg \phi = \deg F_1 = \deg G_1$. Of course, for any $u \in \overline{K}^*$, uF_1 and uG_1 define the same rational map ϕ. We therefore identify each ϕ with a unique point in $\mathbb{P}^{2d+1}$ via

$$\phi \longmapsto [a_d : a_{d-1} : \cdots : a_0 : b_d : b_{d-1} : \cdots b_0].$$

The requirement that F_1 and G_1 share no common factors means, however, that not every point in $\mathbb{P}^{2d+1}$ corresponds to a map of degree d.

The *resultant* of two polynomials F and G is a polynomial in the coefficients of F and G with the property that $\mathrm{Res}(F,G) = 0$ if and only if F and G have a common zero in $\mathbb{P}^1$. (See, for example, Proposition 2.13 of [22] for details.) So the space of rational maps of degree d corresponds to an affine variety (the complement of a hyperplane):

$$\mathrm{Rat}_d = \mathbb{P}^{2d+1} \smallsetminus \{\mathrm{Res}(F_1, G_1) = 0\}.$$

We allow elements of $\mathrm{PGL}_2(\overline{K})$ to act on $\mathbb{P}^1$ as fractional linear transformations in the usual way. For $h \in \mathrm{PGL}_2$ we define $\phi^h = h^{-1}\phi h$. This conjugacy has two agreeable properties related to dynamical systems.

1. It respects iteration. That is,
$$(\phi^n)^h = \left(\phi^h\right)^n.$$

2. If P is a periodic (or preperiodic) point of ϕ, then $h^{-1}(P)$ exhibits the same behavior for ϕ^h.

So linearly conjugate maps have essentially the same dynamical behavior. It is natural, then, to consider the quotient space

$$M_d = \mathrm{Rat}_d \,/\, \mathrm{PGL}_2\,.$$

Generalizing work by Milnor in [11], Silverman proved in [21] that M_d exists as an affine integral scheme over $\mathbb{Z}$ and that M_2 is isomorphic to $\mathbb{A}^2_{\mathbb{Z}}$. In fact, if we let $\lambda_1, \lambda_2, \lambda_3$ be the multipliers of the

three fixed points of ϕ (counted with multiplicity), then the first two symmetric functions of these multipliers form natural coordinates for M_2:

$$M_2 = \{(\sigma_1, \sigma_2)\} \quad \text{where} \quad \sigma_1 = \lambda_1 + \lambda_2 + \lambda_3, \quad \text{and} \quad \sigma_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3.$$

Writing $\phi(x, y) = [F_1(x, y), G_1(x, y)]$, we are able to describe iteration: $\phi^n(x, y) = [F_n(x, y) : G_n(x, y)]$ represents ϕ composed with itself n times, where the functions F_n and G_n are defined recursively by

$$F_n(x, y) = F_{n-1}\left(F_1(x, y), G_1(x, y)\right) \quad \text{and} \quad G_n(x, y) = G_{n-1}(F_1(x, y), G_1(x, y)).$$

We now create a homogeneous polynomial $\Phi_{n,\phi}(x, y)$ whose roots are precisely points of period n for ϕ.

$$\Phi_{n,\phi}(x, y) = yF_n(x, y) - xG_n(x, y).$$

If $P = [x : y] \in \mathbb{P}^1$ is a root of this polynomial, then by construction $\phi^n(P) = P$. The 0-cycle $Z_n(\phi)$ in equation (2.1) is then simply a formal sum of the roots of $\Phi_{n,\phi}(x, y)$, counted with multiplicity.

Definition 3. *The nth* dynatomic polynomial *for ϕ is given by*

$$\Phi^*_{n,\phi}(x, y) = \prod_{k|n} \left(\Phi_{k,\phi}(x, y)\right)^{\mu(n/k)} = \prod_{k|n} \left(yF_k(x, y) - xG_k(x, y)\right)^{\mu(n/k)}.$$

The cycle $Z^*_n(\phi)$ in equation (2.2) is a formal sum of the roots of $\Phi^*_{n,\phi}(x, y)$ counted with multiplicity, and the result that Z^*_n is an effective 0-cycle means that $\Phi^*_{n,\phi}(x, y)$ is a polynomial.

We would like to say that the roots of $\Phi^*_{n,\phi}$ are the points in $\mathbb{P}^1$ with *primitive* period n for ϕ. (In other words, the points for which $\phi^n(\alpha) = \alpha$, but $\phi^i(\alpha) \neq \alpha$ for $0 < i < n$.) All such points are, indeed, roots of $\Phi^*_{n,\phi}$, but it's possible that other points with smaller primitive period arise as roots as well. We call the roots of $\Phi^*_{n,\phi}$ the points of *formal* period n for ϕ.

Example. Let $\phi(x, y) = [-x^2 + y^2 : xy]$. Then we have:

$$\Phi^*_1(x, y) = -y\left(2x^2 - y^2\right)$$
$$\Phi^*_2(x, y) = -y^2$$

So we see that the point at infinity $\alpha = [1 : 0]$ is a fixed point, but it also appears as a double-root of the 2nd dynatomic polynomial.

Recall that if K is a field with $\operatorname{char} K \neq 2$ or 3, and $f(z) \in K[z]$ is a quadratic polynomial, then f is linearly conjugate to $f_c(z) = z^2 + c$ for some $c \in K$. Consider c as a parameter and calculate the nth dynatomic polynomial,

$$\Phi^*_{n,f_c}(z) = \prod_{k|n} \left(f_c^k(z) - z\right)^{\mu(n/k)}.$$

Theorem 5. *Let $f_c(z) = z^2 + c$. Then $\Phi^*_{n,f_c}(z) \in \mathbb{Z}[z, c]$ is irreducible over $\mathbb{C}[z, c]$ for every n.*

This result was first due to Bousch in his thesis [3], and was later generalized by Morton in [13] to generic monic polynomials of degree d.

For every n,

$$C_1(n)\colon \Phi^*_{n,f_c}(z,c) = 0$$

defines an affine algebraic curve. These are modular curves in the sense that they parameterize isomorphism classes of pairs (f,α), where $f(z)$ is a quadratic polynomial and α is a point of formal period n for ϕ. Theorem 5 says that these modular curves are geometrically irreducible. A natural question to ask is how general this result may be. If we consider other families of degree-2 rational maps on $\mathbb{P}^1$, should we expect these modular curves to be irreducible? In this chapter, we tackle this question.

2.2 Level Structure for M_2

We begin with some definitions and notation.

K	a field
$\overline{K}$	a (fixed) algebraic closure of K
$\phi \in K(z)$	a rational map of degree d
$\phi(x,y) = [F_1(x,y) : G_1(x,y)]$	homogenization of $\phi(z)$
$F_n(x,y) = F_{n-1}(F(x,y), G(x,y))$	
$G_n(x,y) = G_{n-1}(F(x,y), G(x,y))$	
$\phi^n(x,y) = [F_n(x,y) : G_n(x,y)]$	ϕ composed with itself n times, with F_n and G_n as above.
$\Phi^*_{n,\phi}(x,y)$	the nth dynatomic polynomial for ϕ as defined in Section 2.1
$\mathbb{P}^1$	the projective line $\mathbb{P}^1(\overline{K})$
PGL_2	the projective linear group over $\overline{K}$
Rat_d	the space of degree d rational maps as described in Section 2.1
M_d	$\mathrm{Rat}_d / \mathrm{PGL}_2$
$\nu_d(n)$	the degree of $\Phi^*_n(x,y) = \sum_{k\mid n} \mu(n/k)\, d^k$

Definition 4. *Let*

$$\mathrm{Rat}_d(N) = \{(\phi,\alpha) : \phi \in \mathrm{Rat}_d \ \textit{and } \alpha \textit{ is a point of formal period } N \textit{ for } \phi\}$$

and

$$M_d(N) = \{(\phi,\alpha) : \phi \in \mathrm{Rat}_d \ \textit{and } \alpha \textit{ is a point of formal period } N \textit{ for } \phi\}/\,\mathrm{PGL}_2 = \mathrm{Rat}_d(N)/\,\mathrm{PGL}_2\,.$$

For each N, we naturally have a surjective map from $M_2(N)$ to M_2, simply forgetting the point α. In fact, $M_2(N)$ is a $\nu_2(N)$-sheeted covering of M_2. An algebraic curve C in M_2 defines a family of (isomorphism classes of) quadratic rational maps ϕ_C. Lying over C in $M_2(N)$ is an algebraic curve $C_1(N)$, parameterizing pairs (ϕ,α), where ϕ is a map in the family ϕ_C and α is a point of formal period N for ϕ.

$$\begin{array}{ccc} C_1(N) & \longrightarrow & M_2(N) \\ \downarrow & & \downarrow \\ C & \longrightarrow & M_2 \end{array}$$

Our main result in this chapter is the following.

Theorem 6. *$M_2(N)$ is geometrically irreducible for every $N > 1$.*

From this we will be able to conclude

Corollary 1. *For every $N > 1$, only a Zariski-closed subset of families $\phi_C \subset M_2$ have reducible modular curves $C_1(N)$.*

Let $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ be a rational function of degree 2, defined over $\mathbb{C}$. Milnor has shown in [11] that each such rational map is $\mathrm{PGL}_2(\mathbb{C})$-conjugate to either $\phi(z) = z + \frac{1}{z}$ (if ϕ has a single fixed point) or to a map of the form $\phi_{a,b}(z) = \frac{z^2+az}{bz+1}$, with $ab \neq 1$, where a and b are the multipliers of the fixed points 0 and ∞ respectively. This representation is not unique. In general, a map ϕ has three distinct fixed points, and so three multipliers, say a, b, and c. Choosing elements of PGL_2 which permute the fixed points, we see that $\phi_{a,b}$, $\phi_{b,a}$, $\phi_{a,c}$, $\phi_{c,a}$, $\phi b, c$, and $\phi_{c,b}$ are all linearly conjugate.

The map $\phi(z) = z + \frac{1}{z}$ has a single fixed point at infinity, with multiplier 1, so this map corresponds to the point $(3,3) \in M_2$. Thus, we have a generically 6-to-1 map. Here $[\phi_{a,b}]$ denotes the isomorphism class of $\phi_{a,b}(z)$ in the moduli space M_2.

$$\begin{aligned} \mathbb{A}^2 \smallsetminus \{ab = 1\} &\longrightarrow M_2 \smallsetminus \{(3,3)\} \\ (a,b) &\longmapsto [\phi_{a,b}] \end{aligned}$$

We claim that this map is ramified only over the so-called symmetry locus, the family of maps in M_2 with a nontrivial PGL_2 autmorphism.

First, we see that any map of the form $\phi_{a,a}$ satisfies $\phi^f = \phi$ for $f(z) = \frac{1}{z}$. If a map has a nontrivial automorphism f, then f must permute the fixed points of ϕ. Taking derivatives on both sides of $\phi f = f\phi$, we see that the multipliers of the interchanged fixed points must be equal. If the multipliers are not ± 1, we conclude that ϕ is conjugate to the map $\phi_{a,a}$.

The identity given in equation (2.3) shows that it is impossible for the two equal multipliers to be -1. If a point has multiplier 1, then it is a double-root of the equation $\Phi_1(x,y)$, so in fact it is a fixed point of multiplicity two. Clearly there can be at most one such point for any $\phi \in M_2$. So the set of multipliers is $\{a, 1, 1\}$ where $a \neq 1$. (We have already seen that if all three multipliers are 1, the map is $\phi(z) = z + \frac{1}{z}$, which we have excluded from the discussion.) By Milnor's normal form, then, such a map is conjugate to one of the form $\phi_{a,1}$. This map has a double-fixed point at infinity and another fixed point at 0. Any automorphism of such a map must fix both of these points, so it is of the form $f(z) = kz$, and a computation shows that we must have $k = 1$. In other words, these maps have no nontrivial automorphisms.

If we consider the parameters a and b as indeterminates, we may compute $\Phi^*_{n,\phi_{a,b}}(x,y)$. Gauss's lemma shows that this will be a polynomial in $\mathbb{Z}[a,b,x,y]$. So for every n, $\Phi^*_n(x,y,a,b) = 0$ defines a

quasi-projective variety in $\mathbb{P}^1 \times \mathbb{A}^2 \smallsetminus \{ab = 1\}$. A point on the variety determines a rational function $\phi_{a,b}$ and a point of formal period n for that function. We begin the proof of Theorem 6 by showing that this quasi-projective variety is irreducible.

Lemma 2. *Let $\phi_{a,b}(x, y) = [x^2 + axy : bxy + y^2]$. For all $n > 1$, the coefficient of $x^{\nu_2(n)}$ in $\Phi^*_{n,\phi_{a,b}}$ (that is, the lead coefficient in x) is $C_n(b)$, the nth cyclotomic polynomial in b. By symmetry, we see that the coefficient of $y^{\nu_2(n)}$ is $C_n(a)$.*

Proof. For ease of notation, we will let $\phi = \phi_{a,b}$ and let $N = \nu_2(n)$ be the degree of $\Phi^*_{n,\phi}(x, y)$.

Let c_k be the coefficient of the highest-degree x-term in $\Phi_{k,\phi}(x, y) = yF_k(x, y) - xG_k(x, y)$. Since $\Phi^*_{n,\phi}(x, y) = \prod_{k|n} (yF_k(x, y) - xG_k(x, y))^{\mu(n/k)}$, and since we know that $\Phi^*_{n,\phi}(x, y, a, b)$ is a polynomial, we must have $c_N = \prod_{k|n} c_k^{\mu(n/k)}$.

We have $F_1(x, y) = x^2 + axy$, $G_1(x, y) = bxy + y^2$, and the iterates

$$\begin{aligned} F_n(x, y) &= (F_{n-1}(x, y))^2 + a\,(F_{n-1}(x, y))\,(G_{n-1}(x, y)) \\ G_n(x, y) &= b\,(F_{n-1}(x, y))\,(G_{n-1}(x, y)) + (G_{n-1}(x, y))^2 \end{aligned}$$

An easy proof by induction shows that for all $n \geq 1$, $\deg_x(F_n) = \deg_x(G_n) + 1$. The result clearly holds for F_1 and G_1, so then we calculate as follows.

$$\begin{aligned} \deg_x(F_n) &= \max(2\deg_x(F_{n-1}, \deg_x(F_{n-1}) + \deg_x(G_{n-1})) \\ &= 2\deg_x(F_{n-1}) \\ \deg_x(G_n) &= \max(2\deg_x(G_{n-1}, \deg_x(G_{n-1}) + \deg_x(G_{n-1})) \\ &= \deg_x(F_{n-1}) + \deg_x(G_{n-1}) \\ \deg_x(F_n) &= 2\deg_x(F_{n-1}) \\ &= \deg_x(F_{n-1}) + \deg_x(G_{n-1}) + 1 \\ &= \deg_x(G_n) + 1 \end{aligned}$$

Claim. F_n is monic of degree 2^n in x, and G_n has degree $2^n - 1$ with lead coefficient $b^n y$ as a polynomial in x.

The fact about the degrees follows from the recursion and from the result above. The fact that F_n is monic in x also follows easily from the recursive definition. It remains to compute the coefficient of x^{2^n-1} in $G_n(x, y)$. It is true for $n = 1$ by the function definition. From the claim above, we see that the highest-degree x term in $G_n(x, y)$ will come from the product $bF_{n-1}G_{n-1}$. We again proceed by induction.

$$\begin{aligned} G_n(x, y) &= b\left(x^{2^{(n-1)}} + \text{lower order terms in } x\right)\left(b^{n-1}yx^{2^{(n-1)}-1} + \text{lower order terms in } x\right) \\ &\quad + (\text{lower order terms in } x) \\ &= b^n y x^{2^n-1} + \text{lower order terms in } x \end{aligned}$$

We are now in a position to calculate c_N, the lead x-coefficient of $\Phi^*_{n,\phi}(x,y)$ for $n > 1$. Note that by the results above, $c_k = y(1-b^k)$.

$$\begin{aligned} c_N &= \prod_{k|n} c_k^{\mu(n/k)} = \prod_{k|n} \left(y(1-b^k)\right)^{\mu(n/k)} \\ &= \prod_{k|n} y^{\mu(n/k)} \prod_{k|n} (1-b^k)^{\mu(n/k)} = \prod_{k|n} (1-b^k)^{\mu(n/k)} \end{aligned}$$

Where the last equality follows because $n > 1$. We see that this is precisely the defining equation of $C_n(b)$, as desired. □

Proposition 2 requires a result of Morton (Corollary 4 in [13]):

Lemma 3. *For $n > 1$, the polynomial $\Phi^*_{n,h}(z,a)$ corresponding to $h(z,a) = z^2 + az$ is irreducible over $\overline{Q}$.*

Proposition 2. *Let $\phi(x,y) = \phi_{a,b}(x,y) = [x^2 + axy : bxy + y^2]$. The polynomial $\Phi^*_{n,\phi}(x,y,a,b)$ is irreducible over $\overline{\mathbb{Q}}$ for all $n > 1$.*

Proof. Suppose for contradiction $\Phi^*_n(x,y,a,b) = A(x,y,a,b)B(x,y,a,b)$ with $\deg(A), \deg(B) \geq 1$. Since the lead x coefficient in $\Phi^*_{n,\phi}$ is $C_n(b)$, the lead x coefficients in A and B are $c_{n,A}(b)$ and $c_{n,B}(b)$, where $c_{n,A}(b)c_{n,B}(b) = C_n(b)$.

Now, we specialize to $b = 0$. Since $C_n(0) = 1$, we see that $c_{n,A}(0)c_{n,B}(0) \neq 0$. So $\Phi^*_n(x,y,a,0) = A(x,y,a,0)B(x,y,a,0)$, where neither A nor B is trivial.

But the specialization to $b = 0$ yields the polynomial $\phi_{a,0}(x,y) = x^2 + axy$, which when dehomogenized is exactly the polynomial $h(z,a)$ in Lemma 3. So $\Phi^*_n(x,y,a,b)$ is irreducible in this case, and must therefore always be irreducible. □

We note that the condition $n > 1$ is necessary, as $\Phi^*_1(x,y,a,b) = xy(x(1-b) + y(1-a))$. This is expected, because part of constructing Milnor's normal form involves moving two of the fixed points to 0 and ∞. The factor of xy in Φ^*_1 reflects these two fixed points for every value of a and b, and the third factor provides the third fixed point.

Proof of Theorem 6. Consider the following commutative diagram.

$$\begin{array}{ccc} \Phi^*_N(x,y,a,b) = 0 & \longrightarrow & M_2(N) \smallsetminus \{\nu_2(N) \text{ points over } (3,3)\} \\ \downarrow & & \downarrow \\ \mathbb{A}^2 \smallsetminus \{ab = 1\} & \longrightarrow & M_2 \smallsetminus \{(3,3)\} \end{array} \tag{2.4}$$

Each map is surjective, with the horizontal maps generically 6-to1 as described above, and the vertical maps $\nu_2(N)$-to-1.

The top map gives a surjection from the geometrically irreducible variety $\Phi^*_N(x,y,a,b) = 0$ to the variety $M_d(N) \smallsetminus \{\text{a finite set of points}\}$. Clearly, then, $M_d(N)$ must also be irreducible □

Proof of Corollary 1. For $\phi \in \mathrm{Rat}_2$, let λ_1, λ_2, and λ_3 be the multipliers of the fixed points of ϕ. Take σ_1 and σ_2 as before, the first two symmetric functions of the multipliers, and let $\sigma_3 = \lambda_1\lambda_2\lambda_3$, the third symmetric function.

The identity in (2.3) can be used to deduce that

$$\sigma_3 = \sigma_1 - 2 \tag{2.5}$$

whenever none of the λ_i is 1. We recall that a multiplier of 1 indicates of fixed point of multiplicity at least two, and it is trivial to check that equation (2.5) continues to hold when any two multipliers are 1, so it holds for every map $\phi \in \mathrm{Rat}_2$.

Note that the quadratic polynomials $f_c(z) = z^2 + c$ have a superattracting fixed point at infinity (that is, the multiplier for that fixed point is 0). So for this family of maps, $\sigma_3 = 0$ and thus $\sigma_1 = 2$. Conversely, any map $\phi \in \mathrm{Rat}_2$ satisfying $\sigma_1 = 2$ must have a fixed point with multiplier of 0, which we may move to the point at infinity with some element of PGL_2. Milnor's normal form then shows that this map is a quadratic polynomial, and hence conjugate to f_c for some c.

The line $\sigma_1 = 2$ corresponds to a hyperplane slice of the surface $M_2(N)$. Bousch's result in Theorem 5 says that for every N, the resulting curve is irreducible. By Bertini's theorem, then, we conclude that the curves lying over families ϕ_C will be irreducible, except perhaps on a Zariski-closed subset of M_2. $\square$

Chapter 3

Maps with automorphisms

3.1 Preliminaries

We continue using the notation from Chapter 2. In addition, we will use the following.

$\mathcal{O}_\phi(\alpha)$	$\{\phi^n(\alpha) : n \geq 0\}$	the forward orbit of a point α under ϕ.
$\mathrm{Fix}(\phi)$	$\{\alpha \in \mathbb{P}^1 : \phi(\alpha) = \alpha\}$	the set of fixed points of a map ϕ.
$\mathrm{Aut}(\phi)$	$\{f \in \mathrm{PGL}_2 : \phi^f = \phi\}$	the automorphism group of a map ϕ.

As before, take $\phi(x, y) \in K(x, y)$ homogeneous, with $\phi(x, y) = [F_1(x, y) : G_1(x, y)]$. Also, fix $h \in \mathrm{Aut}(\phi)$ of prime order p.

Fix some $Q \in \mathbb{P}^1$. Since h has finite order, $\mathcal{O}_h(Q) = \{Q_0, \ldots, Q_{p-1}\}$ is a finite set. As a convention, we take

$$Q = Q_0 \overset{h}{\mapsto} Q_1 \overset{h}{\mapsto} \cdots \overset{h}{\mapsto} Q_{p-1} \overset{h}{\mapsto} Q_0 = Q.$$

If $\infty = [1 : 0] = Q_i$ for some i, choose $f \in \mathrm{PGL}_2$ so that f interchanges Q_i and a point not on the orbit of Q, and replace ϕ by ϕ^f. So with a change of coordinates, we may assume that none of the Q_i is infinity.

Definition 5. *Let $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ and $h \in \mathrm{Aut}(\phi)$. A point $Q \in \mathbb{P}^1$ has* period n relative to h, *or* h-period n for ϕ, *if $Q \neq \phi^n(Q) \in \mathcal{O}_h(Q)$. That is, if $\phi^n(Q) = h^j(Q)$ for some $j > 0$. Q has* primitive *period n relative to h, or* primitive *h-period n for ϕ, if $n > 0$ is the smallest such integer.*

In analogy with the dynatomic polynomials Φ_n^*, we wish to create polynomials which have as roots points of h-period n (rather than points of period n). As in the case of dynatomic polynomials, we wish to eliminate the roots having h-period k for $k < n$. We are led, then, to the following definition.

Definition 6. *Let $\phi(x, y) \in K(x, y)$ be homogeneous, $h \in \mathrm{Aut}(\phi)$, which we may write as $h(x, y) = [ax + by : cx + dy]$. Let $\mathrm{Fix}(h) = \{P_1, P_2\}$ with $P_i = [x_i : y_i]$. For clarity of notation we will write $\phi(x, y) - h(x, y)$ to represent the polynomial $(cx + dy)F_1(x, y) - (ax + by)G_1(x, y)$.*

$$\Psi_{pn,\phi,h}(x,y) = \prod_{j=1}^{p-1} \left(\phi^n(x,y) - h^j(x,y)\right) \tag{3.1}$$

$$\Psi^*_{pn,\phi,h}(x,y) = \prod_{\substack{k|n \\ pk\nmid n}} \left(\Psi_k(x,y)\right)^{\mu(n/k)} \tag{3.2}$$

$$\widetilde{\Psi^*_{pn,\phi,h}}(x,y) = \frac{\Psi^*_{pn}(x,y)}{(y_1x - x_1y)^{\delta_1}(y_2x - x_2y)^{\delta_2}} \tag{3.3}$$

where, for $i = 1, 2$, $\delta_i = \operatorname{ord}_{(y_ix - x_iy)} \Psi^*_{pn,\phi,h}(x,y)$.

By construction, roots of Ψ_{pn} are the points $Q = [x : y]$ such that $\phi^n(Q) = h^j(Q)$ for some $1 \le j \le p-1$. With Ψ^*_{pn}, we are eliminating (usually) the points Q such that $\phi^k(Q) = h^j(Q)$ for some $k < n$. The need to eliminate the fixed points of h as well will become clear as we proceed. Since we will be fixing a rational map ϕ with a particular automorphism h, we will usually suppress dependence on ϕ and h in our notation, writing simply Ψ_{pn}, Ψ^*_{pn}, and $\widetilde{\Psi^*_{pn}}$.

