PREFIXED CURVES IN MODULI SPACE

XAVIER BUFF, ADAM L. EPSTEIN, AND SARAH KOCH

Abstract. We study the geometry of certain algebraic curves in the moduli space of cubic polynomials, and in the moduli space of quadratic rational maps. Given $k \geq 0$, ($k \neq 1$ in the case of quadratic rational maps), we show that the set of conjugacy classes of maps with a prefixed critical point of preperiod k, is an algebraic curve that is irreducible (over $\mathbb{C}$). We then study a closely related question concerning the irreducibility (over $\mathbb{Q}$) of the set of conjugacy classes of unicritical polynomials, of degree $D \geq 2$, with a preperiodic critical point. Our proofs are purely arithmetic; they rely on a result providing sufficient conditions under which irreducibility over $\mathbb{C}$ is equivalent to irreducibility over $\mathbb{Q}$, and on a generalized Eisenstein criterion for irreducibility.

Contents

Introduction

A major goal in complex dynamics is to understand *dynamical moduli spaces*; that is, conformal conjugacy classes of holomorphic dynamical systems. One of the great successes in this regard is the study of the moduli space of quadratic polynomials, which is isomorphic to $\mathbb{C}$. This moduli space contains the famous Mandelbrot set, which has been extensively studied over the past 40 years.

Understanding other dynamical moduli spaces to the same extent tends to be more challenging as they are often higher-dimensional. For example, the moduli space of cubic polynomials and the moduli space of quadratic rational maps are both two-dimensional: the moduli space $\mathscr{P}_3$ of cubic polynomials is isomorphic to $\mathbb{C}^2$ modulo the involution $(a,b) \mapsto (-a,-b)$, and the moduli space $\mathscr{M}_2$ of quadratic rational maps is isomorphic to $\mathbb{C}^2$. In this article, we investigate natural algebraic subvarieties in these moduli spaces, namely those that are defined by the condition that one critical point has finite forward orbit.

It has been known since the time of Fatou and Julia that the global dynamics of a rational map $F : \mathbb{CP}^1 \to \mathbb{CP}^1$ is largely governed by the forward orbits of the critical points of F. It is therefore natural to investigate loci in moduli space

The research of the first author was supported in part by the ANR grant Lambda ANR-13-BS01-0002.

The research of the third author was supported in part by the NSF.

that are determined by restrictions on critical orbits, or by *critical orbit relations*. Given $n \geq 1$, and $k \geq 0$, requiring that one critical point maps to a periodic cycle of period n after k steps, is a critical orbit relation defining an algebraic curve in both moduli spaces $\mathscr{P}_3$ and $\mathscr{M}_2$.

These algebraic curves have been extensively studied over the last few decades, garnering substantial attention in the past 10 years. Milnor initiated the study of them in [M1] and [M2] and raised various questions about their geometry; in particular, it is conjectured that these curves are all irreducible over $\mathbb{C}$. In this article, we exhibit the first infinite collection of them, in $\mathscr{P}_3$ and then in $\mathscr{M}_2$, for which the conjecture holds.

We begin with cubic polynomials. Given $n \geq 1$, and $k \geq 0$, the set of affine conjugacy classes of cubic polynomials with a critical point mapping to a cycle of period n, with preperiod k, is an algebraic curve $\mathscr{S}_{k,n} \subset \mathscr{P}_3$.

Conjecture. *For $k \geq 0$ and $n \geq 1$, the curve $\mathscr{S}_{k,n}$ is irreducible over $\mathbb{C}$.*

Our first theorem applies to the curve $\mathscr{S}_{k,1}$, defined by the condition that one critical point is prefixed.

Theorem 1. *For $k \geq 0$, the curve $\mathscr{S}_{k,1}$ is irreducible over $\mathbb{C}$.*

By Epstein's transversality results [E2], the curve $\mathscr{S}_{k,n}$ is smooth, so $\mathscr{S}_{k,n}$ is irreducible over $\mathbb{C}$ if and only if it is connected.

Corollary 2. *For $k \geq 0$, the curve $\mathscr{S}_{k,1}$ is connected.*

Many of the techniques in the literature used to study these curves involve topological or analytic approaches (for example, see [M2], [BKM], and [Re3]). Recently, Arfeux and Kiwi proved established the irreducibility of the curves $\mathscr{S}_{0,n}$ for all $n \geq 1$ [AK]. Our techniques are very different: our proof is purely arithmetic, and we do not know of an alternative proof. Our results are largely inspired by work of Thierry Bousch [Bo], establishing that for $n \geq 1$, the set of $(c, w) \in \mathbb{C}^2$ such that w is periodic of period n for $f_c : z \mapsto z^2 + c$ is irreducible over $\mathbb{C}$. The proof of Theorem 1 will be given in §1.

In §2, we explain how the proof presented for cubic polynomials adapts to the case of quadratic rational maps. Given $k \geq 0$ with $k \neq 1$ and $n \geq 1$, the set of Möbius conjugacy classes of quadratic rational maps with a critical point preperiodic to a cycle of period n, with preperiod k, is an algebraic curve $\mathscr{V}_{k,n} \subset \mathscr{M}_2$. (Note that $\mathscr{V}_{1,n} \subset \mathscr{M}_2$ is empty, which is why we require $k \neq 1$.)

Conjecture. *For $k \in \{0, 2, 3, 4, \ldots\}$ and $n \geq 1$, the curve $\mathscr{V}_{k,n}$ is irreducible over $\mathbb{C}$.*

As with cubic polynomials, our result applies to the curve $\mathscr{V}_{k,1}$, defined by the condition that one critical point is prefixed.

Theorem 3. *For $k \in \{0, 2, 3, 4, \ldots\}$, the curve $\mathscr{V}_{k,1}$ is irreducible over $\mathbb{C}$.*

Again, Epstein's transversality results [E2] imply that the curve $\mathscr{V}_{k,n}$ is smooth, so $\mathscr{V}_{k,n}$ is irreducible over $\mathbb{C}$ if and only if it is connected.

Corollary 4. *For $k \in \{0, 2, 3, 4, \ldots\}$, the curve $\mathscr{V}_{k,1}$ is connected.*

In each of the proofs of Theorem 1 and Theorem 3, we first reduce the problem to proving that some polynomial $R_k \in \mathbb{Z}[a, b]$ is irreducible over $\mathbb{C}$. As in the work of Bousch, we first show that this is equivalent to irreducibility of R_k over $\mathbb{Q}$. We apply the following lemma of independent interest, which implies that an algebraic curve in $\mathbb{C}^2$ that contains a smooth point with rational coordinates is irreducible over $\mathbb{C}$ if and only if it is irreducible over $\mathbb{Q}$. When $n = 1$, we know how to find such a point, and when $n > 1$, we do not: this is the main reason we restrict our study to the prefixed curves. We note that Ramadas was able to push this idea further in her article [Ra], where she studies the curves $\mathscr{V}_{k,1}$ in the moduli space of quadratic rational maps.

Lemma 5 (Irreducibility Lemma)**.** *Let $R \in \mathbb{Q}[a, b]$ be a polynomial vanishing at the origin with nonzero linear part. Then, R is irreducible over $\mathbb{C}$ if and only if R is irreducible over $\mathbb{Q}$.*

By restricting the complex line $a = 0$, we show that R_k is irreducible over $\mathbb{Q}$. The proof relies on the following result due to Vefa Goksel [G]. Assume $D \in \{2, 3\}$. Let $b_1 \in \mathbb{C}$ and $b_2 \in \mathbb{C}$ be two algebraic numbers such that 0 is preperiodic to a fixed point of $z \mapsto z^D + b_1$ and $z \mapsto z^D + b_2$, with the same preperiod $k \geq 2$. Then, b_1 and b_2 are Galois conjugate. A similar result holds in the cases where 0 is preperiodic to a cycle of period 2 or a cycle of period 3 (see Section 3.2).

More generally, if $D \geq 2$ is an integer, the unicritical polynomials $z \mapsto z^D + b_1$ and $z \mapsto z^D + b_2$ are affine conjugate if and only if $b_1^{D-1} = b_2^{D-1}$. John Milnor [M3] asked whether one can classify the Galois conjugacy classes of parameters b^{D-1} such that the critical point of $z \mapsto z^D + b$ is preperiodic. In §3, we characterize those Galois conjugacy classes in special cases. Our result requires the following generalization of the Eisenstein criterion for irreducibility, which requires that we work over $\mathbb{F}_p$.

Lemma 6 (Generalized Eisenstein Criterion)**.** *Assume $A \in \mathbb{Z}[a]$ and $B \in \mathbb{Z}[a]$ are monic polynomials and p is a prime number such that*

- $A \equiv B^N \pmod{p}$ *for some integer $N \geq 1$;*
- *the polynomial $B \pmod{p}$ is irreducible over $\mathbb{F}_p$;*
- $p^{2\deg(B)}$ *does not divide* $\mathrm{resultant}(A, B)$.

Then, A is irreducible over $\mathbb{Q}$.

We require that $D = p^e$ so that $(z + w)^D = z^D + w^D$ holds in $\mathbb{F}_p$. Our study then reduces to the question of irreducibility of a particular polynomial. The only cases for which this polynomial is irreducible over $\mathbb{F}_p$ are those where the period is 1 or 2 for any prime power $D = p^e$, and where the period is 3 for $D = 2$ and $D = 8$.

