IMRN International Mathematics Research Notices
2005, No. 14

Finitely Ramified Iterated Extensions

Wayne Aitken, Farshid Hajir, and Christian Maire

1 Introduction

Let p be a prime number, K a number field, and S a finite set of places of K. Let K_S be the compositum of all extensions of K (in a fixed algebraic closure $\overline{K}$) which are unramified outside S, and put $G_{K,S} = \mathrm{Gal}(K_S/K)$ for its Galois group. These *arithmetic fundamental groups* play a very important role in number theory. Algebraic geometry provides the most fruitful known source of information concerning these groups. Namely, given a smooth projective variety X/K, the p-adic étale cohomology groups of X are finite-dimensional vector spaces over $\mathbb{Q}_p$ equipped with an action of $G_{K,S}$ where S consists of the primes of bad reduction for X/K together with the primes of K of residue characteristic p. The richness of this action can be judged, for example, by the intimate relationships between algebraic geometry and the theory of automorphic forms which it mediates.

For this and many other reasons, it would be difficult to overstate the importance of these p-adic Galois representations. Nonetheless, linear p-adic groups simply form too restrictive a class of groups to capture *all* Galois-theoretic information, and some important conjectures in the subject, notably the Fontaine-Mazur conjecture [10] (to mention only one, see the discussion in Section 7), point specifically toward the kind of information inside arithmetic fundamental groups which cannot be captured by finite-dimensional p-adic representations.

Received 19 October 2004. Revision received 3 December 2004.
Communicated by Barry Mazur.

In this work, we discuss a method for studying finitely ramified extensions of number fields via *arithmetic dynamical systems on* $\mathbb{P}^1$. At least conjecturally, this method provides a vista on a part of $G_{K,S}$ invisible to p-adic representations. We now sketch the construction, which is quite elementary. Suppose $\varphi \in K[x]$ is a polynomial of degree $d \geq 1$.[1] For each $n \geq 0$, let $\varphi^{\circ n}$ be the n-fold iterate of φ, that is, $\varphi^{\circ 0}(x) = x$ and $\varphi^{\circ n+1}(x) = \varphi(\varphi^{\circ n}(x)) = \varphi^{\circ n}(\varphi(x))$ for $n \geq 0$. Let t be a parameter for $\mathbb{P}^1_{/K}$ with function field $F = K(t)$. We are interested in the tower of branched covers of $\mathbb{P}^1$ given by

$$\Phi_n(x,t) \stackrel{\text{def}}{=} \varphi^{\circ n}(x) - t \in F[x], \tag{1.1}$$

as well as extensions of K obtained by adjoining roots of its specializations at arbitrary $t_0 \in K$. The variable-separated polynomial $\Phi_n(x,t)$ is clearly absolutely irreducible over K (since it is linear in t). It is separable and irreducible, of degree d^n, in $F[x]$; see Lemma 2.1.

Fix an algebraic closure $\overline{F}$ of F, and let $\overline{K}$ be the algebraic closure of K determined by this choice, that is, the subfield of $\overline{F}$ consisting of elements algebraic over K. For $n \geq 0$, let $T_{\varphi,n}$ be the set of roots in $\overline{F}$ of $\Phi_n(x,t)$; it has cardinality d^n. We denote by T_φ the d-regular rooted tree whose vertex set is $\cup_{n\geq 0} T_{\varphi,n}$, and whose edges point from v to w exactly when $\varphi(v) = w$; its root (at ground level) is t.