Example. Let $\phi(x,y) = [x^2 - 2xy : -2xy + y^2]$. It is a simple matter to check that ϕ has an automorphism of order 2 in $f(x,y) = [y : x]$ and an automorphism of order 3 in $g(x,y) = [x - y : x]$. We first compute a few of the dynatomic polynomials $\Phi_{n,\phi}(x,y)$.

$$\begin{aligned}
\Phi^*_2(x,y) &= -x^2 + yx - y^2 \\
\Phi^*_3(x,y) &= 3\left(x^3 - 3yx^2 + y^3\right)\left(x^3 - 3y^2x + y^3\right) \\
\Phi^*_4(x,y) &= \left(-5x^4 + 10yx^3 - 5y^3x + y^4\right)\left(x^4 + yx^3 - 9y^2x^2 + y^3x + y^4\right)\left(-x^4 + 5yx^3 - 10y^3x + 5y^4\right) \\
\Phi^*_6(x,y) &= \left(7x^6 - 21yx^5 + 35y^3x^3 - 21y^4x^2 + y^6\right)\left(x^6 - 6yx^5 - 6y^2x^4 + 29y^3x^3 - 6y^4x^2 - 6y^5x + y^6\right) \\
&\quad \left(x^6 - 21y^2x^4 + 35y^3x^3 - 21y^5x + 7y^6\right)\left(x^{18} - 18yx^{17} - 54y^2x^{16} + 1167y^3x^{15} - 2466y^4x^{14}\right. \\
&\quad - 7344y^5x^{13} + 31065y^6x^{12} - 20619y^7x^{11} - 54513y^8x^{10} + 99326y^9x^9 - 34119y^{10}x^8 \\
&\quad \left. -47844y^{11}x^7 + 51072y^{12}x^6 - 16155y^{13}x^5 - 621y^{14}x^4 + 1329y^{15}x^3 - 207y^{16}x^2 + y^{18}\right) \\
&\quad \left(x^{18} - 207y^2x^{16} + 1329y^3x^{15} - 621y^4x^{14} - 16155y^5x^{13} + 51072y^6x^{12} - 47844y^7x^{11}\right. \\
&\quad - 34119y^8x^{10} + 99326y^9x^9 - 54513y^{10}x^8 - 20619y^{11}x^7 + 31065y^{12}x^6 - 7344y^{13}x^5 \\
&\quad \left. -2466y^{14}x^4 + 1167y^{15}x^3 - 54y^{16}x^2 - 18y^{17}x + y^{18}\right)
\end{aligned}$$

We now compute a few of the relevant $\widetilde{\Psi^*_{pn}}(x,y)$ for ϕ. Note that

$$\operatorname{Fix}(f) = \{\pm 1\} \quad \text{and} \quad \operatorname{Fix}(g) = \{\text{roots of } z^2 - z + 1\}.$$

In other words, points in $\operatorname{Fix}(g)$ are the primitive sixth roots of unity.

Since f has order 2, the $\Psi^*_{N,\phi,f}$ are only defined for even N. We compute the first few of these.

$$\begin{aligned}
\Psi_{2,\phi,f}(x,y) &= \Psi^*_{2,\phi,f}(x,y) \\
&= x\left(x^2 - 2xy\right) - y\left(y^2 - 2xy\right) = (x - y)\left(x^2 - yx + y^2\right) \\
\widetilde{\Psi^*_{2,\phi,f}}(x,y) &= x^2 - yx + y^2
\end{aligned}$$

$$\begin{aligned}
\Psi_{4,\phi,f}(x,y) &= \Psi^*_{4,\phi,f}(x,y) \\
&= x\left(x^2-2xy\right)^2 - 2\left(x^2-2xy\right)\left(y^2-2xy\right) - y\left(y^2-2xy\right)^2 - 2\left(x^2-2xy\right)\left(y^2-2xy\right) \\
&= (x-y)\left(x^4+yx^3-9y^2x^2+y^3x+y^4\right) \\
\widetilde{\Psi^*_{4,\phi,f}}(x,y) &= x^4+yx^3-9y^2x^2+y^3x+y^4
\end{aligned}$$

$$\begin{aligned}
\Psi_{6,\phi,f}(x,y) &= (x-y)\left(x^2-yx+y^2\right)\left(x^6-6yx^5-6y^2x^4+29y^3x^3-6y^4x^2-6y^5x+y^6\right) \\
\Psi^*_{6,\phi,f}(x,y) &= \frac{\Psi_{6,\phi,f}(x,y)}{\Psi_{2,\phi,f}(x,y)} = x^6-6yx^5-6y^2x^4+29y^3x^3-6y^4x^2-6y^5x+y^6 \\
\widetilde{\Psi^*_{6,\phi,f}}(x,y) &= \Psi^*_{6,\phi,f}(x,y)
\end{aligned}$$

Since g has order 3, the $\Psi^*_{N,\phi,g}$ are only defined for N divisible by 3. We compute the first few of these.

$$\begin{aligned}
\Psi_{3,\phi,g}(x,y) &= \left(x\left(x^2-2xy\right)-(x-y)\left(y^2-2xy\right)\right)\left((y-x)\left(x^2-2xy\right)-y\left(y^2-2xy\right)\right) \\
&= -\left(x^3-3yx^2+y^3\right)\left(x^3-3y^2x+y^3\right) \\
\widetilde{\Psi^*_{3,\phi,g}}(x,y) &= \Psi^*_{3,\phi,g}(x,y) = \Psi_{3,\phi,g}(x,y)
\end{aligned}$$

$$\begin{aligned}
\Psi_{6,\phi,g}(x,y) &= -\left(x^2-yx+y^2\right)^2\left(x^3-3yx^2+y^3\right)\left(x^3-3y^2x+y^3\right) \\
\Psi^*_{6,\phi,g}(x,y) &= \frac{\Psi_{6,\phi,g}(x,y)}{\Psi_{3,\phi,g}(x,y)} = \left(x^2-yx+y^2\right)^2 \\
\widetilde{\Psi^*_{6,\phi,g}}(x,y) &= 1
\end{aligned}$$

$$\begin{aligned}
\Psi_{9,\phi,g}(x,y) &= \left(-x^9+9yx^8-84y^3x^6+126y^4x^5-84y^6x^3+36y^7x^2-y^9\right) \\
&\qquad \left(x^9-36y^2x^7+84y^3x^6-126y^5x^4+84y^6x^3-9y^8x+y^9\right) \\
\widetilde{\Psi^*_{9,\phi,g}}(x,y) &= \Psi^*_{9,\phi,g}(x,y) = \Psi_{9,\phi,f}(x,y)
\end{aligned}$$

Based on the example, one might conjecture that $\widetilde{\Psi^*_{pn}}$ is always a polynomial, and that it divides Φ^*_{pn}. In this chapter, we prove these assertions. After determining that Ψ^*_{pn} is almost always nontrivial, we will be able to conclude that the dynatomic polynomials Φ^*_n are reducible for infinitely many n, and hence so are the moduli spaces defined by their vanishing.

3.2 Some useful lemmas

Throughout, we fix a rational map $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d \geq 2$, and a map $h \in \mathrm{Aut}(\phi)$ of prime order p.

Lemma 4.

(a) $\mathrm{Fix}(h)$ *consists of exactly two distinct points.*

(b) If $Q \in \mathrm{Fix}(h)$ *then* $|\mathcal{O}_\phi(Q)| \leq 2$.

Proof. Any nontrivial element of PGL_2 has exactly two fixed points, counted with multiplicity. The only elements with exactly one fixed point are equivalent under a change of coordinates to a nontrivial translation (where the fixed point is the point at infinity), but none of these has finite order.

If $h(Q) = Q$ then for any $k \geq 0$, $h\phi^k(Q) = \phi^k h(Q) = \phi^k(Q)$ because $h \in \mathrm{Aut}(\phi)$. In other words, every point on the orbit of Q is fixed by h, so there can be at most two distinct points on the orbit. □

Lemma 5. *Suppose* Q *has* h*-period* n *for* ϕ.

(a) Then $\phi^{kn}(Q) \in \mathcal{O}_h(Q)$ *for all* k.

(b) If Q *has primitive* h*-period* m*, then* $m \mid n$.

Proof. If $\phi^n(Q) = Q$, the results are well-known for periodic points of a map. (See [22] for example.) Otherwise, $\phi^n(Q) = h^j(Q)$ for some $1 \leq j \leq p-1$. Clearly as sets $\mathcal{O}_h(Q) = \mathcal{O}_{h^j}(Q)$, so we may rename the automorphism so that $\phi^n(Q) = h(Q)$. We may then show, in fact, that $\phi^{kn}(Q) = h^k(Q)$ for all k.

$$\begin{aligned}
\phi^{kn}(Q) &= \phi^{(k-1)n}\phi^n(Q) \\
&= \phi^{(k-1)n}h(Q) \\
&= h\phi^{(k-1)n}(Q) && \text{since } h \in \mathrm{Aut}(\phi) \\
&= h^k(Q) && \text{by induction.}
\end{aligned}$$

For the second result, we have

$$\begin{aligned}
\phi^n(Q) &= \phi^{qm+r}(Q) && \text{with } 0 \leq r < m \\
&= \phi^r\phi^{qm}(Q) = \phi^r h^k(Q) && \text{for some } k\text{, by the result above} \\
&= h^j(Q) && \text{for some } 0 \leq j < p\text{, since } \phi^n(Q) \in \mathcal{O}_h(Q) \\
h^k\phi^r(Q) &= h^j(Q) && \text{since } h \in \mathrm{Aut}(\phi) \\
\phi^r(Q) &= h^i(Q) \in \mathcal{O}_h(Q) && \text{where } i \equiv j-k \pmod{p}.
\end{aligned}$$

By minimality of m, we see that necessarily $r = 0$ and so indeed $m \mid n$. □

If a rational map $\phi \in K(z)$ is defined at $z = Q$ — that is if $Q \neq \infty$ and $\phi(Q) \neq \infty$ — then we may write

$$\phi(z) = \sum_{i=0}^{n} \lambda_i(\phi, Q)(z-Q)^i + \mathcal{O}\left((z-Q)^{n+1}\right)$$

where $\lambda_0(\phi, Q) = \phi(Q)$ and $\mathcal{O}\left((z-Q)^n\right)$ represents a function vanishing to order at least $n+1$ at $z = Q$. We take this as the definition of the $\lambda_i(\phi, Q)$.

Lemma 6. *Let f, g, h be rational maps. Then:*

(a) If $\lambda_i(f, h(Q)) = \lambda_i(g, h(Q))$ for all $0 \leq i \leq n$, then also $\lambda_i(fh, Q) = \lambda_i(gh, Q)$ for all $0 \leq i \leq n$

(b) If $\lambda_i(f, Q) = \lambda_i(g, Q)$ for all $0 \leq i \leq n$ (in particular, if $f(Q) = g(Q)$), then also $\lambda_i(hf, Q) = \lambda_i(hg, Q)$ for all $0 \leq i \leq n$

Remark. Suppose we have $\phi, h \in K(z)$ and let $f \in \mathrm{PGL}_2$ be some change of coordinates. Then Lemma 6 says that

$$\begin{aligned} \lambda_i(\phi, Q) = \lambda_i(h, Q) \text{ for } 0 \leq i \leq n \quad &\Longrightarrow \quad \lambda_i(\phi f, f^{-1}Q) = \lambda_i(hf, f^{-1}Q) \text{ for } 0 \leq i \leq n \\ &\Longrightarrow \quad \lambda_i(f^{-1}\phi f, f^{-1}Q) = \lambda_i(f^{-1}hf, f^{-1}Q) \text{ for } 0 \leq i \leq n. \end{aligned}$$

So if $\phi(Q) = h(Q)$, then equality of the first n coefficients, $\lambda_i(\phi, Q)$ and $\lambda_i(h, Q)$, is preserved under PGL_2 conjugation. This is how the Lemma will be applied.

Proof. The $n = 0$ case is clear. For $1 \leq m \leq n$,

$$\begin{aligned} \lambda_m(fh, P) &= \sum_{k=1}^{m} \lambda_k(f, h(Q)) \prod_{\substack{k-\text{tuples } (i_1,\ldots,i_k) \\ i_1+\cdots+i_k=m}} \lambda_{i_j}(h, Q) \\ &= \sum_{k=1}^{m} \lambda_k(g, h(Q)) \prod_{\substack{k-\text{tuples } (i_1,\ldots,i_k) \\ i_1+\cdots+i_k=m}} \lambda_{i_j}(h, Q) && \text{by the hypothesis} \\ &= \lambda_m(gh, Q) \\ \lambda_m(hf, Q) &= \sum_{k=1}^{m} \lambda_k(h, f(Q)) \prod_{\substack{k-\text{tuples } (i_1,\ldots,i_k) \\ i_1+\cdots+i_k=m}} \lambda_{i_j}(f, Q) \\ &= \sum_{k=1}^{m} \lambda_k(h, g(Q)) \prod_{\substack{k-\text{tuples } (i_1,\ldots,i_k) \\ i_1+\cdots+i_k=m}} \lambda_{i_j}(g, Q) && \text{by the hypothesis} \\ &= \lambda_m(hg, Q) \end{aligned}$$

□

Lemma 7. *For any $Q \in \overline{K}$,*

$$\prod_{i=0}^{p-1} \lambda_1(h, Q_i) = 1 \tag{3.4}$$

Furthermore, if $Q \in \mathrm{Fix}(h)$, then $\lambda_1(h, Q)$ is a primitive p^{th} root of unity.

Proof. The first result follows from the fact that $h^p(z) = z$. For all $Q \in \overline{K}$, this gives $(h^p)'(Q) = 1$, so the numbers $\lambda_1(h, Q) = h'(Q)$ are well-defined (and nonzero) for all $Q \in \overline{K}$. So then

$$\begin{aligned}\prod_{i=0}^{p-1} \lambda_1(h, Q_i) &= \prod_{i=0}^{p-1} h'(Q_i) \\ &= (h^p)'(Q) = 1.\end{aligned}$$

If $Q \in \mathrm{Fix}(h)$, the equation becomes $(\lambda_1(\phi, Q))^p = 1$. If $\lambda_1(\phi, Q) = 1$, then Q is a double root of $h(z) - z = 0$. The automorphism h has exactly two fixed points counted with multiplicity, and from Lemma 4 we know that they are distinct. So $\lambda_1(\phi, Q)$ must be a primitive p^{th} root of unity, since p is prime. □

Lemma 8. *Suppose that $\phi(Q) = h(Q)$. Then*

$$\frac{\lambda_1(\phi, Q_i)}{\lambda_1(h, Q_i)} = \frac{\lambda_1(\phi, Q_j)}{\lambda_1(h, Q_j)} \qquad \text{for all } i, j \geq 0. \tag{3.5}$$

$$\prod_{i=0}^{p-1} \lambda_1(\phi, Q_i) = \left(\frac{\lambda_1(\phi, Q)}{\lambda_1(h, Q)}\right)^p \tag{3.6}$$

Proof. As described in Section 3.1, we assume without loss of generality that infinity is not in $\mathcal{O}_h(Q)$. The required change of coordinates is valid by Lemma 6.

Since $\phi h = h\phi$,

$$\begin{aligned}\lambda_1(\phi h, Q_i) &= \lambda_1(h\phi, Q_i) \\ \lambda_1(\phi, Q_{i+1})\lambda_1(h, Q_i) &= \lambda_1(h, Q_{i+1})\lambda_1(\phi, Q_i) \qquad (3.7)\end{aligned}$$

Dividing each side of equation (3.7) by the product $\lambda_1(h, Q_i)\lambda_1(h, Q_{i+1})$ — which is nonzero by Lemma 7 — along with a simple induction gives the first result.

To prove the second result, divide each side of equation (3.7) by $\lambda_1(h, Q_i)$ to get

$$\lambda_1(\phi, Q_{i+1}) = \lambda_1(\phi, Q_i)\left(\frac{\lambda_1(h, Q_{i+1})}{\lambda_1(h, Q_i)}\right) \tag{3.8}$$

Repeatedly using the substitution in equation (3.8), we have $\lambda_1(\phi, Q_i) = \lambda_1(\phi, Q_0)\left(\frac{\lambda_1(h,Q_i)}{\lambda_1(h,Q_0)}\right)$. Now, using the identity in equation (3.4), we have

$$\begin{aligned}\prod_{i=0}^{p-1} \lambda_1(\phi, Q_i) &= \prod_{i=0}^{p-1} \lambda_1(\phi, Q_0)\left(\frac{\lambda_1(h, Q_i)}{\lambda_1(h, Q_0)}\right) \\ &= \left(\frac{\lambda_1(\phi, Q)}{\lambda_1(h, Q)}\right)^p\end{aligned}$$

□

Lemma 9. *Assume $\phi(Q) = h(Q)$. If $\lambda_j(\phi, Q) = \lambda_j(h, Q)$ for all $1 \leq j \leq e$, then*

(a) $\lambda_j(\phi, Q_i) = \lambda_j(h, Q_i)$ for all $Q_i \in \mathcal{O}_h(Q)$ and all $1 \leq j \leq e$, and

(b) $\lambda_j(\phi^i, Q) = \lambda_j(h^i, Q)$ for all i and all $1 \leq j \leq e$. In particular, we have

- $\lambda_1(\phi^p, Q) = 1$, *and*
- $\lambda_j(\phi^p, Q) = 0$ *for all* $2 \leq j \leq e$.

Proof. Note first that $\lambda_1(h, Q_i) \neq 0$ by the fact that $\prod_{i=1}^{p} \lambda_1(h, Q_i) = 1$ from Lemma 7.

The first assertion is proved by induction. If $\lambda_1(h, Q_i) = \lambda_1(\phi, Q_i)$, neither is 0, so we may cancel them both in equation (3.7) to get $\lambda_1(h, Q_{i+1}) = \lambda_1(\phi, Q_{i+1})$.

Now suppose the implication holds for $e - 1$, and that $\lambda_j(\phi, Q_i) = \lambda_j(h, Q_i)$ for all $1 \leq j \leq e$. Because $\phi h = h\phi$, we get

$$\begin{aligned} \lambda_e(\phi h, z) &= \lambda_e(h\phi, z), && \text{so in particular} \\ \lambda_e(\phi h, Q_i) &= \lambda_e(h\phi, Q_i). \end{aligned}$$

This gives

$$\begin{aligned} &\lambda_e(\phi, Q_{i+1}) \left(\lambda_1(h, Q_i)\right)^e + (*) + \lambda_1(\phi, Q_{i+1})\lambda_e(h, Q_i) \\ &\qquad = \lambda_e(h, Q_{i+1}) \left(\lambda_1(\phi, Q_i)\right)^e + (**) + \lambda_1(h, Q_{i+1})\lambda_e(\phi, Q_i) \end{aligned}$$

where $(*)$ represents terms involving $\lambda_j(\phi, Q_{i+1})$ and $\lambda_k(h, Q_i)$ with $1 \leq j, k < e$, and similarly for $(**)$. These terms will be equal on each side by the induction hypothesis, so they cancel, as do the final two terms by the fact that $\lambda_e(h, Q_i) = \lambda_e(\phi, Q_i)$. We are left with

$$\begin{aligned} \lambda_e(\phi, Q_{i+1}) \left(\lambda_1(h, Q_i)\right)^e &= \lambda_e(h, Q_{i+1}) \left(\lambda_1(\phi, Q_i)\right)^e \\ \lambda_e(\phi, Q_{i+1}) &= \lambda_e(h, Q_{i+1}), \end{aligned}$$

where the last equality follows from the fact that $\lambda_1(\phi, Q_i) = \lambda_1(h, Q_i) \neq 0$ again.

For the second assertion, note that $\lambda_j(\phi^i, Q)$ is some polynomial combination of $\lambda_k(\phi, Q_i)$ for $1 \leq k \leq j$ and $Q_i \in \mathcal{O}_h(Q)$, and $\lambda_j(h^i, Q)$ is the exact same polynomial combination of $\lambda_k(h, Q_i)$. By the first assertion, then, these two must be equal for $1 \leq j \leq e$.

The final two bullets follow immediately from the above, together with the fact that $h^p(z) = z$. This means that $\lambda_1(h^p, z) = 1$ and $\lambda_j(h^p, z) = 0$ for $j \neq 1$. (So in particular, these hold at $z = Q$.) □

Lemma 10. *Assume* $\phi(Q) = h(Q)$, *and let* e *be the smallest positive integer such that* $\lambda_e(\phi, Q) \neq \lambda_e(h, Q)$. *Then*

$$\lambda_e(\phi^j, Q) - \lambda_e(h^j, Q) = j \left(\prod_{i=1}^{j-1} \lambda_1(\phi, Q_i) \right) \left(\lambda_e(\phi, Q) - \lambda_e(h, Q)\right).$$

Proof. We proceed by induction. The claim is trivial for $j = 1$. Assume the relation holds for $j - 1$. Note that by Lemma 9, for all $0 \leq f < e$ we have $\lambda_f(\phi^i, Q_j) = \lambda_f(h^i, Q_j)$ for all non-negative

integers i and j, which gives equality of the terms marked $(*)$ and $(**)$ in the first equation below.

$$\begin{aligned}
\lambda_e(\phi^j, Q) - \lambda_e(h^j, Q) &= \big(\lambda_e(\phi, Q_{j-1})\lambda_1(\phi^{j-1}, Q)^e + (*) + \lambda_1(\phi, Q_{j-1})\lambda_e(\phi^{j-1}, Q)\big) \\
&\quad - \big(\lambda_e(h, Q_{j-1})\lambda_1(h^{j-1}, Q)^e + (**) + \lambda_1(h, Q_{j-1})\lambda_e(h^{j-1}, Q)\big) \\
&= \lambda_1(\phi^{j-1}, Q_1)^e(\lambda_e(\phi, Q_j) - \lambda_e(h, Q_j)) \\
&\quad + \lambda_1(\phi, Q_{j-1})(\lambda_e(\phi^{j-1}, Q) - \lambda_e(h^{j-1}, Q)) \\
&= \lambda_1(\phi^{j-1}, Q)^e(\lambda_e(\phi, Q_{j-1}) - \lambda_e(h, Q_{j-1})) \\
&\quad + (j-1)\left(\prod_{i=1}^{j-1} \lambda_1(\phi, Q_i)\right)(\lambda_e(\phi, Q) - \lambda_e(h, Q)) \qquad (3.9)
\end{aligned}$$

It remains to calculate the first term in this sum. First, note that $\lambda_1(\phi^{j-1}, Q) = \prod_{i=0}^{j-2} \lambda_1(\phi, Q_i)$ (recall that $Q = Q_0$). Next we use the fact that $\phi h = h\phi$ again. In what follows, equality of the terms $(*)$ and $(**)$ follows as usual.

$$\begin{aligned}
\lambda_e(\phi h, Q_i) &= \lambda_e(h\phi, Q_i) \\
\lambda_e(\phi, Q_{i+1})\lambda_1(h, Q_i)^e + (*) + \lambda_1(\phi, Q_{i+1})\lambda_e(h, Q_i) & \\
&= \lambda_e(h, Q_{i+1})\lambda_1(\phi, Q_i)^e + (**) + \lambda_1(h, Q_{i+1})\lambda_e(\phi, Q_i) \\
\lambda_1(\phi, Q_i)^e\left(\lambda_e(\phi, Q_{i+1}) - \lambda_e(h, Q_{i+1})\right) &= \lambda_1(\phi, Q_{i+1})\left(\lambda_e(\phi, Q_i) - \lambda_e(h, Q_i)\right)
\end{aligned}$$

So inductively again

$$\begin{aligned}
\lambda_1(\phi^{j-1}, Q)^e(\lambda_e(\phi, Q_{j-1}) - \lambda_e(h, Q_{j-1})) &= \left(\prod_{i=0}^{j-2} \lambda_1(\phi, Q_i)^e\right)(\lambda_e(\phi, Q_{j-1}) - \lambda_e(h, Q_{j-1})) \\
&= \prod_{i=1}^{j-1} \lambda_1(\phi, Q_i)\left(\lambda_e(\phi, Q) - \lambda_e(h, Q)\right)
\end{aligned}$$

Substituting this into equation (3.9) above gives the desired result. □

Definition 7. *Let*

$$\begin{aligned}
b_Q(pn) &= \mathrm{ord}_{z=Q}(\Psi_{pn}) = \sum_{i=1}^{p-1} \mathrm{ord}_{z=Q}(\phi^n(z) - h^j(z)) \\
b_Q^*(pn) &= \mathrm{ord}_{z=Q}(\Psi_{pn}^*) = \sum_{\substack{k|n \\ pk\nmid n}} \mu(n/k) b_Q(pk) \\
\widetilde{b_Q^*}(pn) &= \mathrm{ord}_{z=Q}(\widetilde{\Psi_{pn}^*}) \\
&= \begin{cases} 0 & \textit{if } Q \in \mathrm{Fix}(h) \\ b_Q^*(pn) & \textit{otherwise} \end{cases}
\end{aligned}$$

Lemma 11. *Suppose Q has h-period 1 for ϕ. If $p \mid N$, then $b_Q(pN) = 0$. If $p \nmid N$, then*

$$\left(\frac{\lambda_1(\phi,Q)}{\lambda_1(h^j,Q)}\right)^N \neq 1 \text{ for all } j \implies b_Q(pN) = b_Q(p) = 1 \tag{3.10}$$

$$\left.\begin{array}{c}\left(\frac{\lambda_1(\phi,Q)}{\lambda_1(h^j,Q)}\right)^N = 1 \text{ for some } j \\ \text{and } \lambda_1(\phi,Q) \neq \lambda_1(h^j,Q)\end{array}\right\} \implies b_Q(pN) > b_Q(p) = 1 \tag{3.11}$$

$$\lambda_1(\phi,Q) = \lambda_1(h^j,Q) \text{ for some } j \implies \begin{cases} b_Q(pN) > b_Q(p) > 1 & \text{if } \operatorname{char} K \mid N \\ b_Q(pN) = b_Q(p) > 1 & \text{otherwise} \end{cases} \tag{3.12}$$

Proof. Before continuing, we have some reductions. From the definition, it's clear that

$$\Psi_{pn,\phi,h} = \Psi_{pn,\phi,h^j}$$

for any $1 \leq j \leq p-1$. So by renaming the automorphism, we may assume that $\phi(Q) = h(Q) \neq Q$. By the proof of Lemma 5, then, $\phi^k(Q) = h^k(Q)$ for all k. In other words, for all $Q_i \in \mathcal{O}_h(Q)$, $\phi(Q_i) = h(Q_i)$. If Q is a point such that $\phi(Q) = h(Q)$, we may change coordinates so that $Q = 0 = [0:1]$ and no $Q_i \in \mathcal{O}_h(Q)$ satisfies $Q_i = \infty = [1:0]$. We will see that the condition $\left(\frac{\lambda_1(\phi,Q)}{\lambda_1(h,Q)}\right)^N = 1$ is equivalent to $\lambda_1(\phi^N,Q) = \lambda_1(h^j,Q)$ where $N \equiv j \pmod p$. By Lemma 6 each of the conditions above are preserved under this change.