Notes and references. For background on the dynamics of cubic polynomials, see [BH]. In [M2], [BKM], [Re3], and [DS], the curves $\mathscr{S}_{0,n}$ are studied. For background on the dynamics of quadratic rational maps, see [M1]. See [M1], [Re1], [Re2], [Re3], and [T] where the curves $\mathscr{V}_{0,n}$ have been extensively studied. In addition, we note that because the curves $\mathscr{S}_{k,n} \subset \mathscr{P}_3$ and $\mathscr{V}_{k,n} \subset \mathscr{M}_2$ are defined by critical orbit relations, they are examples of the *special curves* in moduli space studied by Baker and DeMarco in their work on the dynamical André-Oort conjecture; see [BD].

As previously mentioned, our work is largely inspired by the work of Thierry Bousch, who proved that the *dynatomic curves* associated to the quadratic family $z \mapsto z^2 + c$ are irreducible [Bo].

1. Cubic polynomials

Every cubic polynomial is affine conjugate to a polynomial of the form

$$F_{a,b}(z) = z^3 - 3a^2 z + 2a^3 + b, \quad (a,b) \in \mathbb{C}^2.$$

Those polynomials have critical points at $\pm a$ and $b = F_{a,b}(a)$ is a critical value. A conjugacy between two such polynomials either preserves or exchanges the two critical points. Consequently, the moduli space $\mathscr{P}_3$ is obtained by identifying (a,b) with $(-a,-b)$. It follows that in order to prove Theorem 1, it is enough to show that the set $\mathcal{S}_k$ of parameters $(a,b) \in \mathbb{C}^2$ such that a is preperiodic to a fixed point with preperiod $k \geq 0$ is irreducible.

Note that for $k = 0$, the critical point a is fixed if and only if (a,b) belongs to the line $\mathcal{L}_0 := \{b = a\} \subset \mathbb{C}^2$. Thus, $\mathcal{S}_0 = \mathcal{L}_0$ is irreducible.

Note that for $k = 1$, the critical value $b = F_{a,b}(a)$ is fixed if and only if

$$b = F_{a,b}(b) = b^3 - 3a^2 b + 2a^3 = b + (a-b)^2(2a+b).$$

Consequently, $\mathcal{S}_1 = \mathcal{L}_1 \smallsetminus \mathcal{L}_0 = \mathcal{L}_1 \smallsetminus \big\{(0,0)\big\}$, with $\mathcal{L}_1 := \{b = -2a\} \subset \mathbb{C}^2$. Thus, $\mathcal{S}_1$ is irreducible.

For the remainder of §1, we assume that $k \geq 2$.

1.1. **An equation for $\mathcal{S}_k$.** On the one hand, if a is preperiodic to a fixed point of $F_{a,b}$ with preperiod k, then the points $F_{a,b}^{\circ(k-1)}(a)$ and $F_{a,b}^{\circ k}(a)$ are distinct and have the same image under $F_{a,b}$. For $j \geq 0$, let $P_j \in \mathbb{Z}[a,b]$ be the polynomial defined by

$$P_j(a,b) := F_{a,b}^{\circ j}(a).$$

Then,

$$P_0(a,b) = a, \quad P_1(a,b) = b, \quad \text{and} \quad P_{j+1} = P_j^3 - 3a^2 P_j + 2a^3 + b,$$

so that for $j \geq 1$, the polynomial P_j has degree 3^{j-1}. Note that

$$F_{a,b}(z) - F_{a,b}(w) = (z-w)H(z,w) \quad \text{with} \quad H(z,w) = z^2 + zw + w^2 - 3a^2.$$

Thus, the polynomial

$$Q_k := H(P_{k-1}, P_k) \in \mathbb{Z}[a,b]$$

has degree $2 \cdot 3^{k-1}$ and vanishes on $\mathcal{S}_k$.

On the other hand,

$$H(z,z) = 0 \quad \text{if and only if} \quad z^2 = a^2, \text{ i.e. } z = \pm a. \tag{1}$$

In particular, if $a = F_{a,b}(a)$, i.e. if $a = b$, then $P_{k-1}(a,b) = P_k(a,b) = a$ and $Q_k(a,b) = 0$. Thus, $b - a$ divides Q_k and so,

$$Q_k = (b-a)R_k \quad \text{with} \quad R_k \in \mathbb{Z}[a,b].$$

The polynomial R_k has degree $2 \cdot 3^{k-1} - 1$ and vanishes on $\mathcal{S}_k$. Set

$$\Sigma_k := \big\{(a,b) \in \mathbb{C}^2 \ ; \ R_k(a,b) = 0\big\}.$$

Then, $\mathcal{S}_k \subset \Sigma_k$. Every point in Σ_k satisfies $F_{a,b}^{\circ k}(a) = F_{a,b}^{\circ(k+1)}(a)$. However, we may have $F_{a,b}^{\circ(k-1)}(a) = F_{a,b}^{\circ k}(a)$. Thus, there are points in $\Sigma_k \smallsetminus \mathcal{S}_k$. According to Equation (1), either:

(i) $F_{a,b}^{\circ(k-1)}(a) = F_{a,b}^{\circ k}(a) = a$ in which case a is fixed; or

(ii) $F_{a,b}^{\circ(k-1)}(a) = F_{a,b}^{\circ k}(a) = -a$ in which case $-a$ is fixed and a is prefixed to $-a$ with preperiod j for some $j \in [\![2, k-1]\!]$.

Note that case (i) occurs if and only if $a = b = 0$, i.e., $\Sigma_k \cap \mathcal{S}_1 = \big\{(0,0)\big\}$. Indeed, for $j \geq 1$,

$$\frac{\partial P_{j+1}}{\partial b} = 3(P_j^2 - a^2)\frac{\partial P_j}{\partial b} + 1.$$

Since $P_j(a,a) = a$, it follows by induction that

$$\frac{\partial P_j}{\partial b}(a,a) = 1.$$

Since

$$\frac{\partial Q_k}{\partial b} = (2P_{k-1} + P_k)\frac{\partial P_{k-1}}{\partial b} + (P_{k-1} + 2P_k)\frac{\partial P_k}{\partial b},$$

we deduce that

$$R_k(a,a) = \frac{\partial Q_k}{\partial b}(a,a) = 6a.$$

Thus, on the line $\{a = b\} \subset \mathbb{C}^2$, the polynomial R_k only vanishes at $(0,0)$.

For case (ii), observe that $-a$ is fixed by $F_{a,b}$ if and only if $4a^3 + a + b = 0$, which is a curve of degree 3. Since the degree of R_k is $2 \cdot 3^{k-1} - 1 \neq 3$, once we prove that R_k is irreducible over $\mathbb{C}$, it follows that there are only finitely many points in Σ_k for which case (ii) holds.

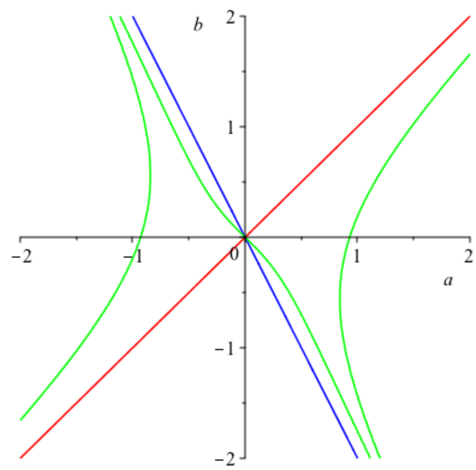

FIGURE 1. Three curves drawn in $\mathbb{R}^2$: $\mathcal{S}_0$, $\mathcal{S}_1$, and $\mathcal{S}_2$.

Thus, Theorem 1 is a corollary of the following result, the proof of which occupies the remainder of §1.

Proposition 7. *For $k \geq 2$, the polynomial $R_k \in \mathbb{Z}[a,b]$ is irreducible over $\mathbb{C}$.*

1.2. **Behavior near the origin.** We will now prove Lemma 5 stated in the Introduction. We recall the statement of the lemma here for convenience. Let $R \in \mathbb{Q}[a,b]$ be a polynomial vanishing at the origin with nonzero linear part. Then, R is irreducible over $\mathbb{C}$ if and only if R is irreducible over $\mathbb{Q}$.

Proof of Lemma 5. Clearly, if R is irreducible over $\mathbb{C}$, then it is irreducible over $\mathbb{Q}$.

Conversely, suppose that R is irreducible over $\mathbb{Q}$. We will show that R is irreducible over $\mathbb{C}$. Suppose that $R = S \cdot T$ where $S \in \mathbb{C}[a,b]$ is irreducible and vanishes at the origin. Such a polynomial S exists because R vanishes at the origin. It then follows that $T \in \mathbb{C}[a,b]$ does not vanish at the origin, since otherwise, the linear part of R at the origin would vanish. Multiplying S by a nonzero constant, we may assume that $T(0,0) = 1$. In that case, the linear parts of R and S at the origin coincide.