We choose and fix an *end* $\xi = (\xi_0, \xi_1, \xi_2, \ldots)$ of this tree; in other words, we choose a compatible system of preimages of t under the iterates of φ: $\varphi(\xi_1) = \xi_0 = t$ and $\varphi(\xi_{n+1}) = \xi_n$ for $n \geq 1$. For each $n \geq 1$, we consider the field $F_n = F(\xi_n) \simeq F[x]/(\Phi_n)$ and its Galois closure $\mathcal{F}_n = F(T_{\varphi,n})$ over F. Let $\mathcal{O}_{\mathcal{F}_n}$ be the integral closure of $K[t]$ in $\mathcal{F}_n$. Corresponding to each $t_0 \in K$, we may fix compatible *specialization maps* $\sigma_{n,t_0} : \mathcal{O}_{\mathcal{F}_n} \to \overline{K}$ with image $\mathcal{K}_{n,t_0}$, a normal extension field of K, and put $\xi_n|_{t_0} = \sigma_{n,t_0}(\xi_n)$ for the corresponding compatible system of roots of $\Phi_n(x,t_0)$. We denote by K_{n,t_0} the image of the restriction of σ_{n,t_0} to $\mathcal{O}_{F_n}$. We refer the reader to Section 2.2 for more details, but we should emphasize here that $\Phi_n(x,t_0)$ is not necessarily irreducible over K; hence, although $\mathcal{K}_{n,t_0}$ depends only on φ, n, and t_0, the isomorphism class of K_{n,t_0} depends a priori on the choice of ξ as well as on the choice of compatible σ_{n,t_0}. Also, the Galois closure of $K_{n,t_0}/K$ is contained in, but possibly distinct from, $\mathcal{K}_{n,t_0}$.

Taking the compositum over all $n \geq 1$, we obtain the *iterated extension* $F_\varphi = \cup_n F_n$ attached to φ, with Galois closure $\mathcal{F}_\varphi = \cup_n \mathcal{F}_n$ over F. Similarly for each $t_0 \in K$, we obtain a specialized iterated extension $K_{\varphi,t_0} = \cup_n K_{n,t_0}$ with Galois closure over K contained in $\mathcal{K}_{\varphi,t_0} = \cup_n \mathcal{K}_{n,t_0}$. We put $\mathcal{M}_\varphi = \mathrm{Gal}(\mathcal{F}_\varphi/F)$ for the *iterated monodromy group* of φ and for $t_0 \in K$, we denote by $\mathcal{M}_{\varphi,t_0} = \mathrm{Gal}(\mathcal{K}_{\varphi,t_0}/K)$ its specialization at t_0. The group $\mathcal{M}_\varphi$ has a natural and faithful action on the tree T_φ, hence comes equipped

[1] This construction actually works for any perfect K as long as the derivative φ' is not identically zero in $K[x]$.

with a rooted tree representation $\mathcal{M}_\varphi \hookrightarrow \operatorname{Aut} T_\varphi$. For more on rooted trees and iterated monodromy groups (in a more general context, in fact), see Nekrashevych [14] as well as Bartholdi-Grigorchuk-Nekrashevych [1].

Since we are interested in finitely ramified towers (meaning those where only finitely many places of the base field are ramified), we need to answer the following question: which polynomials φ have the property that the corresponding iterated tower F_φ/F as well as all of its specializations $K_{\varphi,t_0}/K$ are finitely ramified?

We first recall some standard terminology from polynomial dynamics. We put

$$\mathcal{R}_\varphi \stackrel{\text{def}}{=} \{r \in \overline{K} : \varphi'(r) = 0\}, \qquad \mathcal{B}_\varphi \stackrel{\text{def}}{=} \{\varphi(r) : r \in \mathcal{R}_\varphi\} \tag{1.2}$$

for the set of affine *ramification* and *branch* points, respectively. The elements of $\mathcal{R}_\varphi$ and $\mathcal{B}_\varphi$ are also the *critical points*, respectively, *critical values* of φ. The polynomial φ is called *postcritically finite* if every member of $\mathcal{R}_\varphi$ is a preperiodic point for φ. In other words, φ is postcritically finite exactly when the *postcritical set* $\mathcal{P}_\varphi$, that is, the union of the orbits of critical points under the iterates of φ, is a finite set. It has long been known that the postcritical set plays a crucial role in the dynamics of the polynomial. Indeed, the class of dynamical systems corresponding to postcritically finite polynomials is a well-studied one, having gained prominence following a celebrated theorem of Thurston; see, for example, Douady and Hubbard [8], Bielefeld-Fisher-Hubbard [3], as well as the papers by Poirier [18, 17], Pilgrim [16], and Pakovich [15]; the latter two concern the connection with actions of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on certain finite trees.