Since h has order p, every point $Q \in \mathbb{P}^1$ has period p under h. For $Q \notin \operatorname{Fix}(h)$, the primitive period for Q must be p. Therefore, Q has primitive period p for ϕ as well. Since $\phi^p(Q) = Q \neq h^j(Q)$ for any $1 \leq j \leq p-1$, we see that $b_Q(pN) = 0$ whenever $p \mid N$, which proves the first assertion.

Because Q has primitive period p for h, the orbit $\mathcal{O}_h(Q)$ consists of p distinct points. That is, if $i \neq j$ then $h^i(Q) \neq h^j(Q)$. We assume that $\phi(Q) = h(Q)$, so $\phi(Q) \neq h^j(Q)$ for $2 \leq j \leq p-1$. Hence, $b_Q(p) = \operatorname{ord}_{z=Q}(\phi(z) - h(z))$. We now proceed, focusing just on this term.

We may dehomogenize $\phi(x,y)$ to the rational map $\phi(z)$. Then for each i, we have

$$\phi(z) = Q_{i+1} + \sum_{j=1}^{n} \lambda_j(\phi,Q_i)(z-Q_i)^j + \mathcal{O}\left((z-Q_i)^{n+1}\right) \tag{3.13}$$

$$h(z) = Q_{i+1} + \sum_{j=1}^{n} \lambda_j(h,Q_i)(z-Q_i)^j + \mathcal{O}\left((z-Q_i)^{n+1}\right) \tag{3.14}$$

$$\phi(z) - h(z) = \sum_{j=1}^{n} \left(\lambda_j(\phi,Q_i) - \lambda_j(h,Q_i)\right)(z-Q_i)^j + \mathcal{O}\left((z-Q_i)^{n+1}\right)$$

From this, we see that $b_Q(p) = 1$ if $\lambda_1(\phi,Q) \neq \lambda_1(h,Q)$. Otherwise $b_Q(p) = e > 1$ where e is the smallest integer such that $\lambda_e(\phi,Q) \neq \lambda_e(h,Q)$. (Note there must be such an e since both are rational maps but $\deg\phi > \deg h$ says that they cannot be equal.)

Assume now that $\lambda_1(\phi,Q) \neq \lambda_1(h,Q)$, and let $N = pn + j$ for some $1 \leq j \leq p-1$. Iterating

equation (3.13) starting with $Q_0 = 0$, we have

$$\phi(z) = Q_1 + \lambda_1(\phi, 0)z + \mathcal{O}\left(z^2\right) \tag{3.15}$$

$$\begin{aligned}\phi^2(z) &= Q_2 + \lambda_1(\phi, Q_1)\left(\lambda_1(\phi, 0)z + \mathcal{O}(z^2)\right) + \mathcal{O}(z^2) \\ &= Q_2 + \lambda_1(\phi, Q_1)\lambda_1(\phi, 0)z + \mathcal{O}(z^2).\end{aligned} \tag{3.16}$$

By an easy induction we get

$$\begin{aligned}\phi^p(z) &= \left(\prod_{i=0}^{p-1} \lambda_1(\phi, Q_i)\right) z + \mathcal{O}(z^2) && \text{(recall that } Q_p = Q_0 = 0\text{)} \\ &= \left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^p z + \mathcal{O}(z^2) && \text{by Lemma 8.} \qquad (3.18) \\ \phi^{pn}(z) &= \left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^{pn} z + \mathcal{O}(z^2).\end{aligned} \tag{3.17}$$

$$\phi^{pn+j}(z) = Q_j + \left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^{pn} \prod_{i=0}^{j-1} \lambda_1(\phi, Q_i)z + \mathcal{O}(z^2). \tag{3.19}$$

Combining this with equation (3.14), we have

$$\begin{aligned}\phi^{pn+j}(z) - h^j(z) &= \left(\left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^{pn} \prod_{i=0}^{j-1} \lambda_1(\phi, Q_i) - \lambda_1(h^j, 0)\right) z + \mathcal{O}(z^2) \\ &= \left(\left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^{pn} \prod_{i=0}^{j-1} \lambda_1(\phi, Q_i) - \prod_{i=0}^{j-1} \lambda_1(h, Q_i)\right) z + \mathcal{O}(z^2)\end{aligned}$$

So $b_Q(pN) = b_Q(p) = 1$ unless the coefficient of z above vanishes, or in other words unless

$$\begin{aligned}\left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^{pn} \prod_{i=0}^{j-1} \frac{\lambda_1(\phi, Q_i)}{\lambda_1(h, Q_i)} &= 1 && \text{(since } \prod_{i=0}^{j-1} \lambda_1(h, Q_i) \neq 0 \text{ by Lemma 7)} \\ \left(\frac{\lambda_1(\phi, 0)}{\lambda_1(h, 0)}\right)^{pn+j} &= 1 && \text{(by equation (3.5)),}\end{aligned} \tag{3.20}$$

from which the first two assertions follow.

We now consider the case that $\lambda_1(\phi, Q) = \lambda_1(h, Q)$. We saw above that in this case $b_Q(1) = e > 1$ where e is the smallest positive integer such that $\lambda_e(\phi, Q) \neq \lambda_e(h, Q)$. So by Lemma 9, $\lambda_1(\phi^p, 0) = 1$, and $\lambda_j(\phi^p, 0) = 0$ for all $2 \leq j < e$. Therefore

$$\phi^p(z) = z + \lambda_e(\phi^p, 0)z^e + \mathcal{O}(z^{e+1}). \tag{3.21}$$

We may iterate ϕ^p in this easier form to find that

$$\phi^{pn}(z) = z + n\lambda_e(\phi^p, 0)z^e + \mathcal{O}(z^{e+1}).$$

Composing this version of $\phi^{pn}(z)$ with the expansion of ϕ in equation (3.13), we find the following.

$$\begin{aligned}\phi^{pn+j}(z) &= Q_j + \lambda_1(\phi^j,0)\left(z + n\lambda_e(\phi^p,0)z^e + \mathcal{O}(z^{e+1})\right)\\ &\quad + \lambda_2(\phi^j,0)\left(z + n\lambda_e(\phi^p,0)z^e + \mathcal{O}(z^{e+1})\right)^2 + \cdots\\ &= Q_j + \sum_{i=1}^{e-1}\lambda_i(\phi^j,0)z^i + \left(\lambda_1(\phi^j,0)n\lambda_e(\phi^p,0) + \lambda_e(\phi^j,0)\right)z^e + \mathcal{O}(z^{e+1})\end{aligned}$$

$$\phi^{pn+j}(z) - h^j(z) = \sum_{i=1}^{e-1}\left(\lambda_i(\phi^j,0) - \lambda_i(h^j,0)\right)z^i + \left(\lambda_1(\phi^j,0)n\lambda_e(\phi^p,0) + \lambda_e(\phi^j,0) - \lambda_e(h^j,0)\right)z^e + \mathcal{O}(z^{e+1})$$

By Lemma 9, the terms $\lambda_i(\phi^j,0) - \lambda_i(h^j,0)$, hence $b_Q(pN) \geq e$. By Lemma 10,

$$\begin{aligned}\lambda_e(\phi^p,0) &= \lambda_e(\phi^p,0) - \lambda_e(h^p,0) && \text{since } e > 1 \text{ means } \lambda_e(h^p,0) = 0\\ &= p\left(\prod_{i=0}^{p-1}\lambda_1(\phi,Q_i)\right)\left(\lambda_e(\phi,0) - \lambda_e(h,0)\right).\end{aligned}$$

So the coefficient of z^e vanishes if and only if

$$\left(np\lambda_1(\phi^j,0)\prod_{i=1}^{p-1}\lambda_1(\phi,Q_i) + j\prod_{i=1}^{j-1}\lambda_1(\phi,Q_i)\right)\left(\lambda_e(\phi,0) - \lambda_e(h,0)\right) = 0.$$

Now, $\lambda_e(\phi,0) - \lambda_e(h,0) \neq 0$ by our choice of e. By Lemma 8,

$$\prod_{i=1}^{j-1}\lambda_1(\phi,Q_i) \neq 0,$$

so we may divide by it. Note also that

$$\lambda_1(\phi^j,0) = \prod_{i=0}^{j-1}\lambda_1(\phi,Q_i).$$

So $b_Q(pN) > e$ if and only if

$$\begin{aligned}np\prod_{i=0}^{p}\lambda_1(\phi,Q_i) + j &= 0\\ np + j &= 0 && \text{since by Lemma 9, we know } \prod_{i=1}^{p}\lambda_1(\phi,Q_i) = 1.\\ N &= 0 && \text{by choice of } N.\end{aligned}$$

The coefficient of z^e vanishes if and only if $\operatorname{char} K \mid N$, and in this case $b_Q(pN) > e$. □

Lemma 12. *Suppose* $Q \in \operatorname{Fix}(h) \cap \operatorname{Fix}(\phi)$. *Then*

$$\left(\frac{\lambda_1(\phi,Q)}{\lambda_1(h^j,Q)}\right)^N \neq 1 \textit{ for all } j \implies b_Q(pN) = b_Q(p) = p-1 \tag{3.22}$$

$$\left.\begin{array}{c}\left(\frac{\lambda_1(\phi,Q)}{\lambda_1(h^j,Q)}\right)^N = 1 \textit{ for some } j \\ \textit{and } \lambda_1(\phi,Q) \neq \lambda_1(h^j,Q)\end{array}\right\} \implies b_Q(pN) > b_Q(p) = p-1 \tag{3.23}$$

$$\lambda_1(\phi,Q) = \lambda_1(h^j,Q) \textit{ for some } j \implies \begin{cases} b_Q(pN) > b_Q(p) > p-1 & \textit{if } \operatorname{char} K \mid N \\ b_Q(pN) = b_Q(p) > p-1 & \textit{otherwise} \end{cases} \tag{3.24}$$

Proof. If $\phi(Q) = Q$ and $h(Q) = Q$, then $z = Q$ is a root of $\phi(z) - h^j(z)$ for every $1 \leq j \leq p-1$. This gives the lower bound on $b_Q(p)$.

From Lemma 7, $\lambda_1(h^j,Q)$ is a primitive p^{th} root of unity for each j. But also $\lambda_1(h^j,Q) = (\lambda_1(h,Q))^j$ by the definition of the λ_i and the fact that $Q \in \operatorname{Fix}(h)$. This shows that if $i \neq j$, then $\lambda_1(h^i,Q) \neq \lambda_(h^j,Q)$. So if $\lambda_1(\phi,Q) = \lambda_1(h^j,Q)$, then $\lambda_1(\phi,Q) \neq \lambda_1(h^i,Q)$ for all $i \neq j$.

That is, if $b_Q(p) > p-1$, the excess is accounted for by a single factor of $\Psi_p(x,y)$. The rest of the proof proceeds exactly as in Lemma 11. □

We conclude the section by stating a result from [16] which will be used in the sequel. We begin with a definition.

Definition 8. *Let*

$$a_Q(n) = \operatorname{ord}_{z=Q}(\Phi_n) = \operatorname{ord}_{z=Q}(\phi^n(z) - z)$$
$$a_Q^*(n) = \operatorname{ord}_{z=Q}(\Phi_n^*) = \sum_{k|n} \mu(n/k) a_Q(k)$$

Proposition 3. *Let K be a field, X/K a smooth projective curve, and let $\phi\colon K \to K$ be a non-constant morphism defined over K such that ϕ^n is non-degenerate. Fix a point $Q \in X$ and define integers m, q, r by*

$$\begin{aligned} m &= \textit{the exact period of } Q \textit{ (set } m = \infty \textit{ if } Q \notin \operatorname{Per}(\phi)), \\ q &= \textit{the characteristic of } K, \\ r &= \textit{the multiplicative period of } (\phi^m)'(Q) \textit{ in } \overline{K}^* \\ &\quad\ \textit{(set } r = \infty \textit{ if } m = \infty \textit{ or if } (\phi^m)'(Q) \textit{ is not a root of unity }). \end{aligned}$$

(a) $a_Q^*(n) \geq 0$ *for all* $n \geq 1$.

(b) Let $n \geq 1$. *Then* $a_Q^*(n) \geq 1$ *if and only if one of the following three conditions is true.*

(i) $n = m$.

(ii) $n = mr$.

(iii) $n = q^s mr$ *for some* $s \geq 0$.

3.3 Reducibility results

We now prove the main results for this chapter.

Theorem 7. *Let ϕ be a rational map with an automorphism h of prime order p. Let K be a field over which ϕ, h, and* $\mathrm{Fix}(h)$ *are all defined. The dynatomic polynomiasl Φ^*_{pn} is reducible over K for infinitely many values of n.*

Corollary 2 gives the result for general fields K, and Proposition 9 is a stronger result that holds in characteristic 0.

Proposition 4. *With the hypotheses in Theorem 7, $\widetilde{\Psi^*_{pn}} \in K[x,y]$ (that is, it is a polynomial) for all $n \geq 1$. More specifically, fix a point $Q \in \mathbb{P}^1$ and define integers m, q, and r by*

$$\begin{aligned} m &= \textit{the primitive } h\textit{-period of } Q \textit{ for } \phi \\ &\qquad (\textit{set } m = \infty \textit{ if } \mathcal{O}_h(Q) \cap \mathcal{O}_\phi(Q) = Q), \\ q &= \textit{the characteristic of } K, \\ r &= \textit{the multiplicative period of } \frac{\lambda_1(\phi^m, Q)}{\lambda_1(h^j, Q)}, \textit{ where } 1 \leq j \leq p-1 \textit{ satisfies } \phi^m(Q) = h^j(Q), \\ &\qquad (\textit{set } r = \infty \textit{ if either } m = \infty \textit{ or if } \frac{\lambda_1(\phi^m, Q)}{\lambda_1(h^j, Q)} \textit{ is not a root of unity for any } 1 \leq j \leq p-1). \end{aligned}$$

(a) $\widetilde{b^*_Q}(pn) \geq 0$ *for all* $n \geq 1$.

(b) Let $n \geq 1$. *Then* $\widetilde{b^*_Q}(pn) \geq 1$ *if and only if one of the following conditions is true.*

(i) $n = m$.

(ii) $n = mr$, *with* $p \nmid r$.

(iii) $n = mrq^s$ *for some* $s \geq 1$.

Proof. It's clear from definitions that $\widetilde{\Psi^*_{pn}}(x,y)$ is a polynomial if and only if $\Psi^*_{pn}(x,y)$ is a polynomial. Further, if $Q \in \mathrm{Fix}(h)$, $\widetilde{b^*_Q}(pn) = 0$. Otherwise $\widetilde{b^*_Q}(pn) = b^*_Q(pn)$, so we prove that for $Q \notin \mathrm{Fix}(h)$, $b^*_Q(pn)$ satisfies the statement of the proposition.

From Lemma 5 we see that unless $m \mid n$, $b_Q(pk) = 0$ for any $k \mid n$, so then also $b^*_Q(pn) = 0$. We need only consider the case that $m \mid n$. Now suppose that $p \nmid n$. The condition that $pk \nmid n$ adds no information, so we may calculate

$$b^*_Q(pn) = \sum_{\substack{k \mid n \\ pk \nmid n}} \mu(n/k) b_Q(pk) = \sum_{k \mid n} \mu(n/k) b_Q(pk). \tag{3.25}$$

For clarity we write $b_Q(\phi, pn)$ for $b_Q(pn)$ because we will be dealing with multiple rational maps. Let $\psi = \phi^m$ — so Q has primitive h-period 1 for ψ — and let $N = n/m$. By the argument above,

the only terms which contribute to the sum in equation (3.25) are the ones where $m \mid k$, so

$$\begin{aligned} b_Q^*(\phi, pn) &= \sum_{k|n} \mu(n/k) b_Q(pk) = \sum_{k'|N} \mu(mN/mk') b_Q(\phi, pmk') \\ &= \sum_{k'|N} \mu(N/k') b_Q(\phi^m, pk') = \sum_{k'|N} \mu(N/k') b_Q(\psi, pk') = b_Q^*(\psi, pN) \qquad \text{since } p \nmid N. \end{aligned}$$

Since Q has primitive h-period 1 for ψ, we may apply Lemma 11. For clarity of notation, we rename the automorphism so that $\psi(Q) = h(Q)$.

Case Ia $\left(\frac{\lambda_1(\psi,Q)}{\lambda_1(h,Q)}\right)^N \neq 1$.

Case Ib $\lambda_1(\psi, Q) = \lambda_1(h, Q)$ and $q \nmid N$.

In both cases, we have $b_Q(\psi, p) = b_Q(\psi, pk)$ for all $k \mid N$. So then

$$\sum_{k|N} \mu(N/k) b_Q(\psi, pk) = \sum_{k|N} \mu(N/k) b_Q(\psi, p) = \begin{cases} b_Q(\psi, p) > 0 & \text{if } N = 1 \text{ so that } n = m \\ 0 & \text{if } N > 1 \text{ so that } n > m \end{cases}$$

Since $b_Q(\psi, p) = b_Q(\phi^n, p) = b_Q(\phi, pn)$, we conclude that in these cases $b_Q^*(pn) = b_Q(pn) > 0$ if and only if $m = n$.

Case II $\lambda_1(\psi, Q) = \lambda_1(h, Q)$ and $q \mid N$.

Write $N = q^s M$ with $q \nmid M$. Since $\psi(Q) = h(Q)$, we know from the proof of Lemma 5 that

$$\psi^{q^i}(Q) = h^{q^i}(Q) = h^j(Q) \text{ for some } 0 \leq j \leq p-1.$$

Since $p \neq q$ — we know $p \nmid N$ but $q \mid N$ — we see that in fact $1 \leq j \leq p-1$. Then because $\lambda_1(\psi, Q) = \lambda_1(h, Q)$, Lemma 9 says that also

$$\lambda_1\left(\psi^{q^i}, Q\right) = \lambda_1\left(h^{q^i}, Q\right) = \lambda_1\left(h^j, Q\right).$$

If $k \mid M$, then necessarily $q \nmid k$, so we may apply equation (3.12) to conclude that

$$b_Q\left(\psi, pq^i k\right) = b_Q\left(\psi^{q^i}, pk\right) = b_Q\left(\psi^{q^i}, p\right) = b_Q\left(\psi, pq^i\right).$$

We may then compute

$$\begin{aligned} b_Q^*(\psi, pN) &= \sum_{\substack{k|N \\ pk \nmid N}} \mu(N/k) b_Q(\psi, pk) = \sum_{k|N} \mu(N/k) b_Q(\psi, pk) \qquad \text{since } p \nmid N \\ &= \sum_{k|M} \sum_{i=0}^{s} \mu(q^s M/q^i k) b_Q(\psi, pq^i k) \\ &= \left(\sum_{k|M} \mu(M/k)\right) \left(\sum_{i=0}^{s} \mu(q^{s-i}) b_Q(\psi, pq^i)\right) \\ &= \begin{cases} b_Q(\psi, pq^s) - b_Q(\psi, pq^{s-1}) > 0 & \text{if } M = 1 \\ 0 & \text{if } M > 1. \end{cases} \end{aligned}$$

The fact that $b_Q^*(\psi, pN) > 0$ when $M = 1$ follows from applying equation (3.12) to the difference $b_Q\left(\psi^{q^{s-1}}, pq\right) - b_Q\left(\psi^{q^{s-1}}, p\right)$. So we have shown that in this case, $b_Q^*(\phi, pn) \geq 0$, and that $b_Q^*(\phi, pn) > 0$ if and only if $n = mq^s$.

Case III $\left(\frac{\lambda_1(\psi,Q)}{\lambda_1(h,Q)}\right)^N = 1.$

Since r is the exact order of $\frac{\lambda_1(\psi,Q)}{\lambda_1(h,Q)}$ in $\overline{K}^*$, we have $r \mid N$ (and further $r > 1$ or we are in Case Ib or Case II). If $r \nmid k$, then by Lemma 11, $b_Q(\psi, pk) = b_Q(\psi, p)$. So we may split the sum of $b_Q^*(\psi, pN)$ into two parts:

$$\begin{aligned}
\sum_{k|N} \mu(N/k) b_Q(\psi, pk) &= \left(\sum_{\substack{k|N \\ r\nmid k}} + \sum_{\substack{k|N \\ r|k}}\right) \mu(N/k) b_Q(\psi, pk) \\
&= \left(\sum_{\substack{k|N \\ r\nmid k}} \mu(N/k) b_Q(\psi, p)\right) + \left(\sum_{\substack{k|N \\ r|k}} \mu(N/k) b_Q(\psi, pk)\right) \\
&= \sum_{k|N} \mu(N/k) b_Q(\psi, p) + \sum_{\substack{k|N \\ r|k}} \mu(N/k) \left(b_Q(\psi, pk) - b_Q(\psi, p)\right) \\
&= \sum_{\substack{k|N \\ r|k}} \mu(N/k) \left(b_Q(\psi, pk) - b_Q(\psi, p)\right) \qquad \text{(since } N > 1 \text{ the first sum vanishes).}
\end{aligned}$$

Now if $k \mid N$ and $r \mid k$, then $k = rk'$ for some k' a divisor of N/r. So we can rewrite the final sum as

$$\begin{aligned}
\sum_{\substack{k|N \\ r|k}} \mu(N/k) \left(b_Q(\psi, pk) - b_Q(\psi, p)\right) &= \sum_{k'|(N/r)} \mu\left(\frac{N/r}{k'}\right) \left(b_Q(\psi, prk') - b_Q(\psi, p)\right) \\
&= \sum_{k'|(N/r)} \mu\left(\frac{N/r}{k'}\right) \left(b_Q(\psi^r, pk') - b_Q(\psi, p)\right) \\
&= b_Q^*(\psi^r, pN/r) - \begin{cases} b_Q(\psi, p) & \text{if } N = r \\ 0 & \text{if } N > r. \end{cases}
\end{aligned}$$

If $N = r$, then

$$b_Q^*(\phi, pn) = b_Q^*(\psi, pN) = b_Q^*(\psi^r, p) - b_Q(\psi, p) = b_Q(\psi^r, p) - b_Q(\psi, p) = b_Q(\psi, pr) - b_Q(\psi, p) > 0.$$

And in this case,

$$\begin{aligned}
b_Q^*(\phi, pn) &= b_Q(\psi, pr) - b_Q(\psi, p) \\
&= b_Q(\phi^n, p) - b_Q(\phi^m, p) \qquad (3.26)
\end{aligned}$$

If $N > r$, then

$$b_Q^*(\phi, pn) = b_Q^*(\psi, pN) = b_Q^*(\psi^r, pN/r) \qquad (3.27)$$

Since $p \nmid r$, we have

$$\psi^r(Q) = h^r(Q) = h^j(Q) \text{ for some } 1 \le j \le p-1,$$

and as before we have

$$\frac{\lambda_1(\psi^r, Q)}{\lambda_1(h^j, Q)} = \left(\frac{\lambda_1(\psi, Q)}{\lambda_1(h, Q)}\right)^r = 1.$$

If $N \neq 0$ in K, we may apply Case Ib to ψ^r and conclude that $b_Q^*(\psi^r, pN/r) = 0$ since $N/r > 1$. If $N = 0$ in K, then we can apply Case II to $b_Q^*(\psi^r, pN/r)$ and again conclude that $b_Q^*(\psi^r, pN/r) = 0$ unless $N/r = q^s$ for some $s \ge 1$.

In Case III, we conclude that $b_Q^*(pn) > 0$ if and only if $N = r$ or $N = q^s r$, so $n = mr$ or $n = mq^s r$, where $p \nmid r$.

We must now consider the case that $p \mid n$, so $n = p^t n'$ where $t \ge 1$ and $p \nmid n'$. Then the condition that $pk \nmid n$ means that $k = p^t k'$ for some k' that divides n'. So we have:

$$\begin{aligned} b_Q^*(\phi, pn) &= \sum_{\substack{k \mid n \\ pk \nmid n}} \mu(n/k) b_Q(\phi, pk) = \sum_{k' \mid n'} \mu\left(p^t n'/p^t k'\right) b_Q\left(\phi, p\left(p^t k'\right)\right) \\ &= \sum_{k' \mid n'} \mu(n'/k') b_Q\left(\phi^{p^t}, pk'\right) = b_Q^*\left(\phi^{p^t}, pn'\right) \qquad \text{since } p \nmid n'. \end{aligned} \tag{3.28}$$

Suppose that Q has primitive h-period m' for ϕ^{p^t} and primitive h-period m for ϕ. We know that the primitive h-period for ϕ must divide $p^t m'$. That means $m = p^{t'} m''$ with $0 \le t' \le t$ and $m'' \mid m'$. If $t' < t$, then $\phi^{pm}(Q) = Q \neq h(Q)$. Hence $t' = t$ and also $m'' = m'$ by minimality of m'. So in fact $m = m' p^t$.

We now apply the results above to the map ϕ^{p^t}. We conclude that $b_Q^*(\phi, pn) \ge 0$ for all $Q \in \mathbb{P}^1$ and $b_Q^*(\phi, pn) > 0$ if and only if one of the following conditions hold.

1. Q has primitive h-period n' for ϕ^{p^t}. So by the argument above, Q has primitive h-period $n = p^t n'$ for ϕ.

2. Q has h-period m' for ϕ^{p^t}, $n' = m'r$. In this case, $n = p^t n' = p^t m' r$. By the argument above, Q has primitive h-period $m = p^t m'$ for ϕ. So we have $n = mr$.