Since $R \in \mathbb{Q}[a,b]$, the polynomials S and T have algebraic coefficients. We claim that the coefficients of S are in fact rational. Indeed, assume $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let S^σ be the image of S under the action of σ. Then, S^σ is an irreducible factor of R^σ and $R^\sigma = R$ since $R \in \mathbb{Q}[a,b]$. Note that S and S^σ are equal up to multiplication by a constant since otherwise, $S \cdot S^\sigma$ would divide R, and the linear part of R at the origin would vanish. In addition, the linear part of S^σ is equal to the linear part of $R^\sigma = R$. Thus, $S^\sigma = S$. Since this holds for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the coefficients of S are rational.

Since $S \in \mathbb{Q}[a,b]$ is a factor of R and since R is irreducible over $\mathbb{Q}$, we have that $S = R$. This completes the proof since S is irreducible over $\mathbb{C}$ by assumption. $\square$

Note that every polynomial P of degree D may be uniquely written as

$$P = \sum_{j=0}^{D} P_j$$

where P_j is a homogeneous polynomial of degree j. We say that P_j is the *homogeneous part of degree j* of the polynomial P.

To apply Lemma 5, we need to study the behavior of R_k at the origin.

Lemma 8. *The homogeneous part of least degree of R_k is $3(a+b)$.*

Proof. An elementary induction on $j \geq 1$ shows that the homogeneous part of least degree of P_j is b. As a consequence, the homogeneous part of least degree of Q_k is $3b^2 - 3a^2$. Factoring out $b-a$ to get R_k yields the required result. $\square$

Thus, R_k vanishes at the origin with nonzero linear part $(a,b) \mapsto 3(a+b)$.

Corollary 9. *The polynomial $R_k \in \mathbb{Z}[a,b]$ is irreducible over $\mathbb{C}$ if and only if it is irreducible over $\mathbb{Q}$.*

What really matters in the proof of Lemma 5 is that the curve $\{R = 0\}$ has a single irreducible component containing the origin (indeed, since the derivative of R at the origin is nonzero, the curve is smooth at the origin) and that the origin is fixed by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In fact, we have the following more general result (that we do not use in this article).

Lemma 10. *Let $R \in \mathbb{Q}[a,b]$ be a polynomial. Assume the affine curve $\{R = 0\}$ contains a point $(a_0, b_0) \in \mathbb{Q}^2$ and has a unique locally irreducible (over $\mathbb{C}$) branch at (a_0, b_0). Then R is irreducible over $\mathbb{C}$ if and only if R is irreducible over $\mathbb{Q}$.*

1.3. **The family $z^3 + b$, $b \in \mathbb{C}$.** We now study the intersection of $\mathcal{S}_k$ with the line $\mathcal{L}_2 := \{a = 0\} \subset \mathbb{C}^2$. Note that the map $f_b := F_{0,b}$ is a unicritical polynomial:

$$f_b(z) = z^3 + b.$$

For $j \geq 1$, define $p_j \in \mathbb{Z}[b]$ by

$$p_j(b) := P_j(0,b) \quad \text{so that} \quad p_1 = b \quad \text{and} \quad p_{j+1} = p_j^3 + b.$$

Let $q_k \in \mathbb{Z}[b]$ and $r_k \in \mathbb{Z}[b]$ be defined by

$$q_k(b) := Q_k(0,b) \quad \text{and} \quad r_k(b) := R_k(0,b),$$

so that

$$q_k = p_{k-1}^2 + p_{k-1}p_k + p_k^2 \quad \text{and} \quad q_k = br_k.$$

An easy induction on $j \geq 1$ shows that p_j is a monic polynomial of degree 3^{j-1} with least degree term b. It follows that q_k is a monic polynomial of degree $2 \cdot 3^{k-1}$ with least degree term $3b^2$. Thus, $q_k = br_k = b^2 s_k$ where $s_k \in \mathbb{Z}[b]$ is a monic polynomial of degree $2 \cdot 3^{k-1} - 2$ with $s_k(0) = 3$. The proof of the following result goes back to [G] (see also §3.2).

Proposition 11. *For $k \geq 2$, the polynomial $s_k \in \mathbb{Z}[b]$ is irreducible over $\mathbb{Q}$.*

Proof. Working in $\mathbb{F}_3[b]$, we have that $(x+y)^3 \equiv x^3 + y^3 \pmod 3$. An elementary induction on $j \geq 1$ yields

$$p_j \equiv b^{3^{j-1}} + b^{3^{j-2}} + \cdots + b^3 + b \pmod 3.$$

It follows that

$$p_k - p_{k-1} \equiv b^{3^{k-1}} \pmod 3 \quad \text{and} \quad (p_k - p_{k-1})q_k = (p_k - p_{k-1})^3 \equiv b^{3^k} \pmod 3.$$

Thus,

$$q_k \equiv b^{2 \cdot 3^{k-1}} \pmod 3 \quad \text{and} \quad s_k \equiv b^{2 \cdot 3^{k-1} - 2} \pmod 3.$$

Since $s_k(0) = 3$ is not a multiple of 9, the Eisenstein criterion implies that s_k is irreducible over $\mathbb{Q}$. □

1.4. **Behavior near infinity.** We now study the behavior of R_k when a or b is large.

Lemma 12. *The homogeneous part of greatest degree of R_k is*

$$(b-a)^{4 \cdot 3^{k-2} - 1} \cdot (2a+b)^{2 \cdot 3^{k-2}}.$$

Proof. We first determine the homogeneous part H_k of greatest degree of P_j for $j \geq 2$. Since

$$P_2 = b^3 - 3a^2 b + 2a^3 + b = (b-a)^2(2a+b) + b \quad \text{and} \quad P_{j+1} = P_j^3 - 3a^3 P_j + 2a^3 + b,$$

we have $H_2 = (b-a)^2(2a+b)$ and an elementary induction on $j \geq 2$ yields that $H_j = (H_2)^{3^{j-2}}$. It follows that the homogeneous part of greatest degree of $Q_k = P_{k-1}^2 + P_{k-1}P_k + P_k^2 - 3a^2$ is $(H_2)^{2 \cdot 3^{k-2}} = (b-a)^{4 \cdot 3^{k-2}} \cdot (2a+b)^{2 \cdot 3^{k-2}}$. Factoring out $b-a$ to get R_k yields the required result. □

Let us embed $\mathbb{C}^2$ in $\mathbb{CP}^2$ in the usual way, sending (a,b) to $[a:b:1]$.

Corollary 13. *The closure of Σ_k in $\mathbb{CP}^2$ intersects the line at infinity at only two points: $[1:1:0]$ with multiplicity $4 \cdot 3^{k-2} - 1$, and $[1:-2:0]$ with multiplicity $2 \cdot 3^{k-2}$.*

1.5. **Irreducibility over $\mathbb{Q}$.** We may now complete the proof of Proposition 7.

Proposition 14. *For $k \geq 2$, the polynomial $R_k \in \mathbb{Z}[a,b]$ is irreducible over $\mathbb{Q}$.*

Proof. Assume for a contradiction that $R_k = T_1 \cdot T_2$ with $T_1 \in \mathbb{Z}[a,b]$, $T_2 \in \mathbb{Z}[a,b]$, $\mathrm{degree}(T_1) < \mathrm{degree}(R_k)$, and $\mathrm{degree}(T_2) < \mathrm{degree}(R_k)$.

We first prove that either T_1 or T_2 must have degree 1. Let $t_1 \in \mathbb{Z}[b]$ and $t_2 \in \mathbb{Z}[b]$ be defined by

$$t_1(b) := T_1(0,b) \quad \text{and} \quad t_2(b) := T_2(0,b).$$

Then, $r_k = t_1 \cdot t_2$ with $\mathrm{degree}(t_1) \leq \mathrm{degree}(T_1) < \mathrm{degree}(R_k) = \mathrm{degree}(r_k)$. Similarly, $\mathrm{degree}(t_2) < \mathrm{degree}(r_k)$. Since $r_k = bs_k$ with r_k monic and s_k irreducible over $\mathbb{Q}$, exchanging T_1 and T_2 if necessary, this implies that $t_1 = \pm b$ and $t_2 = \pm s_k$. Then, $\mathrm{degree}(T_2) \geq \mathrm{degree}(s_k) = \mathrm{degree}(R_k) - 1$ and $\mathrm{degree}(T_1) = 1$.