Our starting point is the following characterization of finitely ramified iterated extensions.

Theorem 1.1. The iterated tower of function fields $\mathcal{F}_\varphi/F$ is finitely ramified if and only if φ is postcritically finite. If φ is postcritically finite, every specialization $\mathcal{K}_{\varphi,t_0}/K$ of this tower is finitely ramified. □

The first assertion of the theorem is clear geometrically since $\mathcal{B}_{\varphi^{\circ n}} = \mathcal{B}_\varphi \cup \varphi(\mathcal{B}_\varphi) \cup \cdots \cup \varphi^{\circ n-1}(\mathcal{B}_\varphi)$. The second assertion, however, is not a formal consequence of the first; the proof we give for it proceeds via Proposition 3.2, where we derive a formula for the discriminant of $\Phi_n(x,t)$ (valid for an arbitrary polynomial φ), giving a more precise version of the theorem. The proof of Proposition 3.2 uses basic properties of resultants.

For each postcritically finite $\varphi \in K[x]$, and each $t_0 \in K \setminus \mathcal{P}_\varphi$, Theorem 1.1 provides a surjection $\rho_{\varphi,t_0} : G_{K,S} \twoheadrightarrow \mathcal{M}_{\varphi,t_0}$ for an effectively determined finite set $S = S_{\varphi,t_0}$ of

places of K (see Definition 3.5 and Corollary 3.7). We call ρ_{φ,t_0} the *iterated monodromy representation* attached to φ and t_0.

The study of automorphism groups of rooted trees is a relatively new and quite active topic in group theory (see [1, 2, 14]). The structure of nonabelian subgroups of these automorphism groups appears to be quite different from that of linear p-adic groups (see the papers just cited as well as Bux and Perez [7]). The natural action of iterated monodromy groups on rooted trees leads us to the expectation that iterated monodromy representations ρ_{φ,t_0} attached to postcritically finite polynomials $\varphi \in K[x]$ have the potential of revealing aspects of arithmetic fundamental groups which are not visible to p-adic representations; see the discussion in Section 7 as well as Boston's preprint [4], where tree representations are suggested as the proper framework for studying finitely ramified tame extensions.

Since all finitely ramified p-adic Galois representations with infinite image are expected, by a conjecture of Fontaine and Mazur, to be wildly (even deeply) ramified at some prime of residue characteristic p, an immediate question is what can be said about the presence of wild ramification in specialized iterated extensions $\mathcal{K}_{\varphi,t_0}/K$. Experimentation leads to the expectation that generically the primes of residue characteristic dividing d ramify deeply in $\mathcal{K}_{\varphi,t_0}/K$. For example, if $\varphi(x) = x^d$ with $d > 1$ and $K = \mathbb{Q}$, then for all $t_0 \in \mathbb{Q}$, the extensions $\mathcal{K}_{\varphi,t_0}/K$ are deeply ramified at all p dividing d. (See, however, Questions 7.1 and 7.2 in Section 7.)

Under an assumption of good reduction for φ, we prove a partial result toward this expectation, namely for integral t_0, we estimate from below the power of p dividing the discriminant of $\Phi_n(x, t_0)$. To be precise, in Section 4, we will prove the following theorem.

Theorem 1.2. Let K be a number field. Suppose $\varphi \in K[x]$ is postcritically finite, has degree divisible by p, and has good reduction at a valuation ν of residue characteristic p, that is, φ has ν-integral coefficients with ν-unital leading coefficient. Then for any $t_0 \in \mathcal{O}_K$,

$$\nu\big(\operatorname{disc} \Phi_n(x, t_0)\big) \geq n d^n \nu(p). \tag{1.3}$$

□

Assuming $\Phi_n(x, t_0)$ is K-irreducible for all n, this estimate shows that the tower of rings $\mathcal{O}_K[\xi_n|_{t_0}]$, where $(\xi_n|_{t_0})$ is a compatible sequence of roots of $\Phi_n(x, t_0)$, is wildly ramified at p. Note that $\mathcal{O}_K[\xi_n|_{t_0}]$ is an *order* inside the maximal order of $K(\xi_n|_{t_0})$; it is the discriminant of the latter which is our primary interest, but the theorem estimates the discriminant of the former. This is one sense in which the above theorem is only a partial answer to our question about wild ramification in iterated extensions. On the other

hand, in Section 6, we illustrate with the tower corresponding to $\varphi(x) = x^2 - 2$, the possibility that the orders $\mathbb{Z}[\xi_n|_{t_0}]$ (for a large set of $t_0 \in \mathbb{Z}$) are maximal, giving examples of monogène number fields.