3. Q has h-period m' for ϕ^{p^t}, $n' = m' r q^s$. In this case, $n = p^t n' q^s = p^t m' r q^s$. So with $m = p^t m'$ as above we have $n = mrq^s$. □

We know that the $\widetilde{\Psi_{pn}^*}$ are polynomials. We now show that they are divisors of the associated dynatomic polynomials.

Proposition 5. *For every $n \ge 1$, $\widetilde{\Psi_{pn}^*} \mid \Phi_{pn}^*$.*

Proof. To show that $\widetilde{\Psi_{pn}^*} \mid \Phi_{pn}^*$, we must show that $a_Q^*(pn) \ge \widetilde{b_Q^*}(pn)$ for all $Q \in \mathbb{P}^1$. If $Q \in \mathrm{Fix}(h)$, then $\widetilde{b_Q^*}(pn) = 0$ for all n, and the result is immediate, so we assume $Q \notin \mathrm{Fix}(h)$, in which case $\widetilde{b_Q^*}(pn) = b_Q^*(pn)$. Clearly, we need only consider the case $b_Q^*(pn) > 0$; there are three ways this

can happen, described in Proposition 4. Throughout, we assume that $b^*_Q(pn) > 0$ and that Q has primitive h-period m for some $m \mid n$, and we rename the automorphism so that $\phi^m(Q) = h(Q)$.

Case I $n = m$.

Since Q has primitive h-period n, we also have $\phi^{kn}(Q) = h^k(Q)$ for all $k \geq 1$, so in particular we may conclude $\phi^{pn}(Q) = Q$, and in fact pn is the primitive period of Q. Since $b_Q(pk) = 0$ for $k < n$, we have $b^*_Q(pn) = b_Q(pn)$. Similarly, since pn is the primitive period of Q, $a_Q(k) = 0$ for $k < pn$; therefore $a^*_Q(pn) = a_Q(pn) \geq 1$ by Lemma 3. If $b_Q(pn) = 1$, we are done.

Otherwise, $b_Q(\phi^n, p) = e > 1$ where e is the smallest positive integer such that $\lambda_e(\phi^n, Q) \neq \lambda_e(h, Q)$. By Lemma 9, then, $\lambda_1(\phi^{pn}, Q) = 1$ and $\lambda_i(\phi^{pn}, Q) = 0$ for $1 < i < e$. This says that $a_Q(pn) \geq e$, and we are done in this case.

Case II $n = mr$ with $r > 1$, $p \nmid r$, and $\frac{\lambda_1(\phi^m,Q)}{\lambda_1(h,Q)}$ a primitive r^{th} root of unity.

As above, since Q has primitive h-period m for ϕ, we know that Q has primitive period pm for ϕ. Also, since $\frac{\lambda_1(\phi^m,Q)}{\lambda_1(h,Q)}$ is a primitive r^{th} root of unity and $p \nmid r$, we have by equation (3.18)

$$\lambda_1(\phi^{pm}, Q) = \left(\frac{\lambda_1(\phi^m, Q)}{\lambda_1(h, Q)}\right)^p$$

is also a primitive r^{th} root of unity.

From Proposition 4 (see equation (3.26)), we know that

$$b^*_Q(pn) = b_Q(\phi^n, p) - b_Q(\phi^m, p).$$

A similar proof in [16] shows that, since $\lambda_1(\phi^{pm}, Q)$ is a primitive r^{th} root of unity,

$$a^*_Q(pn) = a_Q(\phi^{pn}, 1) - a_Q(\phi^{pm}, 1).$$

Since $\lambda_1(\phi^{pm}, Q) \neq 1$ and $\lambda_1(\phi^m, Q) \neq \lambda_1(h, Q)$, we conclude that $b_Q(\phi^m, p) = a_Q(\phi^{pm}, 1) = 1$. It remains to show that if $b_Q(\phi^n, p) = e > 1$, then $a_Q(\phi^{pn}, 1) \geq e$, but this follows immediately from Lemma 9, exactly as in Case I. Summarizing, we have

$$\begin{aligned} a^*_Q(pn) &= a_Q(pn) - a_Q(pm) = a_Q(pn) - 1 \\ &\geq b_Q(pn) - 1 = b_Q(pn) - b_Q(pm) = b^*_Q(pn) \end{aligned}$$

Case III $n = mrq^s$ with $\frac{\lambda_1(\phi^m,Q)}{\lambda_1(h^j,Q)}$ a primitve r^{th} root of unity, and $\operatorname{char} K = q$.

Once again, the primitive period of Q is pm. By equation (3.27), we see that

$$\begin{aligned} b^*_Q(pn) &= b^*_Q(\phi^{mr}, pq^s) = b_Q(\phi^{mr}, pq^s) - b_Q(\phi^{mr}, pq^{s-1}) \\ &= b_Q(pmrq^s) - b_Q(pmrq^{s-1}) \end{aligned} \tag{3.29}$$

and in [16] a similar argument shows that

$$a^*_Q(pn) = a_Q(pmrq^s) - a_Q(pmrq^{s-1}). \tag{3.30}$$

From Proposition 4 and Lemma 11, we conclude that $b_Q(\phi^{mr}, pq^{s-1}) = e > 1$ and $b_Q(\phi^{mr}, pq^s) = f > e > 1$. For ease of notation, we let $\psi = \phi^{mrq^{s-1}}$. Then we have $\psi(Q) = h^j(Q)$ for some j, and furthermore since $e > 1$,

$$\lambda_i(\psi, Q) = \lambda_i(h^j, Q) \quad \text{for } 1 \le i < e.$$

By Lemma 10,

$$\begin{aligned}\lambda_e(\phi^{pmrq^{s-1}}, Q) = \lambda_e(\psi^p, Q) &= \lambda_e(\phi^{pm}, Q) - \lambda_e(h^p, Q) && \text{since if } e > 1,\ \lambda_e(h^p, Q) = 0\\ &= p\left(\prod_{i=1}^{p-1} \lambda_1(\phi, Q_i)\right)(\lambda_e(\phi, Q) - \lambda_e(h, Q)).\end{aligned}$$

This can never vanish since $q \neq p$ and neither of the other terms can vanish. This means that

$$a_Q(pmrq^{s-1}) = b_Q(pmrq^{s-1}) = e.$$

The exact same argument applied to $\psi = \phi^{pmrq^s}$ shows that

$$a_Q(pmrq^s) = b_Q(pmrq^s) = f.$$

Equations (3.29) and 3.30, then, show that $a_Q^*(pn) = b_Q^*(pn)$ in this case. □

In order to prove that the dynatomic polynomials Φ_{pn}^* are reducible for infinitely many n, we must be sure that the factors $\widetilde{\Psi_{pn}^*}$ are nontrivial. The example at the end of Section 3.1 shows that this is certainly not always the case. First, we must show that $\deg \widetilde{\Psi_{pn}^*} < \deg \Phi_{pn}^*$ for suitable choice of n. We require one additional lemma.

Lemma 13. *For $n > 1$, $a \ge 2$ and $p \ge 2$,*

$$\sum_{k|n} \mu(n/k) a^{pk} > p \sum_{k|n} \mu(n/k) a^k$$

Proof. Let $f(n) = a^{pn}$ and $g(n) = pa^n$, and define $h = (f - g) * \mu$, where $*$ represents convolution in the usual number-theoretic sense. The statement of the lemma is equivalent to $h(n) > 0$ for all $n > 1$. By properties of convolution (see [10] for example), $h * 1 = ((f - g) * \mu) * 1 = f - g$. In other words,

$$\sum_{k|n} h(k) = a^{pn} - pa^n.$$

We will show by induction that $h(n) < a^{pn}$ and $h(n) > 0$ for all $n > 1$. Since $a \ge 2$ and $p \ge 2$,

$$h(1) = a^p - pa < a^p \quad \text{and} \quad h(1) = a(a^{p-1} - p) \ge 0.$$

In fact, $h(1) = 0$ if and only if $a = p = 2$.

Now consider a prime q,

$$h(q) = a^{pq} - pa^q - h(1) < a^{pq} \qquad \text{since } pa^q > 0 \text{ and } h(1) \ge 0.$$

But also

$$\begin{aligned}
h(q) &= a^{pq} - pa^q - a^p + pa = a^p(a^{p(q-1)} - 1) - pa(a^{q-1} - 1) \\
&\geq a^p(a^{q-1} - 1)(a^{q-1} + 1) - pa(a^{q-1} - 1) && \text{since } p \geq 2 \\
&= (a^{q-1} - 1)(a^{p(q-1)} + 1 - pa) > 0 && \text{since } a^p \geq pa \text{ and } q \geq 2.
\end{aligned}$$

Now suppose for all $k < m$, $h(k) < a^{pk}$ and also that $h(k) > 0$ if $n > 1$. If m is prime, the result holds by the argument above. Assume then that m is composite (so clearly $m > 3$). For all $k \mid m$, if $k \neq m$, we have $h(k) \geq 0$ by the induction hypothesis, so

$$h(m) = a^{pm} - pa^m - \sum_{\substack{k|m \\ k\neq m}} h(k) < a^{pm}.$$

Also by the induction hypothesis, $h(k) < a^{pk}$ for each k in the sum above. Further, the largest divisor of m is at most $m - 2$ since $m \geq 4$. So we can say that

$$\sum_{\substack{k|m \\ k\neq m}} h(k) < a^{p(m-2)} + \cdots + a^p = \frac{a^{p(m-1)} - a^p}{a^p - 1}$$

Using this rough estimate, we find

$$\begin{aligned}
h(m) &> a^{pm} - pa^m - \frac{a^{p(m-1)} - a^p}{a^p - 1} \\
&= \frac{a^{p(m+1)} - a^{pm} - a^{p(m-1)} + a^p}{a^p - 1} - pa^m \\
&= \frac{a^{p(m-1)}(a^{2p} - 1) - a^{pm} + a^p}{a^p - 1} - pa^m \\
&= a^{p(m-1)}(a^p + 1) - \frac{a^{pm} + a^p}{a^p - 1} - pa^m \\
&> a^{pm} + a^{p(m-1)} - a^{pm} + a^p - pa^m && \text{since the denominator is} > 1 \\
&= a^{p(m-1)} + a^p - pa^m > 0 && \square
\end{aligned}$$

Proposition 6. *Begin with the hypotheses in Theorem 7, and let* $\deg \phi = d$.

(a) If $d > 2$, *then* $\deg(\widetilde{\Psi^*_{pn}}) < \deg(\Phi^*_{pn})$ *for all* $n \geq 1$.

(b) If $d = 2$, *then* $\deg(\widetilde{\Psi^*_{pn}}) < \deg(\Phi^*_{pn})$ *for all* $n > 1$.

Proof. From definition 6, we see that $\deg(\widetilde{\Psi^*_{pn}}) \leq \deg(\Psi^*_{pn})$ for every n. So we prove now that $\deg(\Psi^*_{pn}) < \deg(\Phi^*_{pn})$ for $n > 1$. Consider first the case that $p \nmid n$, so if $k \mid n$, we have already $pk \nmid n$.

$$\deg \Psi^*_{pn} = \sum_{\substack{k|n \\ pk\nmid n}} \mu(n/k)(p-1)\left(d^k + 1\right) = \begin{cases} (p-1)(d+1) & \text{if } n = 1 \\ (p-1)\sum_{k|n} \mu(n/k) d^k & \text{if } n > 1 \end{cases}$$

Note that if $k \mid pn$ then either $k \mid n$ or $k = pk'$ for some $k' \mid n$. So

$$\begin{aligned}\deg \Phi^*_{pn} &= \sum_{k|pn} \mu(pn/k)\left(d^k+1\right)\\ &= \sum_{k|n} \mu(pn/k)d^k + \sum_{k|n} \mu(pn/pk)d^{pk} + \sum_{k|pn} \mu(pn/k)\end{aligned}$$

Since by hypothesis $p \nmid n$, we know that $\gcd(p,k)=1$ for k any divisor of n. Therefore $\mu(pn/k) = \mu(p)\mu(n/k) = -\mu(n/k)$. (Recall also that $pn > 1$ so the final term vanishes.)

$$\deg \Phi^*_{pn} = -\sum_{k|n} \mu(n/k)d^k + \sum_{k|n} \mu(n/k)d^{pk} \tag{3.31}$$

Comparing equations (3.31) and (3.31), we see that $\deg \Psi^*_{pn} < \deg \Phi^*_{pn}$ when $n > 1$ follows from the fact that $\sum_{k|n} \mu(n/k)d^{pk} > p\sum_{k|n} \mu(n/k)d^k$ for all $n > 1$, from Lemma 13.

In the $n = 1$ case, we wish to show that $(\deg\phi)^p + 1 - p(\deg\phi + 1) > 0$ when $d > 2$. From equations (3.31) and (3.31), we have

$$\deg \Phi^*_p - \deg \Psi^*_p = (d^p - d) - (p-1)(d+1) = d^p - pd - (p-1),$$

which is increasing with d, so it will be positive for all $d > 2$ if it is positive when $d = 3$. In that case, we calculate

$$\deg \Phi^*_p - \deg \Psi^*_p = 3^p - 3p - (p-1),$$

which is clearly increasing with p, so we simply check that for $p = 2$ we have $9 - 6 - 1 = 2 > 0$.

Now if $p \mid n$, then we have $n = p^r n'$ where $r \geq 1$ and $p \nmid n'$. The condition that $pk \nmid n$ means that $k = p^r k'$ for some $k' \mid n'$. So we have:

$$\begin{aligned}\deg \Psi^*_{pn} &= \sum_{\substack{k|n\\ pk\nmid n}} \mu(n/k)(p-1)\left(d^k+1\right)\\ &= (p-1)\sum_{k'|n'} \mu\left(p^r n'/p^r k'\right)\left(d^{p^r k'}+1\right)\\ &= (p-1)\sum_{k'|n'} \mu\left(n'/k\right)\left(d^{p^r}\right)^{k'} + \sum_{k'|n'} \mu(n'/k')\\ &= \begin{cases}(p-1)\ \sum_{k'|n'} \mu\left(n'/k'\right)\left(d^{p^r}\right)^{k'} & \text{if } n' > 1\\ (p-1)\left(d^{p^r}+1\right) & \text{if } n' = 1\end{cases}\end{aligned} \tag{3.32}$$

Since $n = p^r n'$, $pn = p^{r+1}n'$. If $k \mid pn$ but $p^r \nmid k$, then $p^2 \mid \left(p^{r+1}n'/k\right)$, which means that $\mu(pn/k) = 0$. So the only divisors which contribute to the sum below are ones of the form $p^r k'$ where $k' \mid pn'$.

$$\begin{aligned}\deg \Phi^*_{pn} &= \sum_{k|pn} \mu(pn/k)\left(d^k+1\right)\\ &= \sum_{k'|pn'} \mu(p^{r+1}n'/p^r k')\left(d^{p^r k'}\right)\\ &= \sum_{k'|pn'} \mu(pn'/k')\left(d^{p^r}\right)^{k'}\end{aligned} \tag{3.33}$$

Comparing equations (3.32) and (3.33), we see that if $n' > 1$ we are reduced to the case $p \nmid n$ above. If $n' = 1$, the sum in equation (3.33) is

$$\begin{aligned} d^{p^{r+1}} - d^{p^r} &\geq 4d^{p^r} - d^{p^r} && \text{since } d \geq 2,\ p \geq 2 \text{ and } r \geq 1 \\ &= 3d^{p^r} \\ &> d^{p^r} + 1 && \text{since } d \geq 2,\ p \geq 2 \text{ and } r \geq 1 \end{aligned}$$

So again $\deg \Phi^*_{pn} > \deg \Psi^*_{pn}$. □

We must also prove non-triviality in the sense that $\Psi^*_{pn} \neq 1$. If all roots of Ψ^*_{pn} are in $\mathrm{Fix}(h)$, then the polynomial $\widetilde{\Psi^*_{pn}}$ will be trivial. So we must first examine the possible values of $b^*_Q(pn)$ when $Q \in \mathrm{Fix}(h)$.

Proposition 7. *With the hypotheses in Theorem 7, let $Q \in \mathrm{Fix}(h)$, and define integers q and r as in Proposition 4. Then $b^*_Q(pn) \geq 1$ if and only if one of the following conditions is true.*

(i) $n = p^t$ *for some* $t \geq 0$.

(ii) $n = rp^t$ *for some* $t \geq 0$.

(iii) $n = rq^s p^t$ *for some* $t \geq 0$, $s \geq 1$.

(iv) $n = 2p^t$ *for some* $t \geq 0$.

(v) $n = 2rp^t$ *for some* $t \geq 0$.

(vi) $n = 2rq^s p^t$ *for some* $t \geq 0$, $s \geq 1$.

Proof. Let m be the primitive period of Q for ϕ. From Lemma 4, we know that $m = 1$ or 2. So there are really three cases.

(i) $n = mp^t$ for some $t \geq 0$.

(ii) $n = mrp^t$ for some $t \geq 0$.

(iii) $n = mrq^s p^t$ for some $t \geq 0$, $s \geq 1$.

In the case $p \nmid n$, the proofs follow exactly as in Proposition 4. However, we must reconsider the case where $p \mid n$, since we used in an essential way the assumption that $Q \notin \mathrm{Fix}(h)$.

Suppose, then, that $p \mid n$, so write $n = p^t n'$ where $p \nmid n'$. As in equation (3.28), we find that

$$b^*_Q(\phi, pn) = b^*_Q\left(\phi^{p^t}, pn'\right).$$

Let m' be the primitive period of Q for ϕ^{p^t}. We must have $m' = 1$ if $m = 1$ or if $m = p = 2$, and $m' = 2$ otherwise. Applying the three cases where $p \nmid n$ to $B_Q\left(\phi^{p^t}, pn'\right)$, we see that either $n' = m'$, or $n' = m'r$, or $n' = m'q^s$. Substituting each of these for n' gives the desired result. □

We can now prove a nontriviality result for general fields K by showing that points of primitive h-period ℓ for ϕ exist for almost all primes ℓ. This proof is essentially the same as the proof of existence of points of primitive period ℓ found, for example, in [22].

Proposition 8. *Under the hypotheses of Theorem 7 with* $\deg\phi = d$*, for all prime numbers* ℓ *except for at most* $d+6$ *exceptions, the map* ϕ *has a point of primitive* h*-period* ℓ*.*

Proof. We begin by discarding the finitely many primes satisfying any of the following conditions:

- $\ell = 2$.
- $\ell = p$.
- $\ell = \operatorname{char} K$.
- There is some Q with primitive h-period 1 and some $1 \le j \le p-1$ such that $\frac{\lambda_1(\phi,Q)}{\lambda_1(h^j,Q)}$ is a primitive ℓ^{th} root of unity.
- There is some $Q \in \operatorname{Fix}(\phi)$ and some some $1 \le j \le p-1$ such that $\frac{\lambda_1(\phi,Q)}{\lambda_1(h^j,Q)}$ is a primitive ℓ^{th} root of unity.

There are at most $d+1$ points of primitive h-period 1, and the set $\operatorname{Fix}(h)$ has at most 2 elements, so this list eliminates at most $d+6$ primes. Note that we have eliminated the primes where $b^*_Q(p\ell) \ge 1$ for $Q \in \operatorname{Fix}(h)$.

For any of the remaining primes ℓ, consider a root of $\Psi^*_{\ell n}(x,y)$. This must be a point of h-period ℓ. If it does not have primitive h-period ℓ, then it must have primitive h-period 1 by Lemma 5. Because of the primes we have eliminated, and by results in Proposition 11, we see that $b_Q(p\ell) = b_Q(p)$, so

$$\sum_{\text{roots of } \Psi^*_p \cap \text{roots of } \Psi^*_{p\ell}} b_Q(p\ell) = \sum_{\text{roots of } \Psi^*_p \cap \text{roots of } \Psi^*_{p\ell}} b_Q(p) \le \sum_{\text{roots of } \Psi^*_p} b_Q(p) = d+1.$$

That is, the total multiplicity of all roots of $\Psi^*_{p\ell}$ that do not have primitive h-period ℓ is at most $d+1$. But the degree of $\Psi^*_{p\ell}$ is $d^\ell + 1$. So $\Psi^*_{p\ell}$ has at least one point of primitive h-period ℓ. □

Corollary 2. *For a rational map* ϕ *with* $\deg\phi = d$*, under the hypotheses of Theorem 7, the polynomial* $\widetilde{\Psi^*_{p\ell}}$ *is nontrivial for all primes* ℓ *with at most* $d+6$ *exceptions.*

Proof. This follows immediately from the result above. □

As in the case of periodic points, a stronger result is possible if we restrict ourselves to characteristic 0. The following result parallels a proof by I.N. Baker for periodic points in [1].

Proposition 9. *Let* ϕ *be a rational map of degree* $d \ge 2$ *defined over a field* K *of characteristic* 0*, and let* h *be an automorphism for* ϕ *of prime order* p*. Suppose that* ϕ *has no points of primitive period* $n > 1$ *relative to* h *in* $\overline{K}$*. Then*

$$(d,n,p) \in \{(2,2,2),(2,2,3),(2,2,4),(2,3,2),(2,3,3),(2,3,4),(3,2,2),(3,2,3),(4,2,2)\}.$$

Proof. We begin by bounding p in terms of d. Any rational map ϕ of degree d has at most $d+1$ fixed points, and any automorphism of ϕ must permute these fixed points. So h can have order at most $d+1$.

Suppose that ϕ is as described, and that ϕ has no points of primitive period n relative to h. Then all roots of the (nontrivial) polynomial $\Psi_{pn}(x,y)$ are accounted for by points of primitive h-period $m<n$ or by points in $\mathrm{Fix}(h)$. Let

$$S = \{Q \in \mathbb{P}^1 : \Psi_{pn}(Q) = 0\},$$

and for each $Q \in S$, let

$$m_Q = \begin{cases} \text{the primitive } h\text{-period of } Q \text{ for } \phi & \text{if } Q \notin \mathrm{Fix}(h) \\ \text{the primitive period of } Q \text{ for } \phi \text{ (necessarily 1 or 2)} & \text{if } Q \in \mathrm{Fix}(h). \end{cases}$$

By lemma 5 and similar facts about periodic points, we know that each $m_Q \mid n$. So let

$$M = \{m \in \mathbb{Z} : 1 \le m < n \text{ and } m \mid n\}.$$

We now compute lower and upper bounds for

$$\sum_{Q\in S} \left(b_Q(pn) - b_Q\left(pm_Q\right)\right), \tag{3.34}$$

under the assumption that $Q \in S$ implies that $m_Q \in M$; that is, that there are no points of primitive h-period n. For the lower bound,

$$\sum_{Q\in S} b_Q(pn) = \deg \Psi_{pn} = (p-1)\left(d^n+1\right) \tag{3.35}$$

$$\begin{aligned} \sum_{Q\in S} b_Q(pm_Q) &= \sum_{m\in M} \sum_{\substack{m_Q=m \\ Q\in S}} b_Q(pm_Q) \\ &= \sum_{m\in M} \deg \Psi_{pm} \\ &\le \sum_{m\in M} (p-1)\left(d^m+1\right) \end{aligned} \tag{3.36}$$

Now, when $n=2$, the set $M=\{1\}$, so the final sum in equation (3.36) is exactly

$$(p-1)(d+1) = (p-1)\left(d^{n-1} + (n-1)\right).$$

If $n>2$, then $\gcd(n, n-1) = 1$ and so

$$\sum_{m\in M} \left(d^m+1\right) \le \sum_{i=1}^{n-2} \left(d^i+1\right) \le d^{n-1} + n - 1.$$

So we have our lower bound:

$$(p-1)\left(d^n - d^{n-1} - (n-1)\right) \le \sum_{Q\in S} \left(b_Q(pn) - b_Q\left(pm_Q\right)\right). \tag{3.37}$$

To compute the upper bound, we will use the assumption that all of the points are roots of Ψ_{pm} for some $m \in M$. Then from Lemmas 11 and 12 applied to the map ϕ^m, we see that $b_Q(pn) - b_Q(pm) > 0$ if and only if

$$\frac{\lambda_1\left(\phi^m, Q\right)}{\lambda_1\left(h^j, Q\right)}$$

is a primitive r^{th} root of unity for some r not divisible by p and some $1 \leq j \leq p-1$. Equation (3.18) (again applied to ϕ^m) shows that $\lambda_1(\phi^{pm}, Q)$ must then be a primitive r^{th} root of unity. In other words, Q must be on a rationally indifferent cycle of length pm.

Also, by Proposition 5, we know that $a_Q(pn) \geq b_Q(pn)$ for every n. So we may now compute the upper bound

$$\begin{aligned}
\sum_{Q \in S} \left(b_Q(pn) - b_Q\left(pm_Q\right)\right) &= \sum_{\substack{Q \in S \\ Q \text{ on a rationally indifferent cycle}}} \left(b_Q(pn) - b_Q\left(pm_Q\right)\right) \\
&\leq \sum_{\substack{Q \in S \\ Q \text{ on a rationally indifferent cycle}}} b_Q(pn) \\
&\leq \sum_{\substack{Q \in S \\ Q \text{ on a rationally indifferent cycle}}} a_Q(pn).
\end{aligned}$$

On page 146 of [2], Beardon provides exactly the upper bound we require; he shows that

$$\sum_{\substack{Q \in S \\ Q \text{ on a rationally indifferent cycle}}} a_Q(pn) \leq pn(d-1). \tag{3.38}$$

We now show that the inequality

$$(p-1)\left(d^n - d^{n-1} - (n-1)\right) \leq pn(d-1) \tag{3.39}$$

can never hold for $n \geq 2$ and $d > 4$.