According to Lemma 8, the homogeneous part of least degree of R_k is $3(a+b)$. Thus, T_1 divides $3(a+b)$; in fact, since $t_1 = \pm b$, we have that $T_1 = \pm(a+b)$. So, the closure of Σ_k in $\mathbb{CP}^2$ intersects the line at infinity at the point $[1 : -1 : 0]$. This contradicts Corollary 13. □

2. Quadratic rational maps

To prove Theorem 3, it is convenient to work in a space of dynamically marked quadratic rational maps. A quadratic rational map whose conjugacy class belongs to $\mathscr{V}_{k,1}$ with $k \geq 2$ has a critical point ω whose orbit contains a fixed point α. There is a fixed point $\beta \neq \alpha$ since otherwise, α would be a triple fixed point and its parabolic basin would contain both critical orbits. Note that $\beta \neq \omega$ since ω is not fixed. The conjugacy class may therefore be represented by a rational map f such that

$$\alpha = 0, \quad \beta = \infty \quad \text{and} \quad \omega = 1.$$

The critical value $a = f(1)$ belongs to $\mathbb{C} \setminus \{0\}$ and $f^{-1}(0) = \{0, b\}$ with $b \in \mathbb{C} \setminus \{1\}$. So, the rational map is

$$G_{a,b}(z) := \frac{az(b-z)}{1+(b-2)z} \quad \text{with} \quad (a,b) \in \Lambda := \big(\mathbb{C} \setminus \{0\}\big) \times \big(\mathbb{C} \setminus \{1\}\big).$$

In addition, (a,b) belongs to the curve

$$\mathcal{V}_k := \big\{(a,b) \in \Lambda \ ; \ G_{a,b}^{\circ(k-2)}(a) = b\big\}.$$

Conversely, if (a,b) belongs to the curve $\mathcal{V}_k$, then the conjugacy class of $G_{a,b}$ belongs to $\mathscr{V}_{k,1}$. So, in order to prove Theorem 3, it is enough to prove that the curve $\mathcal{V}_k$ is irreducible.

Remark. A generic conjugacy class in $\mathscr{V}_{k,1}$ has two representatives in $\mathcal{V}_k$ corresponding to the choice of the marked fixed point β. It follows that the quotient map $\mathcal{V}_k \to \mathscr{V}_{k,1}$ has degree 2.

2.1. **An equation for $\mathcal{V}_k$.** Here, we define a polynomial $R_k \in \mathbb{Z}[a,b]$ vanishing on $\mathcal{V}_k$. This polynomial should not be confused with the polynomial R_k defined in §1. However, since they play parallel roles, we keep the same notation. Let us first observe that for $j \geq 2$,

$$G_{a,b}^{\circ(j-2)}(a) = \frac{P_j(a,b)}{Q_j(a,b)}$$

where $P_j \in \mathbb{Z}[a,b]$ and $Q_j \in \mathbb{Z}[a,b]$ are defined recursively by

$$P_2 = a, \quad Q_2 = 1, \quad P_{j+1} = aP_j \cdot (bQ_j - P_j) \quad \text{and} \quad Q_{j+1} = Q_j^2 + (b-2)P_jQ_j.$$

So, $\mathcal{V}_k$ is the set of parameters $(a,b) \in \Lambda$ such that

$$R_k(a,b) = 0 \quad \text{with} \quad R_k := P_k - bQ_k \in \mathbb{Z}[a,b].$$

This shows that $\mathcal{V}_k$ is an algebraic subset of Λ and that Theorem 3 follows from the following result.

Proposition 15. *For $k \geq 2$, the polynomial $R_k \in \mathbb{Z}[a,b]$ is irreducible over $\mathbb{C}$.*

Note that $R_2 = a - b$ is irreducible over $\mathbb{C}$. For the remainder of §2, devoted to the proof of Proposition 15, we assume that $k \geq 3$.

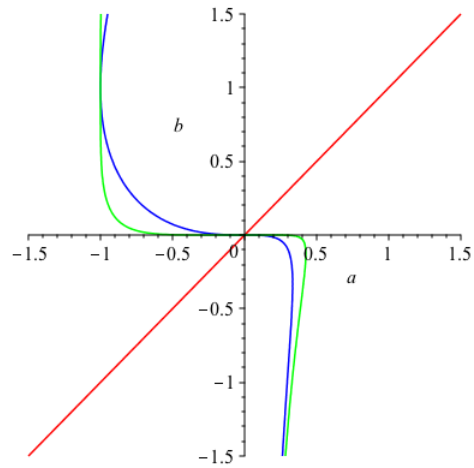

FIGURE 2. Three curves drawn in $\mathbb{R}^2$: $\mathcal{V}_2$, $\mathcal{V}_3$, and $\mathcal{V}_4$.

2.2. **Behavior near the origin.** As in §1.2, we first prove that it is enough to show that R_k is irreducible over $\mathbb{Q}$. And here also, we deduce this from Lemma 5, studying the behavior of R_k near the origin. There is however a fundamental difference between the two approaches, even if this does not appear in the proof. In the case of cubic polynomials, the origin corresponds to the cubic polynomial $z \mapsto z^3$ which belongs to the family we are studying, whereas here, the origin does not belong to our parameter space Λ.

Lemma 16. *For $k \geq 3$, the homogeneous part of least degree of R_k is $-b$.*

Proof. An elementary induction shows that for $j \geq 2$, the homogeneous part of least degree of P_j is $a^{j-1}b^{j-2}$ and the homogeneous part of least degree of Q_j is 1. The result follows immediately. □

As a consequence $R_k \in \mathbb{Z}[a,b]$ vanishes at the origin with nonzero linear part. According to Lemma 5, the polynomial R_k is irreducible over $\mathbb{C}$ if and only if it is irreducible over $\mathbb{Q}$.

2.3. **The family $az(2-z)$, $a\in\mathbb{C}$.** We now study the intersection of $\mathcal{V}_k$ with the line $\mathcal{L} := \{b=2\}\subset\mathbb{C}^2$. Note that the map $g_a := G_{a,2}$ is a quadratic polynomial:

$$g_a(z) = az(2-z).$$

For $j\geq 2$, define $p_j\in\mathbb{Z}[a]$ and $q_j\in\mathbb{Z}[a]$ by

$$p_j(a) := P_j(a,2),\quad q_j(a) := Q_j(a,2)$$

so that

$$p_2 = a,\quad p_{j+1} = -ap_j^2+2ap_j,\quad q_1 = 1\quad\text{and}\quad q_{j+1} = q_j^2.$$

In particular, for $j\geq 3$, the polynomial $-p_j$ is monic with degree $2^{j-1}-1$, and its constant coefficient is 0; and $q_j = 1$. Let $r_k\in\mathbb{Z}[a]$ be defined by

$$r_k(a) := R_k(a,2)\quad\text{so that}\quad r_k = p_k-2.$$

Then, r_k has degree $2^{k-1}-1$ and its constant coefficient is -2.

Lemma 17. *The degree of R_k is $2^{k-1}-1$.*

Proof. An elementary induction shows that the degree of P_k is at most $2^{k-1}-1$ and the degree of Q_k is at most $2^{k-1}-2$. Consequently, the degree of R_k is at most $2^{k-1}-1$.

Since the polynomial p_k has degree $2^{k-1}-1$, the polynomial $r_k = p_k-2$ also has degree $2^{k-1}-1$. Thus,

$$2^{k-1}-1 = \text{degree}(r_k)\leq\text{degree}(R_k)\leq 2^{k-1}-1$$

and the result follows. $\square$

The proof of the following result goes back to [G] (see also §3.2).

Proposition 18. *For all $k\geq 2$, the polynomial $r_k\in\mathbb{Z}[a]$ is irreducible over $\mathbb{Q}$.*

Proof. Working in $\mathbb{F}_2[a]$, we have that for $j\geq 2$,

$$p_{j+1}\equiv ap_j^2 \pmod 2\quad\text{so that}\quad r_k\equiv p_k\equiv a^{2^{k-1}} \pmod 2.$$

The constant coefficient of r_k is -2. It follows from the Eisenstein criterion that r_k is irreducible over $\mathbb{Q}$. $\square$

2.4. **Irreducibility over $\mathbb{Q}$.** We may now complete the proof of Proposition 15.

Proposition 19. *The polynomial $R_k\in\mathbb{Z}[a,b]$ is irreducible over $\mathbb{Q}$.*

Proof. Assume by contradiction that $R_k = T_1\cdot T_2$ with $T_1\in\mathbb{Z}[a,b]$, $T_2\in\mathbb{Z}[a,b]$, degree$(T_1)<$ degree(R_k) and degree$(T_2)<$ degree(R_k). Consider the polynomials $t_1\in\mathbb{Z}[a]$ and $t_2\in\mathbb{Z}[a]$ defined by

$$t_1(a) := T_1(a,2)\quad\text{and}\quad t_2(a) := T_2(a,2).$$

Then, $r_k = t_1\cdot t_2$ with degree$(t_1)\leq$ degree$(T_1)<$ degree$(R_k) =$ degree(r_k). Similarly, degree$(t_2)<$ degree(r_k). This is not possible since r_k is irreducible over $\mathbb{Q}$. $\square$

3. Unicritical polynomials

The previous discussion motivates a more systematic study of irreducibility over $\mathbb{Q}$ within families of unicritical polynomials. This section is devoted to such a study. It can be read independently of the rest of the article. Consider the polynomials $f_a : \mathbb{C} \to \mathbb{C}$ defined by

$$f_a(z) = az^D + 1, \quad a \in \mathbb{C}.$$

The polynomial f_a is unicritical: it has a unique critical point at $z = 0$. We are interested in parameters a such that the critical point is preperiodic for f_a. Note that the preperiod k cannot be equal to 1.