The organization of this paper is as follows. In Section 2, we outline some preliminary facts regarding postcritically finite polynomials, including a classification of the very simplest examples for each degree, namely those that are *critically fixed* (every critical point is fixed, also known as *conservative*) and *simply ramified* (every nontrivial ramification index is 2). In Sections 3 and 4, we prove Theorems 1.1 and 1.2, respectively. In Section 5, we describe the decomposition of unramified primes in iterated towers in terms of simple properties of certain finite graphs. In Section 6, we study the quadratic case in more detail, obtaining a recursion for writing down postcritically finite quadratic polynomials, which give number fields of independent interest; we also discuss the example x^2-2 in detail, proving monogenicity of certain number fields. Finally, in Section 7, we outline a number of questions and open problems.

2 Preliminaries

2.1 The branched cover $\varphi^{\circ n} : \mathbb{P}^1 \to \mathbb{P}^1$

In this section, K is a perfect field and $\varphi(x) = a_d x^d + \cdots + a_0 \in K[x]$ is a polynomial of degree $d \geq 1$ whose derivative φ' is not identically 0. We maintain all other notation introduced in Section 1.

Lemma 2.1. For each $n \geq 1$, $\Phi_n(x,t)$ is separable and absolutely irreducible over K hence irreducible over F. The ring $K[\xi_n, t]$ is integrally closed (in its fraction field F_n). □

Proof. All of this follows essentially from the fact that $\partial_t \Phi_n(x,t) = 1$ never vanishes. The reader can easily check the absolute irreducibility of Φ_n. For separability, assume that $\Phi_n(x,t)$ has a multiple root, ξ_n say. Then ξ_n is a root of $\partial_x \Phi_n(x,t) = (\varphi^{\circ n})'(x)$. Since φ' is not identically 0, neither is $(\varphi^{\circ n})'$, and so ξ_n is algebraic over K, and then so is $t = \varphi^{\circ n}(\xi_n)$, a contradiction. Note that if $\varphi' \equiv 0$, then $\Phi_n(x,t)$ is not separable over F, for in that case, every root of $\Phi_n(x,t)$ is vacuously a root of $\partial_x \Phi_n(x,t)$ and is therefore a multiple root. Next, observe that $K[\xi_n, t] = K[\xi_n]$ since $t = \varphi^{\circ n}(\xi_n)$. Since $K[\xi_n, t] = K[\xi_n]$ is $K[t]$-module of finite type, it cannot be a field; so $K[\xi]$ is isomorphic to $K[x]$. Since $K[x]$ is normal, the same holds for $K[\xi]$. ■

Thinking of φ as a branched cover $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d, the singular fibers are those of cardinality less than d. Leaving aside ∞ which is totally ramified, the points in a singular fiber (the ramification points) are exactly the critical points, that is, the roots

of φ': writing $\varphi(x) - \varphi(r) = (x-r)\psi_r(x)$ for any $r \in \overline{K}$, we have $\varphi'(r) = \psi_r(r)$ hence $(x-r)^2$ divides $\varphi(x) - \varphi(r)$ if and only if $\varphi'(r) = 0$. The critical values (the images under φ of the critical points), are the points having a singular fiber, that is, they are exactly the branch points. In algebraic language, $\beta \in \overline{K}$ is in $\mathcal{B}_\varphi$ if and only if $\varphi(x) - \beta$ has a multiple root, which happens if and only if $\operatorname{disc}_x(\varphi(x) - t)$ has $t = \beta$ as a root. In other words, β is a branch point if and only if the system