Since $\frac{p-1}{p} \geq \frac{1}{2}$ and $\frac{1}{2}\left(d^n - d^{n-1} - (n-1)\right) \geq \frac{1}{2}\left(d^n - d^{n-1}\right) - n$, we may work instead with the inequality

$$\begin{aligned}
\frac{1}{2}\left(d^n - d^{n-1}\right) &\leq nd \\
\frac{1}{2}\left(d^{n-1} - d^{n-2}\right) &\leq n \\
\frac{d-1}{2} d^{n-2} &\leq n \\
2d^{n-2} &\leq n
\end{aligned} \tag{3.40}$$

where the last step follows from the assumption that $d > 4$. The function $2d^{n-2} - n$ is increasing with n and is 0 when $n = 2$. Going back to the original inequality (3.39), we check that for $n = 2$ and $d > 4$ it still cannot hold:

$$\begin{aligned}
\frac{1}{2}\left(d^2 - d - 1\right) &\leq 2(d-1) \\
d(d-1) - 1 &\leq 4(d-1) \\
(d-4)(d-1) - 1 &\leq 0
\end{aligned}$$

which clearly cannot hold for $d > 4$.

When $d = 4$, the inequality in equation (3.40) becomes $\frac{3}{2}2^{n-2} \leq n$. Again, we see that the function $\frac{3}{2}4^{n-2} - n$ is increasing with n and it is already positive when $n = 3$, so the inequality can hold only when $n = 2$. Given the bound on p, it is a simple matter to check that when $d = 4$, $n = 2$, and $p = 3$ or 5, then inequality (3.39) cannot hold. So when $d = 4$, $n = p = 2$ is the only possibility.

Similar computations show that when $d = 3$ and $n \geq 3$, and when $n = 2$ and $d \geq 5$, inequality (3.39) cannot hold. Given the bounds on p, this completes the proof. □

3.4 Reducibility for pure power functions

We are able to provide a complete description of how the dynatomic polynomials factor in the case of the pure power functions and their reciprocals. Note that both maps have the degree 2 automorphism $z \mapsto 1/z$. Additionally, $\phi(z) = z^d$ has a $z \mapsto \zeta_{d-1}$ automorphism and $\phi(z) = \frac{1}{z^d}$ has a $z \mapsto \zeta_{d+1}$ automorphism, where ζ_k represents a kth root of unity.)

Lemma 14. *Let $\phi(z) = z^d$ for $d \geq 2$. Then for $n > 1$,*

$$\Phi^*_{n,\phi}(z) = \prod_{\substack{k \mid d^n - 1 \\ k \nmid d^m - 1, m \mid n, m \neq n}} C_k(z)$$

Remark. We note that this fact has appeared in the literature, for example in [13]. But unable been to find a proof, we provide one here for completeness.

Proof. First we show that this holds for n prime.

$$\Phi^*_{n,\phi}(z) = \prod_{k \mid n} (z^{d^k} - z)^{\mu(n/k)} = \frac{z^{d^n - 1} - 1}{z^{d-1} - 1} = \frac{\prod_{k \mid d^n - 1} C_k(z)}{\prod_{k \mid d - 1} C_k(z)} = \prod_{\substack{k \mid d^n - 1 \\ k \nmid d^m - 1, m \mid n, m \neq n}} C_k(z)$$

Now assume that the result holds for all $n < N$. Since we have the result for primes, we assume N is composite, and write $N = p^e n$ for some prime p, with $e \geq 1$ and $p \nmid n$. If $k \mid N$ and $p^{e-1} \nmid k$, then $p^2 \mid (N/k)$, which gives $\mu(N/k) = 0$; in other words, k will not contribute to the product Φ^*_n. Further, if $p^{e-1}k \mid N$, then $k \mid pn$, so either $k = k_1$ or $k = pk_1$ for some $k_1 \mid n$, and these sets are disjoint since $p \nmid n$. Finally, note that since $p \nmid n$ and hence $p \nmid k$ for any $k \mid n$, we have $\mu(p^e n/p^{e-1}k) = \mu(pn/k) = -\mu(n/k)$, Putting this all together, we may compute

$$\begin{aligned}
\Phi^*_{N,\phi}(z) = \prod_{k \mid N} (z^{d^k} - z)^{\mu(N/k)} &= \left(\prod_{k \mid n} (z^{d^{(p^{e-1}k)}} - z)^{\mu(p^e n/p^{e-1}k)} \right) \left(\prod_{k \mid n} (z^{d^{(p^e k)}} - z)^{\mu(p^e n/p^e k)} \right) \\
&= \left(\prod_{k \mid n} \left(z^{\left(d^{p^{e-1}}\right)^k} - z \right)^{-\mu(n/k)} \right) \left(\prod_{k \mid n} \left(z^{\left(d^{p^e}\right)^k} - z \right)^{\mu(n/k)} \right)
\end{aligned}$$

$$= \left(\prod_{\substack{k \mid \left(d^{p^{e-1}}\right)^n - 1 \\ k \nmid \left(d^{p^{e-1}}\right)^m - 1, m \mid n, m \neq n}} \frac{1}{C_k(z)} \right) \left(\prod_{\substack{k \mid \left(d^{p^e}\right)^n - 1 \\ k \nmid \left(d^{p^e}\right)^m - 1, m \mid n, m \neq n}} C_k(z) \right)$$

$$= \prod_{\substack{k \mid d^N - 1 \\ k \nmid d^m - 1, m \mid N, m \neq N}} C_k(z)$$

The penultimate equality above follows from the induction hypothesis because $n < N$. The final equality follows from the fact that if $k \mid d^m - 1$ for some $m \mid N$ and $m \neq N$, then $k \mid d^{p^e m} - 1$ for some $m \mid n$ or $k \mid d^{p^{e-1} n} - 1$. (Note the divisors of $d^{p^{e-1} m} - 1$ for some $m \mid n$ are included in the first set.) □

Lemma 15. *Let $\phi(z) = \frac{1}{z^d}$ for $d \geq 2$. Then for $N > 2$,*

$$2 \nmid N \implies \Phi^*_{N,\phi}(z) = \prod_{\substack{k \mid d^N + 1 \\ k \nmid d^m + 1, m \mid N, m \neq N}} C_k(z) \tag{3.41}$$

$$N = 2n \text{ with } 2 \nmid n \implies \Phi^*_{N,\phi}(z) = \prod_{\substack{k \mid d^N - 1 \\ k \nmid d^{2m} - 1, m \mid n, m \neq n \\ k \nmid d^n + 1}} C_k(z) \tag{3.42}$$

$$N = 2^e n \text{ with } e \geq 2 \text{ and } 2 \nmid n \implies \Phi^*_{N,\phi}(z) = \prod_{\substack{k \mid d^N - 1 \\ k \nmid d^m - 1, m \mid N, m \neq N}} C_k(z) \tag{3.43}$$

Proof. If $\phi(z) = \frac{1}{z^d}$, then for k odd, we have $\phi^k(z) = \frac{1}{z^{d^k}}$, and for k even, we have $\phi^k(z) = z^{d^k}$. So we may calculate

$$\Phi^*_N(z) = \left(\prod_{\substack{k \mid N \\ 2 \mid k}} \left(z^{d^k} - z \right)^{\mu(N/k)} \right) \left(\prod_{\substack{k \mid N \\ 2 \nmid k}} \left(z^{d^k + 1} - 1 \right)^{\mu(N/k)} \right). \tag{3.44}$$

If $4 \mid N$, then for any odd divisor k of N, we have $\mu(N/k) = 0$, so the second product is empty. We may rewrite

$$\prod_{\substack{k \mid N \\ 2 \mid k}} \left(z^{d^k} - z \right)^{\mu(N/k)} = \left(\prod_{k \mid N} z^{\mu(N/k)} \right) \left(\prod_{k \mid N} \left(z^{d^k - 1} - 1 \right)^{\mu(N/k)} \right) = \prod_{k \mid N} \left(z^{d^k - 1} - 1 \right)^{\mu(N/k)},$$

which simplifies to the expression in equation (3.43) by the exact argument given in lemma 14.

If N is odd, it has no even divisors; so the first term is an empty product. The argument in this case follows word-for-word the argument in lemma 14, with $d^n - 1$ replaced by $d^N + 1$. Note that since N is odd, $d^m + 1 \mid d^N + 1$ when $m \mid N$.

It remains only to consider the case that $2 \mid N$ but $4 \nmid N$. So $N = 2n$ with n odd. Then any odd divisor k of N is simply a divisor of n. We see that for such divisors, $\mu(N/k) = \mu(2n/k) = -\mu(n/k)$. So the second term in equation (3.44) is

$$\begin{aligned}\prod_{\substack{k|N\\2\nmid k}}\left(z^{d^k+1}-1\right)^{\mu(N/k)} &= \prod_{k|n}\left(z^{d^k+1}-1\right)^{-\mu(n/k)}\\ &= \prod_{\substack{k|d^n+1\\k\nmid d^m+1, m|n}}\frac{1}{C_k(z)} \qquad (3.45)\end{aligned}$$

by the argument for the case when N is odd.

Similarly, we recognize that even divisors of N are of the form $2k$ where $k \mid n$, and in this case $\mu(N/2k) = \mu(2n/2k) = \mu(n/k)$. The first term in equation (3.44) then becomes

$$\begin{aligned}\prod_{\substack{k|N\\2|k}}\left(z^{d^k-1}-1\right)^{\mu(N/k)} &= \prod_{k|n}\left(z^{d^{2k}-1}-1\right)^{\mu(n/k)}\\ &= \prod_{\substack{k|d^N-1\\k\nmid d^{2m}-1, m|n}} C_k(z). \qquad (3.46)\end{aligned}$$

Multiplying equations (3.46) and (3.45), we get precisely the expression in equation (3.43). □

Corollary 3. *We assume* $\deg\phi = d \geq 2$.

1. *Let* $\phi(z) = z^d$. *If* $d > 2$, *then* $\Phi_n^*(z)$ *is reducible for every* n. *If* $d = 2$, *then* $\Phi_n^*(z)$ *is irreducible if and only if* $2^n - 1$ *is prime.*

2. *Let* $\phi(z) = \frac{1}{z^d}$. *If* $d > 2$, *then* $\Phi_n^*(z)$ *is reducible for every* n. *If* $d = 2$, *then* $\Phi_n^*(z)$ *is reducible for every* $n > 3$.

Proof. (1). $\Phi_1^*(z) = z^d - z$, which is reducible. Lemma 14 says that $\Phi_n^*(z)$ for $n > 1$ is irreducible if and only if $d^n - 1$ has no divisors other than those which divide $d^m - 1$ where $m \mid n$. We always have $d - 1 \mid d^n - 1$, and if $d > 2$, it's easy to see that the quotient $d^{n-1} + \cdots + d + 1$ does not divide $d^m - 1$ if $m < n$. So then $\Phi_n^*(z)$ is reducible for every n.

In the case $d = 2$, we see that if $2^n - 1$ is prime, then $\Phi_n^*(z) = C_{2^n-1}(z)$ is irreducible. If n is prime but $2^n - 1$ is not prime, then $2^n - 1$ clearly has a factor not of the form $2^m - 1$ with $m|n$. So then $\Phi_n^*(z)$ is reducible. Finally, if n is composite, let k be the smallest positive divisor of n. We argue as above that the quotient of $2^n - 1$ and $2^k - 1$ does not divide $2^m - 1$ for any $m \neq n$. So then $\Phi_n^*(z)$ has at least two nontrivial factors, namely $C_{2^n-1}(z)$ and $C_{(2^n-1)/(2^k-1)}(z)$.

(2). In this case, $\Phi_1^*(z) = z^{d+1} - 1$, which is reducible since $d \geq 2$. If $4 \mid n$, $2^n - 1$ is not prime, so the fact that $\Phi_n^*(z)$ is reducible follows from the fact that it is identical to Φ_n^* for the map $\phi(z) = z^d$, which is reducible in this case by the argument above.

If n is odd, we need to see that $d^n + 1$ has a factor which does not divid $d^m + 1$ for any $m \mid n$. Let k be the smallest nontrivial divisor of n. Then $(d^n + 1)/(d^k + 1) = d^{n-k} - d^{n-2k} + \cdots + 1$. For

this quotient to divide $d^m + 1$, it is certainly necessary that $n - k < m$, But with $n \geq 4$ and k the smallest divisor of n, we have $n - k \leq n/k$ which is the largest divisor of n. So we have at least two nontrivial factors of Φ_n^*, namely $C_{d^n+1}(z)$ and $C_{(d^n+1)/(d^k+1)}(z)$ with k the smallest positive divisor of n.

Finally, if $2 \mid n$ but $4 \nmid n$, we see from equation 3.42 that for m an odd divisor of n, we have $C_{d^m-1}(z) \mid \Phi_n^*(z)$. In particular, $C_{d-1}(z) \mid \Phi_n^*(z)$ is a nontrivial factor as long as $d > 2$. If $d = 2$, we must restrict to the case $n > 3$, in which case we are assured of an odd factor of n greater than one. □

3.5 An irreducibility result

We now focus on the case $\deg \phi = 2$.

Lemma 16. *Let ϕ be a rational map of degree $d = 2$ with a stabilizer group of order 2 and suppose* $\operatorname{char} K \neq 2$. *Then ϕ is* PGL_2*-conjugate to some map of the form*

$$\psi = \frac{z^2 + a}{az + 1} \tag{3.47}$$

Proof. Milnor shows in [11] that any degree-2 rational map with at least two fixed points is linearly conjugate to some map of the form $\frac{z^2+az}{bz+1}$, where a and b are the multipliers of the fixed points at 0 and ∞. The only map with a single fixed point has stabilizer group $\mathcal{S}_3$, so we may disregard this case.

We already argued on page 15 that ϕ must in fact have three distinct fixed points. So then, any element of $\mathrm{Aut}(\phi)$ must interchange two fixed points of ϕ (since it has order 2), and since any nontrivial element of PGL_2 cannot fix three points in $\mathbb{P}^1$. An automorphism must also preserve the multipliers of fixed points, so we see that if ϕ has a nontrivial automorphism, it necessarily has at least two multipliers that are equal. Given this fact, if ϕ has a nontrivial automorphism, we can choose a normal form for ϕ such that $\phi(z) = \frac{z^2+az}{az+1}$. □

Proposition 10. *Let ϕ be a rational map of degree $d = 2$, with an automorphism group of order 2, and let p be a prime such that $2^p - 1$ is prime. Then the dynatomic polynomial $\Phi_p^*(x, y)$ is irreducible.*

Proof. We use the normal form from Lemma 16. Suppose that $\Phi_n^*(x, y) = A(x, y)B(x, y)$ with $\deg(A), \deg(B) \geq 1$. Exactly as in theorem 6, we see that specializing to $a = 0$ will cause neither factor to become trivial.

Specializing to $a = 0$, we have the map $\phi(z) = z^2$, so by theorem 14, $\Phi_p^*(z)$ is a product of cyclotomic polynomials $C_m(z)$ such that $m \mid 2^p - 1$ but $m \not\mid 2^k - 1$ for any $k \mid p$. In the case that $2^p - 1$ is prime, then, we have simply the $(2^p - 1)^{st}$ cyclotomic polynomial, which is irreducible. □

Remark. For $n = 2$, the polynomial has a factor of $a + 1$, but since it is not defined for $a^2 = 1$ (this does not give a degree 2 map), this does not correspond to reducibility in the corresponding variety.

Chapter 4

Rational periodic points

4.1 Preliminaries

If two maps defined over a field K are linearly conjugate, then they must be linearly conjugate over K unless the maps have a nontrivial stabilizer group (see [20]). In the analysis of rational periodic points for quadratic polynomials in [14], [7], and [18], the authors use the fact that every quadratic polynomial is linearly conjugate over $\mathbb{Q}$ to a unique polynomial of the form $f_c(z) = z^2 + c$ with $c \in \mathbb{Q}$. Rational periodic points are in one-to-one correspondence, so it is enough to analyze the existence (or nonexistence) of rational periodic points for the family f_c.

In the case of rational maps with a nontrivial stabilizer group, the situation is more complicated. Up to conjugation by $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ this is a one-parameter family; but, as we have seen in the example on page 4, that equivalence is inadequate for analyzing rational periodic points. We must worry about twists of the one-parameter family, as described in the following lemma.

Lemma 17. *Let K be a field with $\mathrm{char}(K) \neq 2, 3$ and let ϕ be a rational map of degree 2 defined over K. Then $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$ if and only if ϕ is linearly conjugate over K to some map of the form*

$$\phi_{k,b}(z) = kz + \frac{b}{z} \tag{4.1}$$

with $k \in K \smallsetminus \{0, -1/2\}$ and $b \in K^*$. Furthermore, two such maps $\phi_{k,b}$ and $\phi_{k',b'}$ are linearly conjugate over K if and only if $k = k'$ and $b/b' \in (K^*)^2$.

Remark. Note that for fixed k, all maps of the form $\phi_{k,b}(z)$ are linearly conjugate over $\overline{K}$. Conjugate by $f_b(z) = \frac{z}{\sqrt{b}}$ to see that

$$\phi_{k,1}^{f_b}(z) = kz + \frac{b}{z} = \phi_{k,b}(z). \tag{4.2}$$

The content of the lemma, then, is developing a normal form that incorporates the quadratic twists, allowing us to examine rational periodic and preperiodic points. By abuse of notation, we will say that maps $\phi(z)$ as described in the lemma are linearly conjugate over K to a unique map of the form $\phi_{k,b}(z)$ with $k \in K \smallsetminus \{0, -1/2\}$ and $b \in K^*/(K^*)^2$.

Proof. First we prove that $\mathrm{Aut}(\phi)$ contains a subgroup isomorphic to $\boldsymbol{\mu}_2$ if and only if ϕ is linearly conjugate to some map of the form given in (4.1), with $b, k \in \overline{K}$ and $bk \neq 0$. One direction is clear: $z \mapsto -z$ is an automorhpism of $\phi_{b,k}$. By the remarks above, if ϕ is linearly conjugate to some $\phi_{k,b}$, then $\mathrm{Aut}(\phi) \cong \mathrm{Aut}(\phi_{k,b}) \supseteq \boldsymbol{\mu}_2$.

We generalize Milnor's proof in [11] that a quadratic rational map defined over $\mathbb{C}$ possesses a nontrivial automorphism if and only if it is linearly conjugate to a map in the unique normal form $\phi(z) = k(z + z^{-1})$ with $k \in \mathbb{C} \smallsetminus \{0\}$. $\mathrm{Aut}(\phi)$ contains an element f of order 2. By, for example, Theorem 3.1 of [20] and using the fact that $\mathrm{char}(K) \neq 2$, $\langle f \rangle$ is conjugate to $\langle -z \rangle$.

Let $g \in \mathrm{PGL}_2$ such that $g^{-1} f g = -z$. Then $\mathrm{Aut}(\phi^g) \supseteq \langle -z \rangle$. That is,

$$\phi^g(-z) = -\phi^g(z),$$

so ϕ^g must be an odd function. Writing $\phi^g(z) = F(z)/G(z)$ with $F, G \in K[z]$, we see that $\phi^g(z)$ is odd if and only if $F(z)$ is even and $G(z)$ is odd or vice-versa. If $F(z)$ is odd, then we may conjugate by $h(z) = 1/z$ to get

$$\left(\phi^g\right)^h(z) = (\text{even})/(\text{odd}).$$

So $\phi(z)$ is linearly conjugate to a map of the form

$$\phi_{k,b}(z) = \frac{kz^2 + b}{z} = kz + \frac{b}{z}. \tag{4.3}$$

Clearly $kb \neq 0$ because $\deg(\phi) = \deg(\phi_{k,b}) = 2$.

It is easy to check that the multipliers of the three fixed points for $\phi(z)$ are $\{2k-1, 2k-1, 1/k\}$. Linearly conjugate maps must have the same set of fixed-point multipliers, so for a given map $\phi(z)$ as described in the theorem, there is in fact a *unique* nonzero k such that $\phi(z)$ is linearly conjugate to a map of the form given above.

We claim that in fact $k \in K^*$. Let σ_1, σ_2, and σ_3 be the three symmetric functions of the multipliers. From [20], we know that the moduli space of degree-2 rational maps up to linear equivalence is isomorphic to $\mathbb{A}^2$, with coordinates (σ_1, σ_2). If $\phi(z)$ is defined over K, then it necessarily corresponds to a rational point in this moduli space, so σ_1 and σ_2 are both K-rational. Also from [11] we know that $\sigma_3 + 2 = \sigma_1$. (this is proved over $\mathbb{C}$, but it is a purely algebraic statement so the result holds over any field). Therefore, the multipliers are the roots of a monic cubic polynomial with coefficients in K, and $2k-1$ is a multiple root. Since $\mathrm{char}\, K \neq 2, 3$, the polynomial must split into three linear factors, and we conclude that $k \in K^*$ as desired.

All of the above holds for any ϕ with $\mathrm{Aut}(\phi) \supseteq \boldsymbol{\mu}_2$. We now show that $\mathrm{Aut}(\phi_{k,b}) \supsetneq \boldsymbol{\mu}_2$ if and only if $k = -1/2$. Again, we generalize a proof of Milnor's in [11].

By the remark above, $\phi_{-1/2,b}(z)$ is linearly conjugate to $\phi_{-1/2,-1/2}(z)$. Let $f(z) = (z+1)/(z-1)$. It is an easy matter to check that

$$\phi^f_{-1/2,-1/2}(z) = \frac{1}{z^2}.$$

We note that $\mathrm{Aut}(1/z^2) \supseteq \mathcal{S}_3$ since $\mathrm{Aut}(1/z^2) \supseteq \langle 1/z, \zeta_3 z \rangle$ with ζ_3 a primitive cube root of unity. (In fact, $\mathrm{Aut}(1/z^2) \cong \mathcal{S}_3$.) Since $\mathrm{char}(K) \neq 3$ the group $\langle \zeta_3 z \rangle$ is linearly conjugate to some group $G \subsetneq \mathrm{Aut}(\phi_{-1/2,b})$ of order 3, so $\mathrm{Aut}(\phi_{-1/2,b}) \supsetneq \boldsymbol{\mu}_2$.

Now consider some $\phi_{k,b}$ with $\mathrm{Aut}(\phi_{k,b}) \supsetneq \boldsymbol{\mu}_2$. For any rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ and any $f \in \mathrm{Aut}(\phi)$, f permutes the critical points of ϕ. In this case, the critical points of $\phi_{k,b}$ are $\pm\sqrt{b/k}$, which are interchanged by the automorphism $z \mapsto -z$. So using Milnor's notation, we have a subgroup $\mathrm{Aut}^0(\phi_{k,b}) \subset \mathrm{Aut}(\phi_{k,b})$ of index ≤ 2, consisting of automorphisms which fix the two critical points.

Choose $f \in \mathrm{PGL}_2$ such that f sends the critical points to $\{0, \infty\}$, and let $\psi = \phi_{k,b}^f$. Consider some nontrivial $g \in \mathrm{Aut}^0(\psi)$. Since g fixes 0 and ∞, we see that $g(z) = \lambda z$ for some $\lambda \neq 0$, and since g is nontrivial we see also that $\lambda \neq 1$. Then $g \in \mathrm{Aut}(\psi)$ means that $\psi(\lambda z) = \lambda\psi(z)$, so in particular $\psi(0) \in \{0, \infty\}$ and $\psi(\infty) \in \{0, \infty\}$. If ψ fixes both 0 and ∞, then $\psi(z) = \alpha z^2$ for some $\alpha \neq 0$. But then we must have $\lambda = 1$, which contradicts g being nontrivial.

So instead we have $\psi(0) = \infty$ and $\psi(\infty) = 0$, which means that $\psi(z) = \alpha/z^2$, which is conjugate to $1/z^2$. But we have already seen that $z \mapsto 1/z^2$ is conjugate to $\phi_{-1/2,-1/2}(z)$, and that the k value is unique. For any other $k \in K^*$, then, it follows that the stabilizer group is exactly $\langle -z \rangle$.

Now define

$$\mathrm{Twist}(\phi/K) = \left\{ \begin{array}{c} K\text{-equivalence classes of maps } \psi \text{ such that} \\ \psi \text{ is } \overline{K}\text{-equivalent to } \phi \end{array} \right\}.$$

Let $\phi_{k,1}(z) = kz + z^{-1} \in K(z)$ with $k \in K \smallsetminus \{0, -1/2\}$. We claim that there is an isomorphism

$$K^*/(K^*)^2 \xrightarrow{\sim} \mathrm{Twist}(\phi_{k,1}/K),$$

and that in fact each K-equivalence class corresponds to a unique map of the form

$$\phi_{k,b}(z) = kz + \frac{b}{z} \qquad \text{with } b \in K^*/\left(K^*\right)^2.$$

This will complete the proof of the lemma. Any map $\phi(z) \in K(z)$ with the given automorphism group is $\overline{K}$-equivalent to some map $\phi_{k,b}(z)$, which in turn is conjugate to $\phi_{k,1} \in K(z)$. The map ϕ is therefore in some equivalence class of $\mathrm{Twist}(\phi_{k,1}/K)$, and hence must be K-equivalent to a map of the given form. The following argument is adapted from a similar one in Silverman in [22].