For $n \geq 1$, let $P_n \in \mathbb{Z}[a]$ be the polynomial

$$P_n(a) := f_a^{\circ n}(0).$$

Andrew Gleason observed that the discriminant of P_n is 1 (mod D), and thus P_n has simple roots. It follows that

$$P_n = \prod_{m|n} R_m \quad \text{with} \quad R_n := \prod_{m|n} P_m^{\mu(n/m)} \in \mathbb{Z}[a],$$

where μ is the Möbius function defined by $\mu(i) = (-1)^j$ if i is the product of j distinct primes with $j \geq 0$ and $\mu(i) = 0$ otherwise. For example,

$$R_1 = P_1 = 1, \quad R_2 = P_2 = a + 1 \quad \text{and} \quad R_3 = P_3 = a(a+1)^D + 1.$$

It is conjectured that when $D = 2$, the polynomials R_n are irreducible over $\mathbb{Q}$ for all $k \geq 2$. The following result shows that this is not true when $D \equiv 1 \pmod 6$.

Proposition 20 ([Bu])**.** *The polynomial R_3 is irreducible over $\mathbb{Q}$ if and only if D is not congruent to 1 modulo 6. When $D \equiv 1 \pmod 6$, the polynomial R_3 has exactly two irreducible factors over $\mathbb{Q}$, one of which is $a^2 + a + 1$.*

Assume now that 0 is preperiodic for f_a with preperiod $k \geq 2$ and period $n \geq 1$. Then,

$$f_a^{\circ(k+n-1)}(0) = \omega f_a^{\circ(k-1)}(0) \quad \text{with} \quad \omega^D = 1 \quad \text{and} \quad \omega \neq 1. \tag{2}$$

In fact, Equation (2) is satisfied if and only if either 0 is periodic for f_a with period dividing $\gcd(n, k-1)$, or 0 is preperiodic for f_a with preperiod k and period dividing n.

For $k \geq 2$, $n \geq 1$ and $d \geq 2$ dividing D, we therefore consider the monic polynomial $R_{k,n,d}$ whose roots are the parameters $a \in \mathbb{C}$ such that

- 0 is preperiodic for f_a with preperiod k and period n, and
- Equation (2) is satisfied for some primitive d-th root of unity ω.

We claim that $R_{k,n,d} \in \mathbb{Z}[a]$. Indeed, let $\Phi_d \in \mathbb{Z}[X, Y]$ be the (homogenized) d-th cyclotomic polynomial: if Ω_d is the set of primitive d-th roots of unity, then

$$\Phi_d := \prod_{\omega \in \Omega_d} (X - \omega Y).$$

Let $P_{k,n,d} \in \mathbb{Z}[a]$ be the polynomial defined by

$$P_{k,n,d} := \Phi_d(P_{k+n-1}, P_{k-1}) = \prod_{\omega \in \Omega_d} (P_{k+n-1} - \omega P_{k-1}).$$

The polynomial $P_{k+n-1} - \omega P_{k-1}$ has simple roots (see [Bu] for example). In addition, the common roots of P_{k+n-1} and P_{k-1} are the roots of $P_{\gcd(n,k-1)}$. It follows that the multiple roots of $P_{k,n,d}$ are the roots of $P_{\gcd(n,k-1)}$ with multiplicities $\varphi(d) = \deg(\Phi_d)$, where φ is the Euler totient function. As a consequence,

$$P_{k,n,d} = P_{\gcd(n,k-1)}^{\varphi(d)} \cdot \prod_{m|n} R_{k,m,d} \tag{3}$$

and according to the Möbius Inversion Formula,

$$R_{k,n,d} = \prod_{m|n} \left(\frac{P_{k,m,d}}{P_{\gcd(m,k-1)}^{\varphi(d)}} \right)^{\mu(n/m)} \in \mathbb{Z}[a].$$

We also consider the polynomials $P_{k,n} \in \mathbb{Z}[a]$ and $R_{k,n} \in \mathbb{Z}[a]$ defined by

$$P_{k,n} := \prod_{\substack{d|D \\ d\neq 1}} P_{k,n,d} = \frac{P_{k+n-1}^D - P_{k-1}^D}{P_{k+n-1} - P_{k-1}} = \sum_{i+j=D-1} P_{k+n-1}^i \cdot P_{k-1}^j.$$

and

$$R_{k,n} := \prod_{\substack{d|D \\ d\neq 1}} R_{k,n,d} \in \mathbb{Z}[a] \quad \text{so that} \quad P_{k,n} = P_{\gcd(n,k-1)}^{D-1} \cdot \prod_{m|n} R_{k,m}. \tag{4}$$

In [M3, Remark 3.5], Milnor provides geometric motivation for the following conjecture (compare with [HT]).

Conjecture. *For all $k \geq 2$, $n \geq 1$, and $d \geq 2$ that divide $D \geq 2$, the polynomial $R_{k,n,d}$ is irreducible over $\mathbb{Q}$.*

There are few cases where the expression of $R_{k,n,d}$ is sufficiently simple so that existing results in the literature directly apply (see §3.4).

Theorem 21 ([G])**.** *If D is a prime number, then $R_{k,1}(c^{D-1}) \in \mathbb{Z}[c]$ is irreducible for all $k \geq 2$. If $D = 2$, then $R_{k,2}$ is irreducible for all $k \geq 2$.*

We prove the following theorem. In the remainder of the article, p is a prime number.

Theorem 22. *Assume $D = p^e$ is a prime power. Then $R_{k,1,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$, and for all $d \geq 2$ that divide D. More generally, if $n \geq 2$ and the polynomial $R_n \pmod p$ is irreducible over $\mathbb{F}_p$, then $R_{k,n,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$, and for all $d \geq 2$ that divide D.*

Corollary 23. *Assume $D = p^e$ is a prime power. Then $R_{k,2,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$, and for all $d \geq 2$ that divide D.*

Proof. The reduction of $R_2 = a + 1$ modulo p is irreducible over $\mathbb{F}_p$. □

Corollary 24. *If $D = 2$ then $R_{k,3}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.*

Proof. If $D = 2$, then $R_3 = a(a+1)^2 + 1 \equiv 1 + a + a^3 \pmod 2$ and $R_3 \pmod 2$ is irreducible over $\mathbb{F}_2$. □

Corollary 25. *If $D = 8$, then $R_{k,3,2}$, $R_{k,3,4}$ and $R_{k,3,8}$ are irreducible over $\mathbb{Q}$ for all $k \geq 2$.*

Proof. If $D = 8$, then $R_3 = a(a+1)^8 + 1 \equiv 1 + a + a^9 \pmod 2$ and $R_3 \pmod 2$ is irreducible over $\mathbb{F}_2$. □

Remark. The only values of $D = p^e$ and $n \geq 2$ for which the polynomial $R_n \pmod p$ is irreducible over $\mathbb{F}_p$ are the ones listed previously: $n = 2$ for any prime power degree D, and $n = 3$ for both $D = 2$ and $D = 8$ (see §3.5).

Our proof of Theorem 22 relies on the following two results (see §3.3).

Lemma 26. *Assume $d \geq 2$ divides $D \geq 2$. Assume $k \geq 2$, $n \geq 1$ and $m \geq 1$. Then,*

$$\operatorname{resultant}(R_{k,m,d}, R_n) = \begin{cases} \pm p^{\deg(R_n)} & \text{if } n = m \text{ and } d = p^e \text{ is a prime power} \\ \pm 1 & \text{otherwise.} \end{cases}$$

Lemma 27. *Assume $D = p^e$ is a prime power and $d \geq 2$ is a divisor of D. Then for all $k \geq 2$, the polynomials $R_{k,1,d} \pmod p$ are powers of $a \in \mathbb{F}_p[a]$; and for all $k \geq 2$ and all $n \geq 2$, the polynomials $R_{k,n,d} \pmod p$ are powers of $R_n \pmod p$.*

Remark. Lemma 26 shows a connection between the polynomials $R_{k,n,d}$ and the polynomials R_n, valid for all degrees $D \geq 2$. Lemma 27 shows a stronger connection between these polynomials, but only valid for prime power degrees $D = p^e$. We think that it is worth investigating what this relation becomes when D is no longer a prime power.

3.1. **The critical orbit.** On our way to proving Theorem 22, we first study some arithmetic properties of the polynomials $P_k \in \mathbb{Z}[a]$. Recall that by definition, for all $k \geq 1$,

$$P_k(a) := f_a^{\circ k}(0).$$

For $k \geq 0$, set

$$N_k := \frac{D^k - 1}{D - 1} \quad \text{so that} \quad 1 + DN_k = \frac{D - 1 + D^{k+1} - D}{D - 1} = N_{k+1}.$$

Lemma 28. *For all $k \geq 1$, the polynomial P_k has constant coefficient 1 and is monic of degree N_{k-1}.*

Proof. First, note that $P_1 = 1$ and for all $k \geq 1$, $P_{k+1} = aP_k^D + 1$. It follows that the constant coefficient of P_{k+1} is 1. Second, let us prove by induction on $k \geq 1$ that P_k is monic of degree N_{k-1}. The property holds for $k = 1$: indeed, $P_1 = 1$ and $N_0 = 0$. Now, if the result holds for some integer $k \geq 1$, then $P_{k+1} = aP_k^D + 1$ is monic of degree $1 + DN_{k-1} = N_k$. □

Lemma 29. *Assume $D = p^e$ is a prime power. For all $k \geq 1$,*

$$P_{k+1} - P_k \equiv a^{N_k} \pmod p.$$

Proof. We prove the result by induction on $k \geq 1$. For $k = 1$,

$$P_2 - P_1 = a + 1 - 1 = a = a^{N_1}.$$

Now, assume the property holds for some $k \geq 1$. Since $D = p^e$,

$$\begin{aligned} P_{k+2} - P_{k+1} &= (aP_{k+1}^D + 1) - (aP_k^D + 1) \\ &= a \cdot (P_{k+1}^D - P_k^D) \equiv a \cdot (P_{k+1} - P_k)^D \pmod p. \end{aligned}$$

Thus,

$$P_{k+2} - P_{k+1} \equiv a^{1+DN_k} \pmod p \equiv a^{N_{k+1}} \pmod p.$$ □

We conclude this section by the following observation due to Poonen.