$$\varphi(x) = \beta, \qquad \varphi'(x) = 0 \tag{2.1}$$

has a common root $x = r$, and these roots are the ramification points above β. We could adopt the convention that $\mathcal{R}_\varphi$ and $\mathcal{B}_\varphi$ are "multisets" where each critical point or critical value occurs according to the multiplicity of the corresponding roots of φ', but to avoid confusion, we will be explicit about the multiplicities by writing

$$\varphi'(x) = d a_d \prod_{r \in \mathcal{R}_\varphi} (x-r)^{m_r(\varphi)}, \tag{2.2}$$

and putting, for $\beta \in \mathcal{B}_\varphi$,

$$M_\beta(\varphi) = \sum_{r \in \mathcal{R}_\varphi,\, \varphi(r) = \beta} m_r(\varphi). \tag{2.3}$$

2.2 Global specializations

Here we wish to clarify the nature of the specialization maps $\mathcal{F}_n \to \overline{K}$ associated with specializing t to $t_0 \in K$ as well as the relationship between the iterated monodromy group $\mathcal{M}_\varphi$ and its specializations $\mathcal{M}_{\varphi,t_0}$. We do so by defining a notion of *global specialization*. Let $\mathcal{O}_{\mathcal{F}_\varphi}$ be the integral closure of $K[t]$ in $\mathcal{F}_\varphi$. By integrality (and the going up theorem), the maximal ideal $(t - t_0)$ of $K[t]$ extends to a prime ideal $\mathfrak{t}_0$ of $\mathcal{O}_{\mathcal{F}_\varphi}$ such that $\mathfrak{t}_0 \cap K[t] = (t - t_0)$. The ring $\mathcal{O}_{\mathcal{F}_\varphi}/\mathfrak{t}_0$ is integral over K, so is actually a field. Thus $\mathfrak{t}_0$ is maximal, and $\mathcal{O}_{\mathcal{F}_\varphi}/\mathfrak{t}_0$ is algebraic over K. So there are embeddings $\mathcal{O}_{\mathcal{F}_\varphi}/\mathfrak{t}_0 \to \overline{K}$. Fix one, and consider the associated map $\sigma : \mathcal{O}_{\mathcal{F}_\varphi} \to \overline{K}$ with kernel $\mathfrak{t}_0$. We call such a map a *global specialization* associated with t_0. The image of the global specialization, which is a field $\mathcal{K}_{\varphi,t_0}$, is independent of the choice of global specialization σ.

Now we can define the specializations $\sigma_{n,t_0} : \mathcal{O}_{\mathcal{F}_n} \to \overline{K}$ and $\mathcal{O}_{F_n} \to \overline{K}$ by restriction of the global specialization. The field $\mathcal{K}_{n,t_0}$ can be defined as the image of $\mathcal{O}_{\mathcal{F}_n} \to \overline{K}$, and

can be shown to be independent of the choice of global specialization (associated with t_0). However, K_{n,t_0}, the image of $\mathcal{O}_{F_n} \to \overline{K}$, depends on the global specialization σ as well as on the choice of ξ_n.

In this optic, the relationship between the groups $\mathcal{M}_\varphi = \mathrm{Gal}(\mathcal{F}_\varphi/F)$ and the group $\mathcal{M}_{\varphi,t_0} = \mathrm{Gal}(\mathcal{K}_\varphi/K)$ is elucidated as follows. Let D_{t_0} be the *decomposition group* associated to t_0 (consisting of the elements of $\mathrm{Gal}(\mathcal{F}_\varphi/F)$ fixing the chosen maximal ideal t_0 of $\mathcal{O}_{\mathcal{F}_\varphi}$). Then D_{t_0} acts on $\mathcal{O}_{\mathcal{F}_\varphi}/t_0$, and therefore on $\mathcal{K}_{\varphi,t_0}$. Thus we get a homomorphism $D_{t_0} \to \mathrm{Gal}(\mathcal{K}_{\varphi,t_0}/K)$. As usual, this is a surjection, and if t_0 is not in the postcritical set, then it is actually an isomorphism. Thus, for $t_0 \in K \setminus \mathcal{P}_\varphi$, $\mathcal{M}_{\varphi,t_0}$ is isomorphic to a subgroup D_{t_0} of $\mathcal{M}_\varphi$, hence it too has an action on the rooted tree T_φ.