First, we show that there is an injection

$$K^*/(K^*)^2 \hookrightarrow \mathrm{Twist}(\phi_{k,1}/K). \tag{4.4}$$

For a fixed k, all $\phi_{k,b}$ are linearly conjugate (over $\overline{K}$) to $\phi_{k,1}$, so we have a map of sets

$$\begin{aligned} K^* &\longrightarrow \mathrm{Twist}(\phi_{k,1}/K) \\ b &\longmapsto [\phi_{k,b}]_K, \end{aligned} \tag{4.5}$$

where $[\phi_{k,b}]_K$ represents the equivalence class of $\phi_{k,b}$ in $\mathrm{Twist}(\phi/K)$. If $b/c \in (K^*)^2$, then $\phi_{k,b}$ and $\phi_{k,c}$ are K-linearly equivalent. Let $f(z) = z\sqrt{b/c} \in \mathrm{PGL}_2(K)$; then

$$\phi_{k,c} = \phi_{k,b}^f.$$

So (4.5) induces a well-defined map

$$K^*/(K^*)^2 \longrightarrow \mathrm{Twist}(\phi_{k,1}/K).$$

We now use the fact that if two rational maps are K-linearly equivalent, then their n-periodic points generate the same field extension of K. Clearly

$$\mathrm{Per}_n(\phi^f) = \{f^{-1}(P) : P \in \mathrm{Per}_n(\phi)\}.$$

With $f \in \mathrm{PGL}_2(K)$, P and $f^{-1}(P)$ must generate the same extension.

Assume first that $k \neq 1$. Then the finite fixed points of $\phi_{k,b}(z)$ are given by

$$z = \pm\frac{\sqrt{b}}{\sqrt{1-k}}.$$

Hence if $\phi_{k,b}$ and $\phi_{k,c}$ are K-linearly equivalent, then $K\left(\frac{\sqrt{b}}{\sqrt{1-k}}\right)$ and $K\left(\frac{\sqrt{c}}{\sqrt{1-k}}\right)$ are the same, which holds if and only if $b/c \in (K^*)^2$ (we are again using the fact that $\mathrm{char}(K) \neq 2$). So we conclude that (4.4) is an injection, as claimed.

If $k = 1$, we must use the points of period 2 since the point at infinity is the only one fixed by $\phi_{1,b}(z)$. We calculate the second dynatomic polynomial $\Phi_2(x, y) = 2x^2 + by^2$, so the period-2 points are

$$z = \pm\sqrt{-\frac{b}{2}}.$$

The argument above shows that if $\phi_{1,b}$ is K-equivalent to $\phi_{1,c}$, then $b/c \in (K^*)^2$. So indeed the map in (4.4) is an injection.

Now, in [20], we find that

$$\mathrm{Twist}(\phi/K) \hookrightarrow H^1\left(G_K, \mathrm{Aut}(\phi)\right). \tag{4.6}$$

Take $[\psi]_K \in \mathrm{Twist}(\phi/K)$ with $\psi = \phi^f$ for some $f \in \mathrm{PGL}_2(\overline{K})$. Then $[\psi]_K$ maps to the cocycle $\sigma \mapsto f^{-1}f^\sigma$. In this case,

$$H^1\left(G_K, \mathrm{Aut}(\phi_{k,1})\right) = H^1\left(G_K, \boldsymbol{\mu}_2\right)$$

By standard results in Galois cohomology (see, for example, [19]), we have an isomorphism.

$$\begin{aligned} K^*/(K^*)^2 &\xrightarrow{\sim} H^1\left(G_K, \boldsymbol{\mu}_2\right) \\ b &\longmapsto \left(\sigma \mapsto \frac{\sigma\left(\sqrt{b}\right)}{\sqrt{b}}\right). \end{aligned} \tag{4.7}$$

By Hilbert's Theorem 90, every cocycle is equivalent to one of the form $\sigma \mapsto \frac{\sigma(\sqrt{b})}{\sqrt{b}}$ for some $b \in K^*/(K^*)^2$, so we map this cocycle back to b.

We need to show that the two injections in (4.4) and (4.6) are inverses of each other. Begin with some $b \in K^*/(K^*)^2$, define $f_b(z) = \frac{z}{\sqrt{b}} \in \mathrm{PGL}_2$ and consider $\phi_{k,1}^{f_b} = \phi_{k,b}$. Then $[\phi_{k,b}]_K \in$

$\mathrm{Twist}(\phi/K)$, and so $[\phi_{k,b}]_K$ maps in (4.6) to the cocycle $f_b^{-1}f_b^\sigma$, which maps by the isomorphism in (4.7) to b. Then in (4.4), we see that $b \mapsto \phi_{k,b}$.

Reasoning in the oppostie direction, begin with some $[\psi]_K \in \mathrm{Twist}(\phi_{k,1}/K)$. Choose a representative $\psi \in [\psi]_K$, and find f such that $\phi^f = \psi$. Then by (4.6), $[\psi]_K$ maps to the cocycle $\left(\sigma \mapsto f^{-1}f^\sigma\right)$. By the isomorphism in (4.7), this is equivalent to a cocycle of the form

$$\left(\sigma \mapsto \frac{\sigma\left(\sqrt{b}\right)}{\sqrt{b}}\right)$$

for some $b \in K^*/(K^*)^2$. Note that $\phi_{k,b}$ also maps to this cocycle, so by the injectivity of (4.6), $\phi_{k,b} \in [\psi]_K$. Now we see that the given cocycle maps via the isomorphism to b, which maps by the injection in (4.4) to $\phi_{k,b} \in [\psi]_K$. □

4.2 Rational periodic points

From now on, we take $\phi(z) \in \mathbb{Q}(z)$ to be a rational map of degree 2 satisfying $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$. If we wish to examine rational periodic points for ϕ, by Lemma 17 it is enough to examine the case $\phi(z) = kz + \frac{b}{z}$, for $k \in \mathbb{Q} \smallsetminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. We will use $\phi(z) = kz + \frac{b}{z}$ and the homogeneous form $\phi(x, y) = [kx^2 + by^2 : xy]$ interchangeably.

Proposition 11. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q}^*$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then*

(a) For all k and b, the point at infinity is a rational fixed point for $\phi(z)$.

(b) If $b = 1 - k$, then $\phi(z)$ has two finite rational fixed points; otherwise, $\phi(z)$ has no finite rational fixed points.

Proof. Consider the dynatomic polynomial $\Phi_1^*(x, y) = (k - 1)x^2y + by^3$. Roots of this polynomial are precisely the fixed points of $\phi(x, y)$. We see that $P = [1 : 0]$, the point at infinity, is always a root. If $k = 1$, then P is a triple root of the polynomial. (So for $k = 1$ we have no finite fixed points at all.)

We now dehomogenize to find the finite fixed points for $k \neq 1$.

$$\Phi_1^*(z) = (k - 1)z^2 + b.$$

Solving $\Phi_1^*(z) = 0$ for z, we find $z = \pm\sqrt{\frac{b}{1-k}}$, which is rational precisely when $\frac{b}{1-k} \in (\mathbb{Q}^*)^2$. The two finite fixed points are always distinct, since $b \neq 0$. From Lemma 17, this is equivalent to $b = 1 - k$. □

Remark. Proposition 11 says that every degree-2 rational map defined over $\mathbb{Q}$ with automorphism group $\boldsymbol{\mu}_2$ has at least one rational fixed point, since ϕ must be linearly conjugate over K to some map of the form $\phi_{k,b}$ and the fixed point at infinity must map to some rational fixed point of ϕ. This property, which is quite different from most one-parameter families of rational maps, can be explained more intrinsically.

First, if $\mathrm{Aut}(\phi) = \langle f \rangle \cong \boldsymbol{\mu}_2$, then $f \in \mathrm{PGL}_2(\mathbb{Q})$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then

$$\begin{aligned} \phi &= \phi^\sigma && \text{since } \phi \text{ is defined over } \mathbb{Q} \\ &= (\phi^f)^\sigma = (\phi^\sigma)^{f^\sigma} = \phi^{f^\sigma} \end{aligned}$$

So $f^\sigma \in \mathrm{Aut}(\phi$, meaning that $f^\sigma \in \{\mathrm{id}, f\}$. Since f^σ must have order 2, $f = f^\sigma$, and so f is defined over $\mathbb{Q}$ as well.

Now, f must permute the fixed points of ϕ. If ϕ has only one fixed point, clearly f fixes that. If ϕ has three fixed points, f must interchange two of them and fix the third since f has order two. (Recall that ϕ cannot have exactly two fixed points by Proposition 11). In any case, there is exactly one point P fixed by both f and ϕ. We claim that P is a rational point.

Again, let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then

$$\begin{aligned} f(P^\sigma) &= (f(P))^\sigma && \text{since } f \text{ is defined over } \mathbb{Q} \\ &= P^\sigma \end{aligned}$$

The same calculation works for $\phi(P^\sigma)$, so P^σ is the common fixed point of f and ϕ. In other words, $P^\sigma = P$.

Proposition 12. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q}^*$, and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then $\phi(z)$ has a rational point of primitive period 2 if and only if $b = -(k+1)$.*

Proof. Begin with the dynatomic polynomial

$$\Phi_2^*(x, y) = k\left((k+1)x^2 + by^2\right).$$

Roots of this polynomial are precisely the points of formal period 2 for $\phi(x, y)$. We see that $P = [1 : 0]$, the point at infinity, is a root if and only if $k = -1$. We know that $P = [1 : 0]$ is actually a fixed point, so for $k = -1$, we have no two-cycle. Further, for a fixed point have formal period 2, it must have multiplier -1, which can happen only when $k = -1$. Recall that the multipliers are 2k-1, 2k-1 and 1/k.

We now dehomogenize to find the points of period 2 if $k \neq -1$. Solving

$$\Phi_2^*(z) = k\left((k+1)z^2 + b\right) = 0$$

for z, we find $z = \pm\sqrt{\frac{-b}{k+1}}$, which is rational precisely when $\frac{-b}{k+1} \in (\mathbb{Q}^*)^2$, and it has two distinct roots since $b \neq 0$. Again, because b is defined only modulo squares, this is equivalent to $b = -(k+1)$. $\square$

Theorem 8. *Let $\phi(z) = kz + \frac{b}{z}$ with $k, b \in \mathbb{Q}^*$. Then $\phi(z)$ has no rational point of primitive period 3.*

Proof. We compute the third dynatomic polynomial for $\phi(z) = kz + \frac{b}{z}$,

$$\begin{aligned} \Phi_3^*(b, k, z) =& k^6z^6 + k^5z^6 + k^4z^6 + 3bk^5z^4 + 2bk^4z^4 + 3bk^3z^4 \\ &+ bkz^4 + 3b^2k^4z^2 + b^2k^3z^2 + b^2z^2 + 2b^2k^2z^2 - b^2kz^2 + b^3k^3. \end{aligned}$$

We wish to show that there are no rational (allowable) values of b, k, and z such that $\Phi_3^*(b,k,z)=0$. Since the parameter b simply represents quadratic twists of the curve $\Phi_3^*=0$, properties like the reducibility and genus of the curve are independent of b. By Theorem 10, we know that the $\Phi_3^*=0$ is irreducible.

Since $\Phi_3^*=0$ is even in z, by letting $x=z^2$ we see that it covers a curve of genus 2.

$$\begin{aligned}\Theta_3^*(b,k,x) &= k^6x^3+k^5x^3+k^4x^3+3bk^5x^2+2bk^4x^2+3bk^3x^2+bkx^2\\ &\quad +3b^2k^4x+b^2k^3x+b^2x+2b^2k^2x-b^2kx+b^3k^3\\ &=0.\end{aligned}$$

Let F be the curve $\Phi_3^*=0$ and C be the curve $\Theta_3^*=0$. We have a map

$$g: F \longrightarrow C.$$

To find the rational points of F, then, it is sufficient to find the rational points of the genus 2 curve C, and then then to find their preimages under

$$g: F(\mathbb{Q}) \longrightarrow C(\mathbb{Q}).$$

A change of coordinates $x=bx$ and dividing by b^3 removes the dependence on b

$$k^6x^3+k^5x^3+k^4x^3+3k^5x^2+2k^4x^2+3k^3x^2+kx^2+3k^4x+k^3x+x+2k^2x-kx+k^3=0.$$

And another change of coordinates $x=x/k$ and multiplying by k drops the total degree a bit

$$\begin{aligned}G(k,x) &= k^4x^3+k^3x^3+k^2x^3+3k^4x^2+2k^3x^2+3k^2x^2\\ &\quad +x^2+3k^4x+k^3x+x+2k^2x-kx+k^4\\ &=0.\end{aligned}$$

Simultaneously solving $G(k,x)=\frac{\partial}{\partial x}G(k,x)=\frac{\partial}{\partial k}G(k,x)=0$ shows that the curve has no finite singular points. However, it has two singularities on the line at infinity: one of multiplicity four at $[1:0:0]$ and one of multiplicity three at $[0:1:0]$. The curve has genus 2, so it must be birational to a hyperelliptic curve.

Repeatedly blowing up the singularities and changing coordinates allows us to find the birational hyperelliptic curve C_1 defined by

$$v^2=u^6+2u^5-5u^4+10u^3-10u^2+4u-1. \tag{4.8}$$

Here is a sketch of the relevant substitutions. Note that with each substitution, the singularities become less severe. Since the two singularities are at infinity, take a different affine piece. Consider the affine slice with $k=1$, which gives the curve

$$y^3+xy^6-xy^5+2xy^4+xy^3+3xy^2+x^2y^5+3x^2y^3+2x^2y^2+3x^2y+x^3y^2+x^3y+x^3=0.$$

This curve has a triple-point at $(0,0)$, so we substitute $x = x_1 y$ and divide by y^3, which gives another model

$$1 + x_1y^4 - x_1y^3 + 2y^2x_1 + x_1y + 3x_1 + x_1^2y^4 + 3y^2x_1^2 + 2yx_1^2 + 3x_1^2 + y^2x_1^3 + yx_1^3 + x_1^3 = 0.$$

This curve has singularities at $[1:0:0]$, $[-1:0:1]$, and $[0,1,0]$. Take the affine slice $x_1 = 1$ to get another model

$$z^6 + 3z^5 + 3z^4 + z^3 + yz^4 + 2yz^3 + yz^2 + 2y^2z^3 + 3y^2z^2 + y^2z - y^3z^2 + y^4z + y^4 = 0$$

which has a singularity at $(0,-1)$. We substitute $z = z_1 - 1$ to move the singularity to $(0,0)$ and then substitute $z_1 = z_2 y$ and divide by y^3 to get

$$z_2^2 + 2y_1z_2^2 - z_2 - y_1^2z_2^2 + 2y_1z_2 + y_1^3z_2^2 - y_1^2z_2 + z_2^3 - 1 = 0.$$

This curve has a singularity at $(0,-1)$, so again substitute $z_2 = z_3 - 1$ to move the singularity to $(0,0)$ and then blow up again with $z_3 = y_1z_4$ and divide by y_1^2 to get

$$-2z_4^2 + 2y_1z_4^2 - 2z_4 - y_1^2z_4^2 + y_1z_4 + y_1^3z_4^2 - 2y_1^2z_4 + y_1 + y_1z_4^3 = 0.$$

This curve has two double-points at infinity, so we take another affine slice $z_4 = 1$ to get the model

$$y_1x_2^4 - 2x_2^4 + y_1x_2^3 - 2y_1^2x_2^2 - 2x_2^3 + 2y_1x_2^2 - y_1^2x_2 + y_1^3 + y_1x_2 = 0$$

which has a node at $(0,0)$. Substituting $y_1 = y_2x_2$ and dividing by x_2^2 gives

$$y_2x_2^3 - 2x_2^2 + y_2x_2^2 - 2x_2^2y_2^2 - 2x_2 + 2y_2x_2 - x_2y_2^2 + x_2y_2^3 + y_2 = 0.$$

A calculation shows that this curve has a node at infinity along the line $x_2 - y_2 = 0$, which we move to an axis by substituting $y_2 = y_3 + x_2$ to get

$$-x_2^2y_3 + x_2^2y_3^2 - x_2 + 2y_3x_2 - x_2y_3^2 + x_2y_3^3 + y_3 = 0. \tag{4.9}$$

This curve is quadratic in x_2, so it is birational to the curve C_1 defined by

$$v^2 = u^6 - 2u^5 + 5u^4 - 10u^3 + 10u^2 - 4u + 1,$$

where the right hand side of the equation above is the x_2-discriminant of equation (4.9), with $u = y_3$.

C_1 has a few obvious rational points, namely $(0,\pm1)$ and $(1,\pm1)$. Also, since the degree is even in u, the curve has two points at infinity, both of which are rational points because when writing the curve as $v^2 = f(u)$ the lead coefficient of $f(u)$ is a square in $\mathbb{Q}$. We call these points ∞^+ and ∞^-.

Magma gives a bound on the rank of $J(\mathbb{Q})$, the Mordell-Weil group of the Jacobian, as 0; and so the rank is 0. Magma also computes that the torsion subgroup has order 21, giving the entire set of

points on $J(\mathbb{Q})$ as:

$$\begin{array}{ccc}
\text{identity}, & \{\infty^+,\infty^+\}, & \{\infty^-,\infty^-\}, \\
\{(0,1),(0,1)\}, & \{(0,-1),(0,-1)\}, & \{(1,1),(1,1)\}, \\
\{(1,-1),(1,-1)\}, & \{\infty^+,(0,1)\}, & \{\infty^+,(0,-1)\}, \\
\{\infty^+,(1,1)\}, & \{\infty^+,(1,-1)\}, & \{\infty^-,(0,1)\}, \\
\{\infty^-,(0,-1)\}, & \{\infty^-,(1,1)\}, & \{\infty^-,(1,-1)\}, \\
\{(0,1),(1,1)\}, & \{(0,1),(1,-1)\}, & \{(\frac{1+\sqrt{-3}}{2},\frac{3+\sqrt{-3}}{2}),(\frac{1-\sqrt{-3}}{2},\frac{3-\sqrt{-3}}{2})\}, \\
\{(0,-1),(1,1)\}, & \{(0,-1),(1,-1)\}, & \{\frac{1+\sqrt{-3}}{2},\frac{-3-\sqrt{-3}}{2}),(\frac{1+\sqrt{-3}}{2},\frac{-3+\sqrt{-3}}{2})\}.
\end{array}$$

As usual, $\{P_1, P_2\}$ is shorthand for the divisor class containing $P_1 + P_2 - \infty^+ - \infty^-$.

There can therefore be no other points in $C_1(\mathbb{Q})$, apart from the six points already found, since any other points in $C_1(\mathbb{Q})$ would give rise to additional members of $J(\mathbb{Q})$. We need to find the corresponding rational points on the curve F. The change of coordinates from $G(k,x) = 0$ to C_1 is

$$x = \frac{-2u^4 + 5u^3 - 5u^2 + 2u - 1 + v}{2u^2(u^2 - u + 1)} \tag{4.10}$$

$$k = \frac{1 - u^2 + u^3 - 2u + v}{4u(1-u)}. \tag{4.11}$$

Using the equation for C_1, we can find alternate forms for x and k as well,

$$x = \frac{2(u-1)^4}{-2u^4 + 5u^3 - 5u^2 + 2u - 1 - v} \tag{4.12}$$

$$k = \frac{2u(u-1)}{1 - u^2 + u^3 - 2u - v}. \tag{4.13}$$

We see that at $(u,v) = (0,1)$ and $(u,v) = (1,-1)$, the denominator of equation (4.11) vanishes but the numerator does not, so k has a pole at these points. Similarly at $(u,v) = (0,-1)$ and $(u,v) = (1,1)$, the numerator of equation (4.13) vanishes but the denominator does not, so these points give $k = 0$.

It remains to investigate the points ∞^+ and ∞^-. At ∞^+, we have the formal expansion

$$v = u^3 - u^2 + 2u - 3 + 4u^{-2} + \cdots$$

Substituting this into equation (4.11), we find that

$$k = -\frac{u}{2} + \text{powers of } u^{-1},$$

so k has a pole at ∞^+.

Similarly, at ∞^-, we have the formal expansion

$$v = -(u^3 - u^2 + 2u - 3 + 4u^{-2} + \cdots)$$

Substituting this into equation (4.11), we find that

$$k = 0 + \text{powers of } u^{-1},$$

so the point at ∞^- pulls back to $k = 0$.

The curve $G(k, x) = 0$ therefore has just four rational points: $(0, 0)$, $(0, -1)$, and the two points at infinity. The k-values for this curve correspond exactly to the k-values on our original curve C, and $k = 0$ does not give a rational map of degree 2. So no rational maps ϕ have a rational point of primitive (or even formal) period 3. □

This result is quite different from the case of quadratic polynomials. There is a one-parameter family of c values such that $f_c(z) = z^2 + c$ has a rational point of primitive period 3, in which case it has exactly three such points [12]. If a map $\phi_{k,b}$ were to have a rational point of primitive period 3, it would necessarily have six of them, since the three cycles are related by the autmorphism:

$$\{\alpha, \phi(\alpha), \phi^2(\alpha)\} \quad \text{and} \quad \{-\alpha, -\phi(\alpha), -\phi^2(\alpha)\}.$$

By results in Section 4.3, this would give rise to at least 14 rational preperiodic points, which would seem to be "too many" for a rational map of degree 2.

The next theorem also provides a contrast to the quadratic polynomial case, in which $f_c(z)$ can never have a rational point of primitive period 4.

Theorem 9. *Let $\phi(z) = kz + \frac{b}{z}$ with $k \in \mathbb{Q}^*$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

(a) There is a one-parameter family of such maps

$$\phi_m(z) = \frac{2mz}{m^2 - 1} - \frac{m}{z(m^4 - 1)}$$

with a rational point of primitive period 4. In this case, $\phi(z)$ has exactly four points of primitive period 4.

(b) $\phi(z)$ cannot have more than four points of primitive period 4.

Proof. We first calculate the fourth dynatomic polynomial for ϕ, which we know to be reducible by results in Chapter **??**. One factor parameterizes maps and four cycles where z and $-z$ are on the same cycle, and the other factor parameterizes maps and four cycles where z and $-z$ are on different cycles.

$$\Phi_4^*(b, k, z) = \Psi_4^*(b, k, z)\Lambda_4^*(b, k, z) \tag{4.14}$$

$$\Psi_4^*(b, k, z) = k^3z^4 + kz^4 + 2bk^2z^2 + 2bz^2 + b^2k \tag{4.15}$$

$$\begin{aligned}\Lambda_4^*(b, k, z) = {} & z^8k^9 + 4bz^6k^8 + bz^6k^4 + 2bz^6k^6 + 6b^2z^4k^7 + 4b^2z^4k^5 \\ & + 3b^2z^4k^3 + b^2z^4k + 4b^3z^2k^6 + 2b^3z^2k^4 + b^3z^2k^2 + b^3z^2 + b^4k^5\end{aligned} \tag{4.16}$$

We will show that there is a one-parameter family of k and b values for which Ψ_4^* has four rational z roots, and that there are no maps for which Λ_4^* has rational z roots.

Ψ_4^* even in z, so substitute $z^2 = x$ and consider the curve

$$k^3x^2 + kx^2 + 2bk^2x + 2bx + b^2k = 0.$$

A change of coordinates $x = bx_1$ and dividing by b^2 removes dependence on b, so we have

$$k^3x_1^2 + kx_1^2 + 2k^2x_1 + 2x_1 + k = 0.$$

And once again, the change $x_2 = \frac{x_1}{k}$ and multiplying by k drops the total degree, leaving the model

$$k^2x_2^2 + x_2^2 + 2k^2x_2 + 2x_2 + k^2 = 0.$$

This is already quadratic in x_2, with discriminant $4(1+k^2)$, so it is birational to the rational curve

$$d^2 = (1+k^2).$$

This curve is parameterized by $k = \frac{2m}{m^2-1}$ and $d = \frac{m^2+1}{m^2-1}$.

Tracing back the change of coordinates, we find

$$x_2 = \frac{-2(1+k^2) \pm 2d}{2(1+k^2)} = -1 \pm \frac{d}{1+k^2}. \tag{4.17}$$

So let

$$x_2 = -1 + \frac{d}{1+k^2} = -\frac{2}{m^2+1};$$

which means that

$$\begin{aligned} x_1 = kx_2 &= -\frac{4m}{m^4-1}, \\ bx &= -\frac{4m}{m^4-1}. \end{aligned}$$

Since $x = z^2$ is a square, and b is taken as a number modulo squares, we may simply let $b = -\frac{m}{m^4-1}$. (Note that taking the other root for x_2 in (4.17) results in the same b value modulo squares.) Let

$$\phi_m(z) = kz + \frac{b}{z} = \frac{2mz}{m^2-1} - \frac{m}{z(m^4-1)}. \tag{4.18}$$

We now recalculate the fourth dynatomic polynomial for this $\phi_m(z)$

$$\begin{aligned} \Phi_4^* = &\left(\frac{-2m^4}{(m-1)^{12}(m+1)^{12}\left(m^2+1\right)^6}\right) \\ &\left(m^2z+z-1\right)\left(m^2z+z+1\right)\left(m^2z+z-m\right)\left(m^2z+z+m\right) \\ &(-512z^8m^{14} - 2048z^8m^{12} - 3072z^8m^{10} - 2048z^8m^8 - 512z^8m^6 + 16z^6m^{16} \\ &+ 112z^6m^{14} + 1104z^6m^{12} + 2864z^6m^{10} + 2864z^6m^8 + 1104z^6m^6 \\ &+ 112z^6m^4 + 16z^6m^2 - 2z^4m^{16} - 16z^4m^{14} - 88z^4m^{12} - 752z^4m^{10} \\ &- 1356z^4m^8 - 752z^4m^6 - 88z^4m^4 - 16z^4m^2 - 2z^4 + z^2m^{14} - z^2m^{12} \\ &+ 29z^2m^{10} + 227z^2m^8 + 227z^2m^6 + 29z^2m^4 - z^2m^2 + z^2 - 32m^6) \end{aligned} \tag{4.19}$$

So as long as $m \notin \{-1, 0, 1\}$ we have the following four rational points of period 4.

$$\frac{1}{m^2+1} \xmapsto{\phi_m} \frac{-m}{m^2+1} \xmapsto{\phi_m} \frac{-1}{m^2+1} \xmapsto{\phi_m} \frac{m}{m^2+1} \xmapsto{\phi_m} \frac{1}{m^2+1} \xmapsto{\phi_m} \cdots$$

Note that the condition on m (which is necessary so that b and k are both defined and nonzero) insures that all four points in the cycle are distinct.