Lemma 30 (Poonen)**.** *For $m \neq n$, we have that* resultant$(R_m, R_n) = \pm 1$.

Proof. Assume $n > m$. It is not hard to see by induction on $k \geq 1$, that

$$P_{m+k} \equiv P_k \pmod{P_m^D}.$$

Indeed, $P_{m+1} = aP_m^D + 1 = P_1 + aP_m^D$ and if $P_{m+k} \equiv P_k \pmod{P_m^D}$, then

$$P_{m+k+1} = aP_{m+k}^D + 1 \equiv aP_k^D + 1 \pmod{P_m^D} \equiv P_k \pmod{P_m^D}.$$

This implies that, $P_{mn} \equiv P_m \pmod{P_m^D}$. Since $m < n$, $P_m R_n$ divides P_{mn}. So, there are polynomials $A \in \mathbb{Z}[a]$ and $B \in \mathbb{Z}[a]$ such that

$$AP_m R_n = P_{mn} = P_m + BP_m^D.$$

Dividing by P_m yields $AR_n - BP_m^{D-1} = 1$. It follows that R_m and R_n are relatively prime in $\mathbb{Z}[a]$ and resultant$(R_m, R_n) = \pm 1$. □

3.2. **When the critical point is preperiodic to a fixed point.** As a next step toward proving Theorem 22, we prove the following proposition that is due to Vefa Goksel. Our proof differs significantly from the one given in [G].

Proposition 31. *If D is prime, then $R_{k,1}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.*

Proof. Our proof relies on the following two lemmas.

Lemma 32. *For $k \geq 2$ and $n \geq 1$, the polynomial $P_{k,n}$ has constant coefficient D and is monic of degree $(D-1)N_{k+n-2}$.*

Proof. By Lemma 28, if $i + j = D - 1$, the polynomial $P_{k+n-1}^i \cdot P_{k-1}^j$ has constant coefficient 1 and is monic of degree

$$i \cdot N_{k+n-2} + j \cdot N_{k-2} \leq (D-1)N_{k+n-2}$$

with equality if and only if $i = D - 1$ and $j = 0$. There are D pairs $(i,j) \in \mathbb{N}^2$ such that $i + j = D - 1$. Only one pair contributes to the leading term. Thus the polynomial is monic. Every pair contributes to the constant coefficient, which therefore is equal to D. □

Lemma 33. *If D is prime, then for all $k \geq 1$,*

$$R_{k,1} = P_{k,1} \equiv a^{(D-1)N_{k-1}} \pmod{D}.$$

Proof. Assume D is prime. On the one hand, according to Lemma 29:

$$P_k^D - P_{k-1}^D \equiv (P_k - P_{k-1})^D \pmod{D} \equiv a^{DN_{k-1}} \pmod{D}. \tag{5}$$

On the other hand, by definition of $P_{k,1}$:

$$P_k^D - P_{k-1}^D = (P_k - P_{k-1}) \cdot P_{k,1} \equiv a^{N_{k-1}} P_{k,1} \pmod{D}.$$

As a consequence,

$$a^{N_{k-1}} P_{k,1} \equiv a^{DN_{k-1}} \pmod{D} \quad \text{so that} \quad P_{k,1} \equiv a^{(D-1)N_{k-1}} \pmod{D}. \qquad \square$$

The proposition now follows from the Eisenstein criterion: $R_{k,1}$ is monic, D divides all the coefficients except the one of the leading term, and D^2 does not divide the constant coefficient. □

3.3. **The general case.** This section is devoted to the proof of Theorem 22. We first prove Lemmas 26 and 27.

Proof of Lemma 26. Assume $d \geq 2$ divides $D \geq 2$, $k \geq 2$, $n \geq 1$ and $m \geq 1$. We need to show that

$$\operatorname{resultant}(R_{k,m,d}, R_n) = \begin{cases} \pm p^{\deg(R_n)} & \text{if } n = m \text{ and } d = p^e \text{ is a prime power} \\ \pm 1 & \text{otherwise.} \end{cases}$$

The proof splits into several cases.

Case 1: n does not divide m. Assume α is a root of R_n. Then, $P_{j_1}(\alpha) = P_{j_2}(\alpha)$ if and only if $j_1 \equiv j_2 \pmod{n}$. Since n does not divide m, for all $k \geq 2$,

$$P_{k+m-1}(\alpha) - P_{k-1}(\alpha) \neq 0 \quad \text{and} \quad \alpha P_{k,m}(\alpha) = \frac{P_{k+m}(\alpha) - P_k(\alpha)}{P_{k+m-1}(\alpha) - P_{k-1}(\alpha)},$$

so that

$$\alpha^n \prod_{j=0}^{n-1} P_{k+j,m}(\alpha) = 1.$$

The polynomial R_n is monic with constant coefficient 1. So, α is an algebraic unit. Thus,

$$\prod_{j=0}^{n-1} \operatorname{resultant}(P_{k+j,m}, R_n) = \prod_{j=0}^{n-1} \prod_{\alpha \in R_n^{-1}(0)} P_{k+j,m}(\alpha) = \prod_{j=0}^{n-1} \prod_{\alpha \in R_n^{-1}(0)} \frac{1}{\alpha^n} = \pm 1.$$

Since $R_{k,m,d}$ divides $P_{k,m}$, it follows that

$$\operatorname{resultant}(R_{k,m}, R_n) = \pm 1.$$

Case 2: n divides m. Set

$$\nu := \Phi_d(1,1) = \begin{cases} p & \text{if } d = p^e \text{ is a prime power} \\ 1 & \text{otherwise.} \end{cases}$$

It is enough to prove that

$$\prod_{\ell | m} \operatorname{resultant}(R_{k,\ell,d}, R_n) = \pm \nu^{\deg(R_n)}. \tag{6}$$

Indeed, assume Equation (6) holds. We have seen that $\operatorname{resultant}(R_{k,\ell,d}, R_n) = \pm 1$ when n does not divide ℓ. So, for $m = n$,

$$\begin{aligned} \pm \nu^{\deg(R_n)} &= \operatorname{resultant}(R_{k,n,d}, R_n) \cdot \prod_{\substack{\ell | n \\ \ell \neq n}} \operatorname{resultant}(R_{k,\ell,d}, R_n) \\ &= \pm \operatorname{resultant}(R_{k,n,d}, R_n). \end{aligned}$$

Now, if n divides $m \neq n$, the polynomial $R_{k,n,d} \cdot R_{k,m,d}$ divides $P_{k,m,d}$; and

$$\operatorname{resultant}(R_{k,n,d} \cdot R_{k,m,d}, R_n) = \pm \nu^{\deg(R_n)} \cdot \operatorname{resultant}(R_{k,m,d}, R_n)$$

divides

$$\operatorname{resultant}(P_{k,m,d}, R_n) = \pm \nu^{\deg(R_n)}.$$

This forces

$$\operatorname{resultant}(R_{k,m,d}, R_n) = \pm 1.$$

So, it is enough to prove that Equation (6) holds.

Case 2.a: n does not divide $k-1$. Assume α is a root of R_n. Since n divides m, we have that $P_{k+m-1}(\alpha) = P_{m-1}(\alpha)$ and

$$P_{k,m,d}(\alpha) = \Phi_d\big(P_{k+m-1}(\alpha), P_{k-1}(\alpha)\big) = P_{k-1}^{\varphi(d)}(\alpha)\cdot\Phi_d(1,1) = \nu P_{k-1}^{\varphi(d)}(\alpha).$$

It follows that

$$\begin{aligned}\mathrm{resultant}(P_{k,m,d}, R_n) &= \prod_{\alpha\in R_n^{-1}(0)} P_{k,m,d}(\alpha)\\ &= \nu^{\deg(R_n)}\cdot\prod_{\alpha\in R_n^{-1}(0)} P_{k-1}^{\varphi(d)}(\alpha) = \nu^{\deg(R_n)}\cdot\mathrm{resultant}(P_{k-1}^{\varphi(d)}, R_n).\end{aligned}$$

Since n does not divide $k-1$, Lemma 30 yields $\mathrm{resultant}(R_\ell, R_n) = \pm1$ for any divisor ℓ of $k-1$. Thus,

$$\begin{aligned}\mathrm{resultant}(P_{k,m,d}, R_n) &= \nu^{\deg(R_n)}\cdot\mathrm{resultant}(P_{k-1}^{\varphi(d)}, R_n)\\ &= \nu^{\deg(R_n)}\cdot\prod_{\ell\mid k-1}\big(\mathrm{resultant}(R_\ell, R_n)\big)^{\varphi(d)} = \pm\nu^{\deg(R_n)}.\end{aligned}$$

Equation (6) now follows from Equation (3).