2.3 Dynamical systems on $\mathbb{P}^1$

Definition 2.2. Two self-maps φ, ψ of $\mathbb{P}^1$ defined over K (i.e., $\varphi, \psi \in K(x)$), are equivalent over K (or K-conjugate) if there exists an automorphism γ of $\mathbb{P}^1$ (defined over K) such that the diagram

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\gamma} & \mathbb{P}^1 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ \mathbb{P}^1 & \xrightarrow{\gamma} & \mathbb{P}^1 \end{array} \tag{2.4}$$

commutes. In other words, φ and ψ are equivalent over K if and only if there exist $a, b, c, d \in K$ satisfying $ad - bc \neq 0$ such that $\varphi(x) = \gamma^{-1}\psi\gamma(x)$ where $\gamma(x) = (ax + b)/(cx + d)$. The equivalence (or conjugacy) class of φ, denoted $[\varphi]$, is a *dynamical system* on $\mathbb{P}^1$. For $\varphi \in \mathbb{C}(x)$, we say $[\varphi]$ is *arithmetic* if there exists $\psi \in \overline{\mathbb{Q}}(x)$ with $[\varphi] = [\psi]$.

Note that if $\varphi \in K[x]$ is a polynomial map, the images of φ under *affine* transformations $\gamma(x) = ax + b$ over K form exactly the set of polynomial maps K-isomorphic to φ. Also, if γ takes $\varphi^{\circ n}$ to $\psi^{\circ n}$ for $n = 1$, then it does so for all $n \geq 1$. Thus, the study of iterations of φ and ψ coincide (they simply take place in different coordinates) precisely when φ and ψ are conjugate. In particular, if $[\varphi] = [\psi]$, then the iterated extensions $\mathcal{F}_\varphi$ and $\mathcal{F}_\psi$ are isomorphic. For a more detailed discussion, including the relationship between fields of moduli and fields of definition of dynamical systems on $\mathbb{P}^1$, we refer the reader to Silverman [21].

When discussing the coefficients of a postcritically finite polynomial, it is often convenient to normalize by working with *monic* postcritically finite polynomials.

Lemma 2.3. Every polynomial $\varphi \in K[x]$ of degree $d > 1$ is equivalent over some finite extension K'/K to a monic polynomial in $K'[x]$. Furthermore, if ψ and φ are two K'-equivalent monic polynomials for some finite extension K'/K, then

$$\psi(x) = \zeta^{-1}\varphi(\zeta x + c) - \zeta^{-1}c, \tag{2.5}$$

where c is in K' and ζ is a $(d-1)$th root of unity. □

Proof. Suppose ax^d is the leading term of φ. If $\gamma(x) = bx + c$, then $\gamma^{-1}(x) = b^{-1}x - b^{-1}c$. So $\gamma^{-1} \circ \varphi \circ \gamma(x)$ has leading term $b^{d-1}ax^d$. When we let b be a root of $x^{d-1} - a^{-1}$, we find that $\gamma^{-1} \circ \varphi \circ \gamma$ is monic. Now let φ and ψ be monic equivalent polynomials in $K'[x]$. If $\gamma(x) = bx + c$, then $\gamma^{-1} \circ \varphi \circ \gamma(x)$ has leading term $b^{d-1}x^d$. Thus if $\psi = \gamma^{-1} \circ \varphi \circ \gamma$, then b must be a $(d-1)$th root of unity. ■

2.4 Examples: critically fixed simply ramified polynomials

Postcritically finite polynomials can be classified in terms of certain combinatorial objects called *Hubbard trees*, see [3, 18, 17], as well as [16] for their relationship, in the case of two critical values, to *dessins d'enfant* of genus 0. Instead of describing this classification, in this subsection, we simply want to illustrate that postcritically finite polynomials are in plentiful supply by describing some of the most simple families of examples. In order to avoid rationality questions, in this subsection we assume that $K = \overline{K}$ is algebraically closed. To write down examples, we can make various simplifying assumptions; for example, we can limit the number of critical points (or values). If φ has only one critical point and this point is fixed, we see quickly that φ is conjugate to $x \mapsto x^d$; specializations of this map constitute the classical theory of "pure" extensions. Another family of examples is given by the *Chebyshev polynomials* which have only two critical values; we study the quadratic one $x^2 - 2$ in Section 6. More generally, polynomials with two critical values are called *generalized Chebyshev polynomials* or more commonly *Shabat polynomials*; they have quite a rich structure, as can be seen from the survey of Shabat and Zvonkin [20].