If $\phi(z) = kz + \frac{b}{z}$ is to have more than four rational points of primitive period 4, there must be rational roots of $\Lambda_4^*(b,k,z) = 0$. Following Morton in [14], we define the *trace* of an n-cycle in $\mathbb{C}$ of $\phi(z) = kz + \frac{b}{z}$ to be the sum of the elements in the cycle. Then we let $\tau_n(z,b,k) \in \mathbb{Q}(b,k)[z]$ be the polynomial whose roots for generic b,k are the traces of all the n-cycles where the trace is nonzero. Only modest modifications to Morton's method of computing the polynomials τ_n are necessary for the case of rational functions.

Rational solutions to $\Lambda_4^*(b,k,z) = 0$ necessarily yield rational solutions to $\tau_4(b,k,z) = 0$. The hope is to find only finitely many solutions to the second equation, and then find the corresponding solutions to the first one. In this case, however, $\tau_4(b,k,z) = 0$ has infinitely many rational solutions, meaning that there are infinitely many rational b and k values such that $\phi_{k,b}$ has three Galois-stable 4-cycles. (See Remark 4.2 following this proof.)

Instead, for fixed b and k, let α be a root of $\Lambda_4^*(z,b,k)$. Then the other roots are necessarily $\phi(\alpha)$, $\phi^2(\alpha)$, $\phi^3(\alpha)$, $-\alpha$, $-\phi(\alpha)$, $-\phi^2(\alpha)$, and $-\phi^3(\alpha)$. Let $t_1 = \alpha + \phi^2(\alpha)$, $t_2 = \phi(\alpha) + \phi^3(\alpha)$, $t_3 = -\alpha - \phi^2(\alpha)$, and $t_4 = -\phi(\alpha) - \phi^3(\alpha)$.

We let $\tau_{4,2}(z,b,k) \in \mathbb{Q}(b,k)[z]$ be the polynomial whose roots for generic b,k are the t_i for $i = 1,\ldots,4$. We see that $\tau_{4,2}(z,b,k)$ must have degre 4 in z, and it is easy to check that the coefficients of the linear and cubic terms both vanish. Let $\tau_{4,2}(z,b,k) = z^4 + Uz^2 + V$ and solve for U and V so that this polynomial vanishes identically modulo $\Lambda_4^*(z,b,k)$. We find that

$$\tau_{4,2}(z,b,k) = z^4 + \frac{4bk^4 + 4bk^2 + b}{k^5}z^2 + \frac{4b^2k^4 + 4b^2k^2 + b^2}{k^8}.$$

Since $\tau_{4,2}$ is even in z, we may substitute $x = z^2$ and consider instead roots of

$$x^2 + \frac{4bk^4 + 4bk^2 + b}{k^5}x + \frac{4b^2k^4 + 4b^2k^2 + b^2}{k^8} = 0.$$

A change of variables $x \to bx$ and dividing by b^2 removes dependence on b:

$$x^2 + \frac{4k^4 + 4k^2 + 1}{k^5}x + \frac{4k^4 + 4k^2 + 1}{k^8} = 0. \tag{4.20}$$

This curve is already quadratic in x, and the discriminant is

$$d^2 = \frac{(2k^2 - 2k + 1)(2k^2 + 2k + 1)(1 + 2k^2)^2}{k^{10}}.$$

So we may search for rational points on the elliptic curve

$$y^2 = (2k^2 - 2k + 1)(2k^2 + 2k + 1). \tag{4.21}$$

Letting $k \to 2k/y$ and $y \to -1 + 2k^3/y^2$ and multiplying both sides by y^4/k^3 puts the curve in Weierstrass form

$$y^2 = k^3 - 16k,$$

which has the minimal model

$$y^2 = k^3 - k.$$

This is curve 32a2 in Cremona's tables [4]. It has rank 0 and torsion subgroup of order 4. The curve in equation (4.21) must then have exactly four rational points. It has a double-point at infinity (since it has the form $y^2 =$ quartic), and the obvious points $(k, y) = (0, \pm 1)$. That must be all of the rational points, so the only possible finite k-value is 0, which does not yield a valid rational map of degree 2. □

Example. Let $m = 2$. Computing k and b from equation (4.18), we have the rational map $\phi_2(z) = \frac{4z}{3} - \frac{2}{15z}$ with the four-cycle

$$\frac{1}{5} \xmapsto{\phi_2} \frac{-2}{5} \xmapsto{\phi_2} \frac{-1}{5} \xmapsto{\phi_2} \frac{2}{5} \xmapsto{\phi_2} \frac{1}{5} \xmapsto{\phi_2} \cdots$$

Remark. Let $\phi_{m_1} = k_1 z + \frac{b_1}{z}$ and $\phi_{m_2} = k_2 z + \frac{b_2}{z}$ with k_1, k_2, b_1, and b_2 as given in equation (4.18). By lemma 17, these rational maps are linearly conjugate over $\mathbb{Q}$ if and only if $k_1 = k_2$ and $\frac{b_1}{b_2} \in (\mathbb{Q}^*)^2$. We can solve

$$\begin{aligned} k_1 &= k_2 \\ \frac{2m_1}{m_1^2 - 1} &= \frac{2m_2}{m_2^2 - 1} \\ (m_2 - m_1)(m_1 m_2 + 1) &= 0 \\ m_1 = m_2 \text{ or } m_1 &= -\frac{1}{m_2} \end{aligned}$$

If $m_1 \neq m_2$, then $k_1 = k_2$ if and only if $m_1 = -\frac{1}{m_2}$. We can now compute the relevant b_1 and b_2 in this case.

$$\begin{aligned} b_1 &= -\frac{m_1}{m_1^4 - 1} \\ b_2 &= -\frac{m_2}{m_2^4 - 1} = -\frac{(-1/m_1)}{(-1/m_1)^4 - 1} = -\frac{m_1^3}{m_1^4 - 1} = m_1^2 b_1 \end{aligned}$$

We see, therefore, that ϕ_{m_1} is linearly conjugate to ϕ_{m_2} if and only if $m_1 = m_2$ or $m_1 = -\frac{1}{m_2}$.

Remark. If we consider the curve $C : \Lambda_4^*(b, k, z) = 0$ where the parameter b merely represents quadratic twits of the curve, then C has an automorphism $(b, k, z) \mapsto (b, k, \phi(z))$. The curve $\tau_4(b, k, z) - 0$, represents $C/$, the quotient of C by this automorphism. The curve C also has an automorphism $(b, k, z) \mapsto (b, k, \phi^2(z))$, and the quotient of C by this second automorphism is given by $\tau_{4,2}(b, k, z) = 0$.

Examining $\tau_4(b, k, z)$, we can show that for any k value, we may choose a b so that $\phi_{k,b}$ has three Galois-stable four cycles, but no rational points of primitive period 4.

If α is a root of Ψ_4^*, then so is $-\alpha$, and that Ψ_4^* represents a single four-cycle with trace 0. (Clearly, this gives a Galois-stable four cycle.) To compute τ_4, then, we want the traces of the

cycles given by $\Lambda_4^*(b,k,z)$, so we expect τ_4 to be quadratic. Further, we can see that the sum of the two traces will vanish: if α is on one 4-cycle, then $-\alpha$ is on the other. Therefore the irreducible polynomial for the traces will be of the form $\tau_4(z,b,k) = z^2 + V$ for some $V \in \mathbb{Q}(b,k)$, and it is an easy matter (with Mathematica) to compute

$$\tau_4(z,b,k) = z^2 + \frac{b\left(4k^4+4k^3+4k^2+2k+1\right)}{k^5}.$$

Since τ_4 is even in z, we may let $x = z^2$ and consider instead the polynomial

$$x + \frac{b\left(4k^4+4k^3+4k^2+2k+1\right)}{k^5} = 0.$$

A change of variables $x \to bx/k^5$ and then multiplying by k^5/b, and we have

$$x + \left(4k^4+4k^3+4k^2+2k+1\right) = 0.$$

Any rational k yields a rational x. We may then choose b so that k^5x/b is a square. In fact, it is enough to let $b = -\left(4k^4+4k^3+4k^2+2k+1\right)$. (It is an easy matter to check that this relationship between k and b is different from the one in equation (4.18), so that if $\phi_{k,b}$ has three Galois-stable four-cycles, it does not have any rational points of primitive period 4.)

Using this substitution, we may recompute the 4th dynatomic polynomial.

$$\begin{aligned}
\Phi_4^*(k,z) = k^4(&16k^{10}+32k^9+48k^8+48k^7+40k^6+24k^5+12k^4+4k^3+k^2\\
&-8z^2k^6-8z^2k^5-16z^2k^4-12z^2k^3-10z^2k^2-4z^2k-2z^2+z^4k^2+z^4)\\
(&16k^{11}+32k^{10}+48k^9+48k^8+40k^7+24k^6+12k^5+4k^4+k^3\\
&+16zk^9+16zk^8+16zk^7-8zk^5-16zk^4-12zk^3-8zk^2-3zk-z\\
&-8z^2k^6-12z^2k^3-8z^2k^2-12z^2k^5-16z^2k^4-3z^2k-z^2\\
&-4z^3k^5-4z^3k^4-4z^3k^3-2z^3k^2-z^3k-z^4k^3)\\
(&16k^{11}+32k^{10}-+48k^9+48k^8+40k^7+24k^6+12k^5+4k^4+k^3\\
&16zk^9-16zk^8-16zk^7+8zk^5+16zk^4+12zk^3+8zk^2+3zk+z\\
&-8z^2k^6-12z^2k^5-16z^2k^4-12z^2k^3-8z^2k^2-3z^2k-z^2\\
&+4z^3k^5+4z^3k^4+4z^3k^3+2z^3k^2+z^3k-z^4k^3).
\end{aligned}$$

We conclude by presenting evidence that for $n = 5$ and $n = 6$, there are no rational periodic points for $\phi(z) = kz + \frac{b}{z}$ of primitive period n. It seems reasonable that there are no rational periodic points of period $n > 4$, but certainly a different approach would be necessary to prove this result.

Proposition 13. *Let $\phi(z) = kz + \frac{b}{z}$ with $k \in \mathbb{Q} \smallsetminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then there are at most finitely many ϕ with a rational point of primitive period 5. In fact, there are only finitely many such maps with a Galois-stable five cycle.*

Proof. Again, irreducibility of the curve $\Phi_5^*(b,k,z) = 0$ is unaffected by the parameter b. By Theorem 10, we know that $\Phi_5^*(1-k,k,z) = 0$ is irreducible over $\overline{\mathbb{Q}}$. It is a seemingly unweildy polynomial

of degree 30 in each k and z, but using techniques like those in the previous lemmas, we can consider the trace of an orbit of a given five-cycle, and calculate the polynomial $\tau_5(b,k,z)$. Since $-\alpha$ is a root of Φ_5^* whenever α is, and since α and $-\alpha$ are necessarily on different orbits, we see that $\tau_5(b,k,z) \in \mathbb{Q}(b,k)[z]$ will be a degree-6 polynomial that is even in z.

Mathematica allows us to calculate the coefficients as before, and we find that

$$\begin{aligned}\tau_5(b,k,z) = z^6 &+ \frac{b\left(11k^6+11k^5+11k^4+7k^3+5k^2+2k+1\right)}{k^7}z^4 \\ &+ \frac{b^2\left(19k^8+38k^7+57k^6+60k^5+55k^4+38k^3+24k^2+9k+3\right)}{k^{10}}z^2 \\ &+ \frac{b^3\left(3k^3+3k^2+3k+1\right)^2\left(k^4+k^3+k^2+k+1\right)}{k^{13}}.\end{aligned}$$

We may substitute $x = z^2$ to get

$$\begin{aligned}\tau_5(b,k,x) = x^3 &+ \frac{b\left(11k^6+11k^5+11k^4+7k^3+5k^2+2k+1\right)}{k^7}x^2 \\ &+ \frac{b^2\left(19k^8+38k^7+57k^6+60k^5+55k^4+38k^3+24k^2+9k+3\right)}{k^{10}}x \\ &+ \frac{b^3\left(3k^3+3k^2+3k+1\right)^2\left(k^4+k^3+k^2+k+1\right)}{k^{13}}.\end{aligned}$$

Substituting $x \to \frac{b}{k^3}x$ and multiplying by k^{13}/b^3 removes the dependence on b and leaves a polynomial. So we seek rational solutions to

$$\begin{aligned}0 = k^4x^3 &+ \left(11k^6+11k^5+11k^4+7k^3+5k^2+2k+1\right)x^2 \\ &+ \left(19k^8+38k^7+57k^6+60k^5+55k^4+38k^3+24k^2+9k+3\right)x \\ &+ \left(3k^3+3k^2+3k+1\right)^2\left(k^4+k^3+k^2+k+1\right).\end{aligned} \tag{4.22}$$

The curve described in equation (4.22) has genus 4 and is not hyperelliptic. Certainly any rational triple (b,k,z) such that $\Phi_5^*(b,k,z) = 0$ would yield a rational point on this curve. Furthermore, any rational point on this curve with $k \neq 0$ corresponds to a Galois-stable five cycle for $\phi(z)$. By Falting's Theorem [6], there can be only finitely many such points. □

Remark. It seems likely that there are not any finite rational points on the curve in equation (4.22) other than the point $(k,x) = (-1/2, -11/4)$. The author has tested rational points with height $\leq 1,000$ and found no other rational solutions. However, the author can find no map to curves of lower genus nor any other method for proving there are no such points.

Recall that $k = -1/2$ gives a map with additional automorphisms. For this k-value we can trace back the substitutions and find that this corresponds to the map

$$\phi(z) = -\frac{z}{2} + \frac{22}{z}.$$

This map has two Galois-stable five cycles, but no rational points of period 5.

One might ask if for every n (or even just for infinitely many n) there is always a map in $\text{Twist}\left(\phi_{-1/2,1}/\mathbb{Q}\right)$ with a Galois-stable n-cycle.

Proposition 14. *Let $\phi(z) = kz + \frac{b}{z}$ with $k \in \mathbb{Q} \smallsetminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

(a) There are no such maps ϕ such that ϕ has exactly six rational points of primitive period 6.

(b) There are at most finitely many ϕ with more than six rational points of primitive period 6.

Proof. Again, from results in Chapter **??** we know that the sixth dynatomic polynomial for this family factors as

$$\Phi_6^*(b, k, z) = \Psi_6^*(b, k, z)\Lambda_6^*(b, k, z).$$

Further, it is shown that there is a natural isomorphism (over $\mathbb{Q}$) between the curves $\Phi_3^*(b, k, z) = 0$ and $\Psi_6^*(b, k, z) = 0$. The fact that there are no rational points on $\Psi_6^*(b, k, z) = 0$ follows from Theorem 8, which proves part (a). since if $\Lambda_6^*(b, k, z)$ had a rational z-root, it would necessarily have 12 of them because the autmorphism interchanges the cycles of α and $-\alpha$.

The rest of the proof follows exactly as in the case of Proposition 13. If we let $\tau_6(b, k, z)$ be the polynomial with roots t_i such that t_i is the trace of a six-cycle corresponding to some root α of $\Lambda_6^*(b, k, z) = 0$, then $\tau_6(b, k, z)$ is an even polynomial in z of degree 8. Letting $x = z^2$, we can change variables to remove the dependence on b and get a polynomial $\tau_5(k, x)$ in k and x. The curve $\tau_5(k, x) = 0$ has genus 7, so we may again invoke Falting's theorem to conclude that there are at most finitely many points on the curve. The rest follows as before. □

Remark. We note for interest that $\tau_6(k, x)$ defined about does indeed have at least one finite rational point, namely $(k, x) = (-1/2, 6)$. The corresponding b value must then be 6 since as before we have $xb = z^2$ and b is defined only modulo squares. The map $\phi(z) = -\frac{1}{2}z + \frac{6}{z}$ had the expected Galois-stable 6-cycle in $\Psi_6^*(b, k, z)$, but it has two others as well; there are two degree-6 factors of $\Lambda_6^*(b, k, z)$, though there are no rational 6-cycles.

4.3 Rational preperiodic points

We now wish to classify not just rational periodic points, but also rational preperiodic points. Therefore, we follow Poonen in [18] for the notation describing preperiodic points.

Definition 9. *Let m and n be positive integers. Given a rational map ϕ, we say that P is a* preperiodic point of type m_n *if P enters an m cycle after n iterations. That is, $\phi^{n+m}(P) = \phi^n(P)$.*

Example. As shown in Poonen's article, $z = 3/4$ is a point of type 3_2 for the polynomial $\phi(z) = z^2 - 29/16$ since we have

$$3/4 \overset{\phi}{\mapsto} -5/4 \overset{\phi}{\mapsto} -1/4 \overset{\phi}{\mapsto} -7/4 \overset{\phi}{\mapsto} 5/4 \overset{\phi}{\mapsto} -1/4 \overset{\phi}{\mapsto} -7/4 \cdots$$

The following small lemma will be helpful throughout the section.

Lemma 18. *Let K be a field. Let $\phi(z) = kz + \frac{b}{z} \in K(z)$, with $bk \neq 0$, and let $\alpha_1, \alpha_2 \in \overline{K}^*$. Then $\phi(\alpha_1) = \phi(\alpha_2)$ if and only if $\alpha_1 = \alpha_2$ or $\alpha_1 = \frac{b}{k\alpha_2}$.*

Proof. This is a simple algebra exercise:

$$\begin{aligned} k\alpha_1 + \frac{b}{\alpha_1} &= k\alpha_2 + \frac{b}{\alpha_2} \\ k\alpha_1^2\alpha_2 + b\alpha_2 &= k\alpha_1\alpha_2^2 + b\alpha_1 \\ (k\alpha_1\alpha_2 - b)(\alpha_1 - \alpha_2) &= 0, \end{aligned}$$

and the result follows. □

We begin by describing rational preperiodic points of type m_1.

Proposition 15. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q} \smallsetminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then*

(a) For all k and b, $z = 0$ is a point of type 1_1 for $\phi(z)$.

(b) There are as many rational points of type m_1 as there are rational points of primitive period m, unless $m = 1$ and $k = 1/2$.

(c) If $k = b = 1/2$, then $\phi(z)$ has three rational fixed points, but $z = 0$ is the only point of type 1_1.

Proof. For part (a), we begin with the homogeneous form for ϕ. We see that $\phi(0, 1) = [b : 0] = [1 : 0]$, which is a fixed point from Proposition 11. So $z = 0$ is always a point of type 1_1.

For part (b), if w is a rational point of period m, then some rational point α_1 satisfies $\phi(\alpha_1) = w$ (namely the preimage of w on the m-cycle). We know from Lemma 18, then, that $\alpha_2 = \frac{b}{k\alpha_1}$ is also a rational preimage of w. Unless $\alpha_1 = \alpha_2$, it cannot be on the m-cycle, so it is a rational point of type m_1. Since a point can have only two preimages under ϕ, this exhausts all points of type m_1.

If $\alpha_1 = \alpha_2$, then $\alpha_1^2 = b/k$, so modulo squares we may take $b = k$, and our map $\phi(z) = k\left(z + \frac{1}{z}\right)$. Also, we see that α_1 is a double-root of the polynomial $\phi(z) - \phi(\alpha_1)$, which says α_1 is a critical point of $\phi(z)$. Given our form for $\phi(z)$, we have $\alpha_1 = \pm 1$.

We claim that the only rational k-values for which ± 1 can possibly be periodic are $k = \pm 1/2$. Since $-\phi(z) = \phi(-z)$, it is enough to analyze the case $\alpha_1 = 1$.

If $k > 1$, then one may check that $\lim_{r\to\infty} \phi^r(1)$ diverges to infinity. Likewise, it grows negative without bound for $k < -1$, so the only possible k values to result in a periodic critical point are those $-1 < k < 1$.

Let $k = \frac{m}{n}$ in lowest terms, and suppose $n \neq 2$. Consider any prime $p|n$. If $p \neq 2$, then

$$\operatorname{ord}_p(\phi(1)) = \operatorname{ord}_p\left(\frac{2m}{n}\right) < 0,$$

and furthermore, if $\operatorname{ord}_p\left(\frac{s}{t}\right) < 0$ for some $\frac{s}{t} \in \mathbb{Q}$ in lowest terms, then

$$\operatorname{ord}_p\left(\phi\left(\frac{s}{t}\right)\right) = \operatorname{ord}_p\left(\frac{m(s^2+t^2)}{nst}\right) < \operatorname{ord}_p\left(\frac{s}{t}\right).$$

So then $\phi^r(1)$ diverges to infinity p-adically, and α_1 cannot be periodic. Finally, we just need to consider the case $k = \frac{m}{n}$, $n = 2^e$ for some $e > 1$. Then we have

$$\mathrm{ord}_2(\phi(1)) = \mathrm{ord}_2\left(\frac{m}{2^{e-1}}\right) < 0,$$

and the rest of the argument follows as above. So in this case, $\phi^r(1)$ diverges to infinity 2-adically, and $\alpha_1 = 1$ cannot be periodic.

Hence, the only possible k-values to yield a periodic (or preperiodic) critical point are $k = \pm 1/2$. Recall that we do not consider the case $k = -1/2$ because the corresponding rational maps ϕ have automorphism group $\mathcal{S}_3$, so we need only consider the case that $k = 1/2$. It is easy to check that for $k = 1/2$, the points ± 1 are fixed points for $\phi(z)$. So, in this case, there are no points of type 1_1 other than $z = 0$. Every other rational point of period m has a corresponding point of type m_1. This completes the proof of part (c) as well. □

We now move on to rational preperiodic points of type m_2.

Proposition 16. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q} \setminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then*

(a) $\phi(z)$ has no rational points of type 1_2 unless $k = -b$. In this case there are two preimages of 0, and there are never any other points of type 1_2.

(b) $\phi(z)$ has both points of type 1_2 and finite fixed points if and only if $k = \frac{1}{1-x^2}$ and $b = \frac{-1}{1-x^2}$ for some $x \in \mathbb{Q}^*$.

(c) $\phi(z)$ has no rational points of type 2_2.

(d) $\phi(z)$ has no rational points of type 4_2.

Proof. For part (a), consider possible preimages of $z = 0$.

$$\begin{aligned} \phi(\alpha) = k\alpha + \frac{b}{\alpha} &= 0 \\ k\alpha^2 + b &= 0 \\ \alpha^2 &= -\frac{b}{k} \end{aligned}$$

This has a solution in $\mathbb{Q}$ if and only if $-\frac{b}{k} \in (\mathbb{Q}^*)^2$, in which case it has two distinct solutions since $b \neq 0$. Because b is only defined modulo squares, this is equivalent to $k = -b$.

We now consider other points of type 1_2, which map after two iterations to a finite rational fixed point. Because we assume that we have finite rational fixed points, we know that $b = 1 - k$.

Let α be a rational fixed point and x the corresponding point of type 1_1. Without loss of generality, we may take the positive point, so let $\alpha = \sqrt{\frac{b}{1-k}} = 1$ by our normalization. Then $x = \frac{b}{k\alpha} = \frac{1-k}{k}$. We seek a point w such that $\phi(w) = x$.

$$\begin{aligned} kw + \frac{b}{w} &= \frac{b}{k\alpha} \\ kw + \frac{(1-k)}{w} &= \frac{1-k}{k} \\ k^2w^2 - (1-k)w + k(1-k) &= 0 \end{aligned}$$

The final equation is quadratic in w, and it has rational roots if and only if the discriminant $(1-k)^2 - 4k^3(1-k)$ is a square. Because k must be rational, we are left with the task of finding rational points on the elliptic curve

$$y^2 = (x-1)(2x-1)(2x^2+x+1). \tag{4.23}$$

A change of variables $x \to \frac{x}{x-1}$ and $y \to \frac{2y+x+1}{(x-1)^2}$ transforms the curve in equation (4.23) to the reduced form

$$y^2 + xy + y = x^3 - x. \tag{4.24}$$

This is curve 14a4 in Cremona's tables [4]. The curve has rank 0, and torsion group $\mathbb{Z}/6\mathbb{Z}$. It is a simple matter to find the six rational points on this curve:

$$\{\mathcal{O}, (1,0), (0,0), (-1,0), (0,-1), (1,-2)\}.$$

Using the change of coordinates, we may find the six rational points on our original curve:

$$\{(0,1), (0,-1), (1/2,0), (1,0)\}$$

and a double point at infinity.

Since the x-coordinate corresponds to our k value, we see that we may eliminate the point at infinity and the points $(0, \pm 1)$. We need only consider what happens when $k = 1/2$ or $k = 1$.

When $k = 1$, we know from Proposition 11 that $\phi(z)$ has a triple fixed point at infinity and no finite rational fixed points. Since the preimages of $z = 0$ have already been discussed, we are done in this case. Similarly for $k = 1/2$, we have $b = 1 - k = 1/2$. In this case, we have seen above that there are no points of type 1_1 other than $z = 0$, so there can be no points of type 1_2 except for preimages of 0. This concludes part (a).