Case 2.b: n divides $k-1$. As in the proof of Lemma 30, if n divides ℓ, then

$$P_\ell = P_n \pmod{P_n^D} = P_n\cdot(1+H_\ell)$$

with $H_\ell\in\mathbb{Z}[a]$ divisible by P_n. It follows that

$$P_{k,m,d} = \Phi_d\big(P_{k+m-1}, P_{k-1}\big) = P_n^{\varphi(d)}\cdot(\nu + H_{k,m,d})$$

with $H_{k,m,d}\in\mathbb{Z}[a]$ divisible by P_n. Since n divides $\gcd(m,k-1)$, Equation (3) yields

$$\left(\prod_{\substack{\ell\mid\gcd(m,k-1)\\ \ell\text{ does not divide }n}} R_\ell^{\varphi(d)}\right)\cdot\left(\prod_{\ell\mid m} R_{k,\ell,d}\right) = \nu + H_{k,m,d}P_n^{D-1}$$

and since $\mathrm{resultant}(R_\ell, R_n) = \pm1$ for $\ell\neq n$, we deduce that

$$\begin{aligned}\prod_{\ell\mid m}\mathrm{resultant}(R_{k,\ell,d}, R_n) &= \mathrm{resultant}(\nu + H_{k,m,d}P_n^{D-1}, R_n)\\ &= \mathrm{resultant}(\nu, R_n) = \pm\nu^{\deg(R_n)}.\end{aligned}$$

This is Equation (6).

The proof of Lemma 26 is completed □

Proof of Lemma 27. Assume $D = p^e$ is a prime power and $d\geq 2$ is a divisor of D. We need to show that for all $k\geq 2$, the polynomials $R_{k,1,d} \pmod p$ are powers of $a\in\mathbb{F}_p[a]$; and for all $k\geq 2$ and $n\geq 2$, the polynomials $R_{k,n,d} \pmod p$ are powers of $R_n \pmod p$. Since $R_{k,n,d}$ divides $R_{k,n}$ for all $n\geq 1$, it is enough to prove that for all $k\geq 2$, the polynomials $R_{k,1} \pmod p$ are powers of $a\in\mathbb{F}_p[a]$; and for all $k\geq 2$ and $n\geq 2$, the polynomials $R_{k,n} \pmod p$ are powers of $R_n \pmod p$.

For $k\geq 2$, set $M_{k,1} := (D-1)N_{k-1}$ and for $n\geq 2$, set

$$M_{k,n} := \begin{cases}(D-1)(D^{k-1}-1) & \text{if } n \text{ divides } k-1\\ (D-1)D^{k-1} & \text{if } n \text{ does not divide } k-1.\end{cases}$$

We prove that for $k \geq 2$ and $n \geq 2$,

$$R_{k,1} \equiv a^{M_{k,1}} \pmod p \quad \text{and} \quad R_{k,n} \equiv R_n^{M_{k,n}} \pmod p. \tag{7}$$

Note that $N_{i+j} - N_i = D^i N_j$ for all integers $i \geq 0$ and $j \geq 0$. So, according to Lemma 29, if $k \geq 2$ and $n \geq 1$,

$$\begin{aligned} P_{k+n-1} - P_{k-1} &\equiv a^{N_{k-1}} + a^{N_k} + \cdots + a^{N_{k+n-2}} \pmod p \\ &\equiv a^{N_{k-1}} \cdot \left(a^{D^{k-1}N_0} + a^{D^{k-1}N_1} + \cdots + a^{D^{k-1}N_{n-1}} \right) \pmod p \\ &\equiv a^{N_{k-1}} \cdot \left(a^{N_0} + a^{N_1} + \cdots + a^{N_{n-1}} \right)^{D^{k-1}} \pmod p \\ &\equiv a^{N_{k-1}} P_n^{D^{k-1}} \pmod p. \end{aligned}$$

As a consequence,

$$P_{k+n-1}^D - P_{k-1}^D \equiv a^{DN_{k-1}} P_n^{D^k} \pmod p$$

and

$$P_{k,n} \equiv a^{(D-1)N_{k-1}} P_n^{D^k - D^{k-1}} \pmod p \equiv a^{M_{k,1}} P_n^{(D-1)D^{k-1}} \pmod p.$$

In particular, for $n = 1$, this yields

$$R_{k,1} = P_{k,1} \equiv a^{M_{k,1}} \pmod p.$$

According to Equation (4),

$$\left(\prod_{m \mid \gcd(n,k-1)} R_m^{D-1} \right) \cdot \left(\prod_{m \mid n} R_{k,m} \right) = P_{k,n} \equiv a^{M_{k,1}} \cdot \prod_{m \mid n} R_m^{(D-1)D^{k-1}} \pmod p$$

and since $R_1 = 1$ and $R_{k,1} \equiv a^{M_{k,1}} \pmod p$,

$$\prod_{\substack{m \mid n \\ m \neq 1}} R_{k,m} \equiv \prod_{\substack{m \mid n \\ m \neq 1}} R_m^{M_{k,m}} \pmod p.$$

Equation (7) now follows from the Möbius inversion formula, completing the proof of Lemma 27. □

To complete the proof of Theorem 22, we will prove the generalized Eisenstein criterion stated in the Introduction in Lemma 6. For convenience, we recall the statement here. Let $A \in \mathbb{Z}[a]$ and $B \in \mathbb{Z}[a]$ be monic polynomials, and let p be a prime number such that

- $A \equiv B^N \pmod p$ for some integer $N \geq 1$;
- the polynomial $B \pmod p$ is irreducible over $\mathbb{F}_p$;
- $p^{2\deg(B)}$ does not divide resultant(A, B).

Then A is irreducible over $\mathbb{Q}$.

Proof of Lemma 6. Assume by contradiction that A is reducible over $\mathbb{Q}$, so that $A = A_1 A_2$ with $A_1 \in \mathbb{Z}[a]$ and $A_2 \in \mathbb{Z}[a]$ non constant. Let $\overline{A}_1$, $\overline{A}_2$ and $\overline{B}$ be the reductions of the polynomials modulo p. Then, $\overline{A}_1 \overline{A}_2 = \overline{B}^N$ and since $\overline{B}$ is irreducible over $\mathbb{F}_p$, we have that $\overline{A}_1 = \overline{B}^{N_1}$ and $\overline{A}_2 = \overline{B}^{N_2}$ for some positive integers $N_1 \geq 1$ and $N_2 \geq 1$. In other words, $A_1 = B^{N_1} + pC_1$ and $A_2 = B^{N_2} + pC_2$ for some polynomials $C_1 \in \mathbb{Z}[a]$ and $C_2 \in \mathbb{Z}[a]$. In that case,

$$\begin{aligned}\mathrm{resultant}(A,B) = \mathrm{resultant}(A_1A_2,B) &= \mathrm{resultant}(A_1,B)\cdot\mathrm{resultant}(A_2,B)\\ &= \mathrm{resultant}(pC_1,B)\cdot\mathrm{resultant}(pC_2,B)\\ &= p^{2\deg(B)}\mathrm{resultant}(C_1C_2,B).\end{aligned}$$

This contradicts the assumption that $p^{2\deg(B)}$ does not divide resultant(A,B). □

We now complete the proof of Theorem 22. Assume $D = p^e$ is a prime power and $d \geq 2$ is a divisor of D. Then d is a power of p.

According to Lemma 27, the polynomial $R_{k,1,d} \pmod p$ is a power of $a \in \mathbb{F}_p[a]$, which is irreducible over $\mathbb{F}_p$; and according to Lemma 26, $p^{2\deg(R_n)}$ does not divide resultant$(R_{k,1,d}, R_1) = \pm p^{\deg(R_n)}$. It follows from Lemma 6 that $R_{1,k,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.

Similary, according to Lemma 27, if $n \geq 2$, the polynomial $R_{k,n,d} \pmod p$ is a power of $R_n \pmod p$; and according to Lemma 26, $p^{2\deg(R_n)}$ does not divide resultant$(R_{k,n,d}, R_n) = \pm p^{\deg(R_n)}$. It follows from Lemma 6 that when $R_n \pmod p$ is irreducible over $\mathbb{F}_p$, the polynomial $R_{k,n,d}$ is irreducible over $\mathbb{Q}$ for all $k \geq 2$.

This completes the proof of Theorem 22.

3.4. **Particular cases.** For small values of k and n, the expression of $R_{k,n,d}$ is quite simple and we may obtain irreducibility as follows.