For part (b), recall that $\phi(z)$ has finite fixed points if and only if $b = 1 - k$, and it has points of type 1_2 if and only if $b = -k$. We need to see when these two conditions give the same value of $b \in \mathbb{Q}/(\mathbb{Q}^*)^2$. Letting $b = -kx^2 = 1 - k$, we have

$$\frac{1}{1-x^2} = k.$$

So we see that we have both rational fixed points and rational points of type 1_2 if and only if there is some $x \in \mathbb{Q}^*$ such that $k = \frac{1}{1-x^2}$. (Note that $x \neq 0$ since $b \neq 0$.) In this case,

$$b = -k = -\frac{1}{1-x^2}.$$

For part (c), we need to look for preimages of points of type 2_1. If we have a rational two-cycle, we know that $b = -(k+1)$. With this normalization, the points of the two cycle are ± 1, and the type 2_1 points satisfy $x = \mp\frac{(1+k)}{k}$. So we seek rational w such that

$$\begin{aligned} kw + \frac{b}{w} &= \frac{-(k+1)}{k} \\ kw - \frac{(k+1)}{w} &= \frac{-(k+1)}{k} \\ k^2w^2 + (1+k)w - k(1+k) &= 0 \end{aligned}$$

A rational root w requires that the discriminant $(k+1)^2 + 4k^3(k+1)$ is a square. Since k must be rational, we are left with the task of finding rational points on the elliptic curve

$$y^2 = (x+1)(2x+1)(2x^2 - x + 1). \tag{4.25}$$

A change of variables $x \to -x$ maps this curve isomorphically onto the one in (4.23), for which we've already found the rational points $\{(0,1),(0,-1),(1/2,0),(1,0)\}$ and a double point at infinity. The rational points on the curve in equation (4.25) must then be

$$\{(0,1),(0,-1),(-1/2,0),(-1,0)\} \text{ and a double point at infinity.}$$

Again, the $x-$coordinate corresponds to our k value. We know that $k = -1/2$ is not an allowable value, and that for $k = -1$ we have no rational two-cycle by Proposition 12.

For part (d), we must assume that $\phi(z)$ has a rational 4-cycle, so from Theorem 9

$$\phi(z) = \frac{2mz}{m^2-1} - \frac{m}{z(m^4-1)}.$$

The four cycle contains the rational points $\{\pm\frac{1}{m^2+1}, \pm\frac{m}{m^2+1}\}$. So we first calculate the relevant type 4_1 points.

$$\begin{aligned} x = \frac{b}{k\alpha} &= \left(-\frac{m}{z(m^4-1)}\right)\left(\frac{m^2-1}{2mz}\right)\left(\pm m^2+1\right) \\ &= \mp\frac{1}{2}. \end{aligned}$$

Similarly,

$$\begin{aligned} x = \frac{b}{k\alpha} &= \left(-\frac{m}{z(m^4-1)}\right)\left(\frac{m^2-1}{2mz}\right)\left(\pm\frac{m^2+1}{m}\right) \\ &= \mp\frac{1}{2m}. \end{aligned}$$

Because of the automorphism of ϕ, without loss of generality we may consider only the positive type 4_1 points. We first will seek preimages of the point $x = 1/2$.

$$\begin{aligned} \phi(w) = \frac{2mw}{m^2-1} - \frac{m}{w(m^4-1)} &= \frac{1}{2} \\ 4m(m^2+1)w^2 - (m^4-1)w - 2m &= 0 \end{aligned}$$

The final equation is quadratic in w, so again rational solutions require that the discriminant $(m^2+1)(m^6 - m^4 + 31m^2 + 1)$ is a square.

In other words, we seek rational points on the genus 3 hyperelliptic curve

$$F : d^2 = (m^2+1)(m^6 - m^4 + 31m^2 + 1). \tag{4.26}$$

Since the equation is even in m, there is a map to an elliptic curve

$$E : d^2 = (x+1)(x^3 - x^2 + 31x + 1),$$

defined by $f : (m, d) \mapsto (m^2, d)$.

The minimal Weierstrass model for E is $y^2+xy = x^3-x^2-x+1$, which is curve 58a in Cremona's table [4]. Unfortunately, this curve has rank 1, so we are unable to use it to find the finitely many rational points on the curve F.

However, there is also a map to a curve of genus 2

$$C : y^2 = x(x+1)(x^3 - x^2 + 31x + 1),$$

defined by $g : (m, w) \mapsto (m^2, mw)$.

To find all of the rational points on F, it is sufficient to find all rational points on the genus 2 curve C, and then to find their preimages under

$$g : F(\mathbb{Q}) \longrightarrow C(\mathbb{Q}).$$

Magma tells us that the rank of $J(\mathbb{Q})$, the Mordell-Weil group of the Jacobian, is 0 and that the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Hence the total number of elements in $J(\mathbb{Q})$ is 16. A short search yields the 16 rational members of the Jacobian:

$$\begin{array}{cc}
\text{identity}, & \{(-1,0),\infty\}, \\
\{(1,8),\infty\}, & \{(1,8),(1,8)\}, \\
\{(1,-8),\infty\}, & \{(0,0),\infty\}, \\
\{(-1,0),(1,8)\}, & \{(-1,0),(0,0)\}, \\
\{(-1,0),(1,-8)\}, & \{(4+\sqrt{17},-116-28\sqrt{17}),(4-\sqrt{17},-116+28\sqrt{17})\}, \\
\{(0,0),(1,8)\}, & \{(4+\sqrt{17},116+28\sqrt{17}),(4-\sqrt{17},116-28\sqrt{17})\}, \\
\{(0,0),(1,-8)\}, & \{(8+\sqrt{65},548+68\sqrt{65}),(8-\sqrt{65},548-68\sqrt{65})\}, \\
\{(1,-8),(1,-8)\}, & \{(8+\sqrt{65},-548-68\sqrt{65}),(8-\sqrt{65},-548+68\sqrt{65})\},
\end{array}$$

where, as usual, $\{P_1, P_2\}$ represents the divisor class containing $P_1 + P_2 - 2\infty$. There can therefore be no other points in $C(\mathbb{Q})$, apart from the five obvious points:

$$\{\infty, (0,0), (-1,0), (1,8), (1,-8)\},$$

since any other members of $C(\mathbb{Q})$ would give rise to additional members of $J(\mathbb{Q})$. Using

$$\begin{aligned} g : F(\mathbb{Q}) &\longrightarrow C(\mathbb{Q}) \\ (m, w) &\longmapsto (m^2, mw) \end{aligned}$$

we see that $(-1, 0)$ can have no preimages. The points $\{(0,0), (1,8), (1,-8), \infty\} \in C(\mathbb{Q})$ have $x \in \{0, 1, \infty\}$, and so any preimages in $F(\mathbb{Q})$ must have $m \in \{0, 1, -1, \infty\}$. We find the points

$$(m, w) \in \{(0,1), (0,-1), (1,8), (1,-8), (-1,8), (-1,-8), \infty^+, \infty^-\}.$$

This must give all of $F(\mathbb{Q})$. We see that necessarily $m \in \{0, \pm 1, \infty\}$, none of which are allowable in the parameterization of $\phi(z)$ given in Theorem 9. So, indeed, there are no points of type 4_2 which are preimages of $\pm 1/2$.

Following the same calculations as above for the point $x = 1/2m$, we get the curve

$$G : d^2 = (m^2 + 1)(m^6 + 31m^4 - m^2 + 1).$$

By a change of coordinates $d \to d/m^4$ and $m \to 1/m$, this is isomorphic to the curve F in equation (4.26). This change preserves the set of possible m values given above, so again we find that no rational points on the curve G correspond to rational points of type 4_2. □

Proposition 17. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q} \setminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then*

(a) $\phi(z)$ has no rational points of type 1_n for $n > 2$.

(b) $\phi(z)$ has no rational points of type 2_n for $n > 1$.

(c) $\phi(z)$ has no rational points of type 4_n for $n > 1$.

Proof. Parts (b) and (c) follow immediately from Proposition 16.

For part (a), it is enough to prove that there are no rational points of type 1_3. From Proposition 16, we need only consider the case $k = -b$. In this case, the only possible rational points of type 1_2 are preimages of 0, so to examine points of type 1_3, we must find the preimages of such points. If α is a point of type 1_2, then $\alpha = \pm 1$. We seek $w \in Q$ such that

$$k\left(w - \frac{1}{w}\right) = 1$$
$$kw^2 - w + k = 0.$$

Rational roots of this quadratic exist if and only if the discriminant $1 + 4k^2$ is a square in $\mathbb{Q}$. This is equivalent to seeking integer solutions to the equation $m^2 + 4n^2 = 1$, which clearly has only $(\pm 1, 0)$ as solutions. Since $k \neq 0$, these solutions do not correspond to any points of type 1_3, and therefore none exist. □

Finally, we consider if and when it's possible for $\phi(z)$ to have rational points of period m and n simultaneously when $m \neq n$.

Proposition 18. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q} \setminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then*

(a) $\phi(z)$ has two finite rational fixed points and *a point of period 2 if and only if for some $m \in \mathbb{Q}$ we have*

$$k = \frac{1 + m^2}{1 - m^2} \qquad \text{and} \qquad b = \frac{2}{m^2 - 1}.$$

(b) $\phi(z)$ has points of type 1_2 and *a rational point of period 2 if and only if for some $x \in \mathbb{Q}$ we have*

$$k = \frac{1}{x^2 - 1} \qquad \text{and} \qquad b = \frac{-1}{x^2 - 1}.$$

(c) $\phi(z)$ has two finite rational fixed points, rational points of type 1_2, and *a rational point of period 2 if and only if for some $t \in \mathbb{Q}$ we have*

$$k = -\frac{\left(t^2 + 2t + 2\right)^2}{4t(t+1)(t+2)} \qquad \text{and} \qquad b = \frac{1}{t(t+1)(t+2)}.$$

Proof. We know from Proposition 11 that $\phi(z)$ has finite rational fixed points if and only if $b = 1-k$, and we know from Proposition 12 that $\phi(z)$ has a rational two-cycle if and only if $b = -(1+k)$. For some $m \in \mathbb{Q}^*$, we want

$$\begin{aligned} 1-k &= -(1+k)m^2 \\ 1+x^2 &= k(1-m^2) \\ k &= \frac{1+m^2}{1-m^2} \end{aligned}$$

Solving $b = 1-k$, we find $b = \frac{2m^2}{m^2-1}$ which is equivalent modulo squares to the expression in part (a).

For part (b), b must satisfy both $b = -k$ and $b = -(1+k)$ modulo squares. This requires some $x \in \mathbb{Q}^*$ such that

$$\begin{aligned} -kx^2 &= -(1+k) \\ k &= \frac{1}{x^2-1}. \end{aligned}$$

The value for b follows immediately from this.

For part (c), we begin with the expressions from part (a). If we also require points of type 1_2, we need $b = -k$. That is, for some $y \in \mathbb{Q}^*$ we want

$$\begin{aligned} -by^2 &= k \\ \frac{-2y^2}{m^2-1} &= \frac{1+m^2}{1-m^2} \\ 2y^2 &= 1+m^2 \end{aligned}$$

This rational curve is parameterized by

$$(m, y) = \left(-\frac{t^2+4t+2}{t^2-2}, -\frac{t^2+2t+2}{t^2-2}\right).$$

Substituting m into the expressions for b and k in part (a) yields the parameterization given in part (c). □

Proposition 19. *Let $\phi(z) = kz + \frac{b}{z}$, with $k \in \mathbb{Q} \setminus \{0, -1/2\}$ and $b \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then*

(a) $\phi(z)$ cannot have both finite rational fixed points and *a rational point of period* 4.

(b) $\phi(z)$ has both rational points of type 1_2 and *a rational point of period* 4 *if and only if for some $t \in \mathbb{Q}^*$, we have*

$$k = -\frac{\left(t^2-2\right)\left(t^2+4t+2\right)}{4t(t+1)(t+2)} \qquad \textit{and} \qquad b = \frac{\left(t^2-2\right)\left(t^2+4t+2\right)}{t(t+1)(t+2)}.$$

(c) $\phi(z)$ cannot have both a rational point of period 2 and *a rational point of period* 4.

Proof. From Proposition 11, $\phi(z)$ has finite rational fixed points if and only if $b = 1 - k$, and from Theorem 9, $\phi(z)$ has a rational point of period 4 if and only if $k = 2m/(m^2-1)$ and $b = -m/(m^4-1)$. We need to show that these cannot both be true, taking b modulo squares. If they were true, we would have some $x \in \mathbb{Q}^*$ such that

$$\begin{aligned} bx^2 &= 1 - k \\ \frac{-mx^2}{m^4-1} &= \frac{2m}{m^2-1} \\ mx^2 + (m^2 - 2m - 1)(m^2 + 1) &= 0 \end{aligned}$$

This has rational solutions in x if and only if the discriminant

$$-4m(m^2 + 1)(m^2 - 2m - 1)$$

is a square. So we seek rational points on the genus 2 curve

$$C : d^2 = -m(m^2 + 1)(m^2 - 2m - 1). \tag{4.27}$$

Magma tells us that the rank of $J(\mathbb{Q})$, the Mordell-Weil group of the Jacobian, is 0 and that the torsion subgroup is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Hence the total number of elements in $J(\mathbb{Q})$ is 20. A short search yields the 20 rational members of the Jacobian:

$$\begin{array}{cccc} \text{identity}, & \{(-1,2),\infty\}, & \{(-1,-2),\infty\}, & \{(0,0),\infty\}, \\ \{(1,2),\infty\}, & \{(1,-2),\infty\}, & \{(-1,2),(-1,2)\}, & \{(-1,-2),(-1,-2)\}, \\ \{(1,2),(1,2)\}, & \{(1,-2),(1,-2)\}, & \{(1,2),(-1,2)\}, & \{(1,-2),(-1,-2)\}, \\ \{(1,2),(-1,-2)\}, & \{(1,-2),(-1,2)\}, & \{(0,0),(-1,2)\}, & \{(0,0),(-1,-2)\}, \\ \{(0,0),(1,-2)\}, & \{(0,0),(1,2)\}, & \{(\sqrt{-1},0),(-\sqrt{-1},0)\}, & \{(1+\sqrt{2},0),(1-\sqrt{2},0)\}, \end{array}$$

There can therefore be no other points in $C(\mathbb{Q})$, apart from the six obvious points:

$$\{\infty, (0,0), (1,2), (-1,2), (1,-2), (-1,-2)\},$$

since any other points of $C(\mathbb{Q})$ would give rise to additional members of $J(\mathbb{Q})$. The only finite m values represented here are $m \in \{0, \pm 1\}$, none of which are allowable in the parameterization in Theorem 9. This proves part (a).

For part (b), we know that $\phi(z)$ has rational points of type 1_2 if and only if $b = -k$. Reasoning as above, we need to find $x \in \mathbb{Q}^*$ such that

$$\begin{aligned} bx^2 &= -k \\ -\frac{mx^2}{m^4-1} &= -\frac{2m}{m^2-1} \\ x^2 &= 2m^2 + 2 \end{aligned}$$

This describes a rational curve which may be parameterized by

$$(x, m) = \left(\frac{2t^2 + 4t + 4}{t^2 - 2}, \frac{-t^2 - 4t - 2}{t^2 - 2} \right).$$

Substituting this m into the expressions for k and b gives the desired parameterization.

Finally, from Proposition 12, $\phi(z)$ has a rational two-cycle if and only if $b = -(1+k)$. Reasoning as above, we would have some $x \in \mathbb{Q}^*$ such that

$$\begin{aligned} bx^2 &= -(1+k) \\ \frac{-mx^2}{m^4-1} &= -\left(1 + \frac{2m}{m^2-1}\right) \\ mx^2 - (m^2+2m-1)(m^2+1) &= 0 \end{aligned}$$

Again, this has rational solutions in x if and only if the discriminant

$$4m(m^2+1)(m^2+2m-1)$$

is a square. So we seek rational points on the genus 2 curve

$$D : d^2 = m(m^2+1)(m^2+2m-1). \tag{4.28}$$

A change of variables $m \to -m$ maps the curve D above isomorphically onto the curve C in (4.27). We see on the list of rational points for C that $(-m, d)$ was a rational point whenever (m, d) was. The rational points on D must therefore be exactly the same set. So again, we have no valid m values. □

Combining the results of Propositions 15–19, we see that the maximal number of rational preperiodic points landing eventually at a fixed point or a two cycle will occur in two different cases:

- when $\phi(z)$ has finite rational fixed points, points of type 1_2, and a rational two cycle as described in Proposition 18(c), or
- when $\phi(z)$ has a rational four cycle and points of type 1_2, as described in Proposition 19(b).

In each case, there are a total of 12 rational preperiodic points, including the fixed point at infinity. And we have proved the following.

Theorem 10. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be morphism of degree 2 defined over $\mathbb{Q}$, and suppose that $\mathrm{Aut}(\phi) \cong \boldsymbol{\mu}_2$. Then*

$$\#\{P \in \mathbb{Q} | P \textit{ is preperiodic and lands on a cycle of length at most four}\} \leq 12.$$

4.4 Examples

In this section, we give a complete list of the possible directed graphs corresponding to rational preperiodic points for $\phi(z) = kz + \frac{b}{z}$, based on the results in Section 4.3. A diagram of each possibility is shown in Figure 4.1.

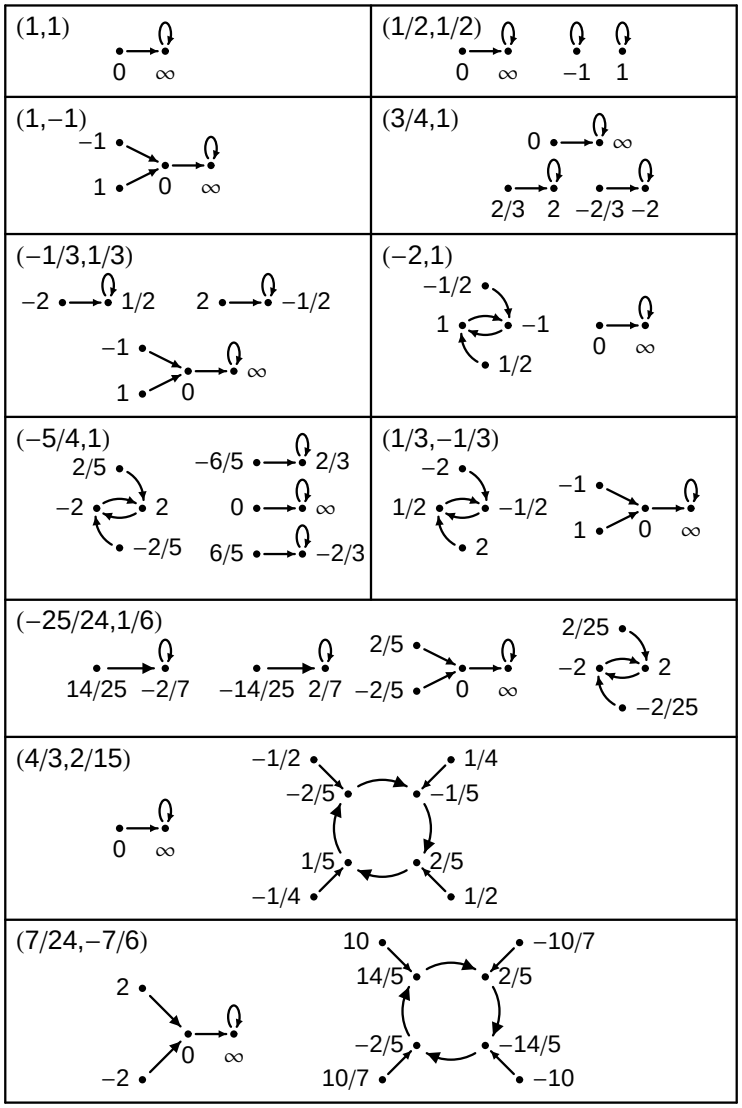

Figure 4.1: All possible directed graphs; (k, b) values are shown for each.

(a) $\phi(z) = z + z^{-1}$
$k = 1$, so there are no fixed points other than the one at infinity. Furthermore $b \neq 2$ and $b \neq -k$, there is no rational 2-cycle and no points of type 1_2.

(b) $\phi(z) = \dfrac{1}{2}\left(z + z^{-1}\right)$
$k = b = 1/2$, so there are finite rational fixed points at ± 1, but no points of type 1_1 other than 0 and no rational points of period 2 or 4.

(c) $\phi(z) = z - z^{-1}$
$k = 1$ and $b = -k$, so we do have points of type 1_2, but in this case there are no finite rational fixed points, and no rational points of period 2 or 4.

(d) $\phi(z) = \dfrac{3}{4}z + \dfrac{1}{z}$
$\frac{b}{1-k}$ is a square and $k \neq 1/2$, so we have two finite rational fixed points and three rational points of type 1_1. There are no rational points of type 1_2 and no rational points of period 2 or 4.

(e) $\phi(z) = -\dfrac{1}{3}z + \dfrac{1}{3z}$
$k = \frac{1}{1-x^2}$ and $b = -\frac{1}{1-x^2}$ (here $x = 2$), so we have two finite rational fixed points, three rational points of type 1_1 and two rational points of type 1_2. There are no rational points of period 2 or 4.

(f) $\phi(z) = -2z + z^{-1}$
$\frac{b}{1-k}$ is not a square but $\frac{-b}{1+k}$ is a square, so we have rational points of period 2 but no finite rational fixed points. Whenever we have rational points of period 2, we have points of type 2_1 and no rational points of period 4.

(g) $\phi(z) = -\dfrac{5}{4}z + \dfrac{1}{z}$
$k = -\frac{1+m^2}{1-m^2}$ and $b = \frac{2}{m^2-1}$ (in this case, we take $m = 3$, so $k = -5/4$ and $m = 1/4 \equiv 1$ modulo squares), so we have finite rational fixed points and rational points of period 2. Since $k \neq 1/2$, there are three points of type 1_1, and since we have rational points of period 2, we have points of type 2_1. We have no points of type 1_2 and no rational points of period 4.

(h) $\phi(z) = \dfrac{1}{3}z - \dfrac{1}{3z}$
$k = \frac{1}{x^2-1}$ and $b = \frac{-1}{x^2-1}$, so we have points of type 1_2 and a rational points of period 2. There are no finite rational fixed points and no points of period 4.

(i) $\phi(z) = -\dfrac{25}{24}z + \dfrac{1}{6z}$
$k = -\frac{\left(t^2+2t+2\right)^2}{t(t+1)(t+2)}$ and $b = \frac{1}{t(t+1)(t+2)}$ (here $t = 1$), so $\phi(z)$ has rational fixed points, points of type 1_2 , and rational points of period 2. Since $k \neq 1/2$, there are three points of type 1_1, and since we have rational points of period 2, we have points of type 2_1 but no rational points of period 4.

(j) $\phi(z) = \dfrac{4}{3}z - \dfrac{2}{15z}$
$k = \frac{2m}{m^2-1}$ and $b = -\frac{m}{m^4-1}$ (we took $t = 2$) , so $\phi(z)$ has rational points of period 4. Since $\phi(z)$

has rational points of period 4, it can have no finite rational fixed points nor any rational points of period 2. In this case, we have no points of type 1_2.

(k) $\phi(z) = \dfrac{7}{24}z - \dfrac{7}{6z}$
$k = -\frac{(t^2-2)(t^2+4t+2)}{4t(t^2+3t+2)}$ and $b = \frac{(t^2-2)(t^2+4t+2)}{t(t+1)(t+2)}$ (we took $t = 1$), so $\phi(z)$ has four rational points of period 4 and two points of type 1_2. Since $\phi(z)$ has rational points of period 4, it can have no finite rational fixed points nor any rational points of period 2.

Bibliography

[1] I. N. Baker. Fixpoints of polynomials and rational functions. *J. London Math. Soc.*, 39:615–622, 1964.

[2] Alan F. Beardon. *Iteration of rational functions*, volume 132 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[3] Thierry Bousch. *Sur Quelques Probl'emes de Dynamique Holomorphe*. PhD thesis, Universite de Paris-Sud, Centre dOrsay, 1992.

[4] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. web interface to the tables available at http://www.ma.utexas.edu/ tornaria/cnt/cremona.html.

[5] Najmuddin Fakhruddin. Questions on self maps of algebraic varieties. *J. Ramanujan Math. Soc.*, 18(2):109–122, 2003.

[6] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[7] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90(3):435–463, 1997.

[8] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[9] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[10] Steven J. Miller and Ramin Takloo-Bighash. *An invitation to modern number theory*. Princeton University Press, Princeton, NJ, 2006. With a foreword by Peter Sarnak.

[11] John Milnor. Geometry and dynamics of quadratic rational maps. *Experiment. Math.*, 2(1):37–83, 1993.

[12] Patrick Morton. Arithmetic properties of periodic points of quadratic maps. *Acta Arith.*, 62(4):343–372, 1992.

[13] Patrick Morton. On certain algebraic curves related to polynomial maps. *Compositio Math.*, 103(3):319–350, 1996.

[14] Patrick Morton. Arithmetic properties of periodic points of quadratic maps. II. *Acta Arith.*, 87(2):89–102, 1998.

[15] Patrick Morton and Joseph H. Silverman. Rational periodic points of rational functions. *Internat. Math. Res. Notices*, (2):97–110, 1994.

[16] Patrick Morton and Joseph H. Silverman. Periodic points, multiplicities, and dynamical units. *J. Reine Angew. Math.*, 461:81–122, 1995.

[17] D. G. Northcott. Periodic points on an algebraic variety. *Ann. of Math. (2)*, 51:167–177, 1950.

[18] Bjorn Poonen. The classification of rational preperiodic points of quadratic polynomials over $\mathbf{Q}$: a refined conjecture. *Math. Z.*, 228(1):11–29, 1998.

[19] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[20] Joseph H. Silverman. The field of definition for dynamical systems on $\mathbf{P}^1$. *Compositio Math.*, 98(3):269–304, 1995.

[21] Joseph H. Silverman. The space of rational maps on $\mathbf{P}^1$. *Duke Math. J.*, 94(1):41–77, 1998.

[22] Joseph H. Silverman. *The arithmetic of dynamical systems*. Graduate Texts in Mathematics. Springer-Verlag, 2007. to appear.