Proposition 34. *For all $D \geq 2$ and all d that divide D, the polynomial $R_{2,1,d}$ is irreducible over $\mathbb{Q}$.*

Proof. We have that

$$R_{2,1,d} = \Phi_d(a+1, 1).$$

Since cyclotomic polynomials are irreducible over $\mathbb{Q}$, so is $R_{2,1,d}$. □

Proposition 35. *For all $D \geq 2$ even, the polynomial $R_{3,1,2}$ is irreducible over $\mathbb{Q}$.*

Proof. Setting $b := a + 1$, we have that

$$R_{3,1,2} = \Phi_2(P_3, P_2) = P_3 + P_2 = a(a+1)^D + 1 + (a+1) = b^{2d+1} - b^{2d} + b + 1.$$

By [FJ, Theorem 2], this quadrinomial is irreducible for all $d \geq 1$. □

Proposition 36. *For all $D \geq 2$ even, the polynomial $R_{2,2,2}$ is irreducible over $\mathbb{Q}$.*

Proof. Assume $D = 2d$ is even. Then setting $b = a + 1$ as previously,

$$\begin{aligned}R_{2,2,2} = \frac{\Phi_2(P_3,P_1)}{\Phi_2(P_2,P_1)} &= \frac{P_3+P_1}{P_2+P_1}\\ &= \frac{a(a+1)^D+2}{a+2}\\ &= \frac{b^{2d+1}-b^{2d}+2}{b+1} = b^{2d} - 2b^{2d-1} + 2b^{2d-2} - \cdots - 2b + 2.\end{aligned}$$

According to the Eisenstein criterion, this polynomial is irreducible over $\mathbb{Q}$. □

3.5. **Irreducibility over $\mathbb{F}_p$.** Here, $D = p^e$ is a prime power, and we work over the field $\mathbb{F}_p$ or its algebraic closure $\overline{\mathbb{F}}_p$. Abusing notation, we keep the notation P_n and R_n for their reductions modulo p. In other words, $P_n \in \mathbb{F}_p[a]$ and $R_n \in \mathbb{F}_p[a]$ are defined by

$$P_n := \sum_{k=0}^{n-1} a^{N_k} \quad \text{with} \quad N_k := \frac{D^k - 1}{D - 1} \quad \text{and} \quad R_n := \prod_{m|n} P_m^{\mu(n/m)}.$$

We study the irreducibility of R_n over $\mathbb{F}_p$. Note that

$$R_1 = 1 \quad \text{and} \quad R_2 = a + 1.$$

So, we restrict our study to the case $n \geq 3$.

Proposition 37. *Assume $D = p^e$ is a prime power and $n \geq 3$. Then, the polynomial $R_n \in \mathbb{F}_p[a]$ is irreducible over $\mathbb{F}_p$ if and only if either $n = 3$ and $D = 2$, or $n = 3$ and $D = 8$.*

Proof. Let $f : \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ be the Frobenius automorphism $x \mapsto x^p$.

Lemma 38. *If $\alpha \in \overline{\mathbb{F}}_p$ is a root of R_n, then α is a periodic point of f of period dividing $n \cdot e$.*

Proof. Assume α is a root of R_n. Then, $P_n(\alpha) = 0$, so that

$$\begin{aligned} 1 = 1 + \alpha P_n^D(\alpha) &= 1 + \alpha P_n(\alpha^D) \\ &= 1 + \sum_{k=0}^{n-1} \alpha^{1+DN_k} \\ &= 1 + \sum_{k=0}^{n-1} \alpha^{N_{k+1}} = P_n(\alpha) + \alpha^{N_n} = \alpha^{N_n}. \end{aligned}$$

It follows that

$$f^{\circ(n\cdot e)}(\alpha) = \alpha^{D^n} = \alpha^{1+(D-1)N_n} = \alpha \cdot \left(\alpha^{N_n}\right)^{D-1} = \alpha. \qquad \square$$

As a consequence, if R_n is irreducible over $\mathbb{F}_p$, then the degree of R_n divides $n \cdot e$. The degree of R_n is

$$\deg(R_n) = \sum_{m|n} \mu\left(\frac{n}{m}\right) \deg(P_m) = \sum_{m|n} \mu\left(\frac{n}{m}\right) N_{m-1} \geq D^{n-2}.$$

So, if R_n is irreducible over $\mathbb{F}_p$, then $p^{(n-2)e} \leq n \cdot e$.

Set $\kappa := (n-2)\log(p) > 0$. The function $(0, +\infty) \ni x \mapsto \exp(\kappa x)/x \in (0, +\infty)$ reaches a minimum at $x = 1/\kappa$ with value $\kappa \cdot \exp(1)$. It follows that for $n \geq 3$,

$$\frac{p^{(n-2)e}}{n \cdot e} \geq \left(1 - \frac{2}{n}\right) \log(p) \exp(1).$$

If $n \geq 3$ and $p \geq 5$, or if $n \geq 4$ and $p = 3$, or if $n \geq 5$ and $p = 2$, this is greater than 1. So, it is enough to study the following cases.

Case $n = 3$ and $p = 2$. In that case, for $e \geq 1$,

$$\deg(R_n) = 1 + D = 2^e + 1 \quad \text{and} \quad n \cdot e = 3e.$$

The function $(0, +\infty) \ni x \mapsto (2^x + 1)/(3x) \in (0, +\infty)$ is increasing on $[2, +\infty)$ and takes the values 1 at $x = 1$, $5/6$ at $x = 2$ and 1 at $x = 3$. It follows that $\deg(R_n)$

divides $n \cdot e$ if and only if $e = 1$ or $e = 3$, i.e. $D = 2$ or $D = 8$; in those two cases, R_3 is irreducible.

Case $n = 3$ and $p = 3$. In that case, for $e \geq 1$,

$$\deg(R_n) = 1 + D = 3^e + 1 > 3e = n \cdot e = 3e.$$

So, R_n cannot be irreducible in that case.

Case $n = 4$ and $p = 2$. In that case, for $e \geq 1$,

$$\deg(R_n) = 1 + D + D^2 = 1 + 3^e + 3^{2e} > 4e = n \cdot e.$$

So, R_n cannot be irreducible in that case. □

References

[AK] M. Arfeux & J. Kiwi *Irreducibility of the set of cubic polynomials with one periodic critical point*, Preprint, https://arxiv.org/abs/1611.09281

[BD] M. Baker & L. DeMarco *Special curves and postcritically-finite polynomials*, Forum Math. PI 1 (2013).

[BH] B. Branner & . H. Hubbard *The iteration of cubic polynomials. Part I: The global topology of parameter space*, Acta Math., 160(3-4) (1988), 143–206.

[BKM] A. Bonifant, J. Kiwi & J. Milnor *Cubic polynomial maps with periodic critical orbit. II. Escape regions*. Conform. Geom. Dyn., 14 (2010), 68–112.

[Bo] T. Bousch *Sur quelques problèmes de dynamique holomorphe*, Ph.D. thesis, Université de Paris- Sud, Orsay, (1992).

[Bu] X. Buff *On Postcritically Finite Unicritical Polynomials*, Preprint, https://www.math.univ-toulouse.fr/~buff/Preprints/Gleason/Gleason.pdf.

[DS] L. DeMarco & A. Schiff *Enumerating the basins of infinity of cubic polynomials* J. Difference Equ. Appl., 16(5–6), (2010), 451–461.

[E1] A. L. Epstein *Integrality and rigidity for postcritically finite polynomials*, Bull. London Math. Soc. 44 (2012), 39–46.

[E2] A. L. Epstein *Transversality in holomorphic dynamics*, Preprint.

[FJ] C. Finch & L. Jones *On the irreducibility of $\{-1, 0, 1\}$-quadrinomials*, Integers 6 (2006).

[G] V. Goksel *On the orbit of a post-critically finite polynomial of the form $x^d + c$*, Preprint, https://arxiv.org/abs/1806.01208.

[HT] B. Hutz & A. Towsley *Misiurewicz points for polynomial maps and transversality*, New York J. Math. 21 (2015), 297–319.

[M1] J. Milnor *Geometry and dynamics of quadratic rational maps*, Experiment. Math. Volume 2, Issue 1 (1993), 37–83.

[M2] J. Milnor *Cubic polynomials with periodic critical orbit, Part I*, In “Complex Dynamics Families and Friends”, ed. D. Schleicher, A. K. Peters (2009), 333–411.

[M3] J. Milnor *Arithmetic of unicritical polynomial maps*, Frontiers in Complex Dynamics: In Celebration of John Milnor’s 80th Birthday (2012), 15–23.

[Ra] R. Ramadas *Moduli spaces of quadratic rational maps: arithmetic and geometry*, Preprint, https://arxiv.org/abs/2205.07349.

[Re1] M. Rees *A partial description of parameter space of rational maps of degree two. i*, Acta Math., 168(1-2) (1992), 11–87.

[Re2] M. Rees *A partial description of the parameter space of rational maps of degree two. ii*, Proc. London Math. Soc. (3), (1995), 644–690.

[Re3] M. Rees *View of Parameter Space: Topographer and Resident*, Astérisque 288, (2003).

[T] V. Timorin *Topological regluing of rational functions*, Invent. Math., (2010), 61– 506.

Email address: xavier.buff@math.univ-toulouse.fr

Institut de Mathématiques de Toulouse, UMR5219, Université de Toulouse, CNRS, UPS, F-31062 Toulouse Cedex 9, France

Email address: adame@maths.warwick.ac.uk

Mathematics institute, University of Warwick, Coventry CV4 7AL, United Kingdom

Email address: kochsc@umich.edu

Department of Mathematics, 530 Church Street, East Hall, University of Michigan, Ann Arbor MI 48109, United States