Here we make a different set of simplifying assumptions, and completely classify the resulting postcritically finite dynamical systems for each degree $d > 1$. Namely, we assume that the critical points are fixed and that all the ramification indices are 2; the latter condition is equivalent to requiring that the polynomial has $d - 1$ critical points. Other than $\varphi(x) = x^d$, this is the simplest family of postcritically finite polynomials. It gives simple examples of postcritically finite polynomials not equivalent to any monic polynomial with *integer* coefficients.

Definition 2.4. A polynomial $\varphi \in K[x]$ of degree $d > 1$ is said to be *critically fixed*, *simply ramified* (CFSR) if φ has $d-1$ critical points, each of which is a fixed point for φ.

We note that any conjugate of a CFSR polynomial is also CFSR.

Example 2.5. If K does not have characteristic 2, the polynomial $\varphi(x) = x^2$ has exactly one critical point, $x = 0$, which is a fixed point. Thus φ is a CFSR polynomial. It is easy to see that φ is the unique such polynomial, up to equivalence, of degree 2.

Example 2.6. Let $K = \overline{\mathbb{Q}}$. The polynomial $\varphi(x) = x^3 + (3/2)x$ has derivative $\varphi'(x) = 3x^2 + 3/2$. Thus φ has two critical points $\pm i/\sqrt{2}$. The fixed points of φ are 0 and the two critical points, so φ is a CFSR polynomial.

This polynomial φ gives an example of a monic, post-critically finite polynomial which does not have integral coefficients. Is there a monic polynomial ψ equivalent to φ with integer coefficients? By Lemma 2.3 we only need to consider polynomials of the form

$$\psi(x) = \varphi(x + c) - c \qquad \text{or} \qquad \psi(x) = -\varphi(-x + c) + c. \tag{2.6}$$

In the first case,

$$\psi(x) = (x + c)^3 + \frac{3}{2}(x + c) - c = x^3 + 3cx^2 + \left(3c^2 + \frac{3}{2}\right)x + \left(c^3 + \frac{1}{2}c\right). \tag{2.7}$$

Let ν be a place (valuation) in $\mathbb{Q}(c)$ above 2 normalized so that $\nu(2) = 1$. We want to find c so that the coefficients are integral. So, $\nu(3c^2 + 3/2) \geq 0$. This implies $\nu(c) = -1/2$. Thus the coefficient of x^2 is not 2-integral. A similar argument applies to the second case. We conclude that there are no monic polynomials with integral coefficients equivalent to φ.

This gives an example of a post-critically finite polynomial not equivalent to any monic polynomial with integral coefficients.

We will now assume that K has characteristic 0 (we already assumed it is algebraically closed). Thus, up to equivalence, CFSR polynomials can be taken to be monic. In an effort to normalize further, consider the roots of the fixed point polynomial $\varphi(x) - x$. These include all $d-1$ critical points (roots of φ'), but the polynomial is of degree d. Thus there is a dth root r; here, we allow r to be one of the $d-1$ critical points if $\varphi(x) - x$ has a double root. After conjugating by a translation γ, we can assume that $r = 0$. In particular, $\varphi(x) - x = d^{-1}x\varphi'(x)$. Conversely, suppose $\varphi \in K[x]$ is such that $\varphi(x) - x = d^{-1}x\varphi'(x)$.

Then it is easy to see that neither $\varphi'(x)$ nor $\varphi(x) - x$ has multiple roots (differentiate $\varphi(x) - x = d^{-1}x\varphi'(x)$ and substitute $x = r$, where r is any root of $\varphi'(x)$, to see that $\varphi''(r) \neq 0$ and $r \neq 0$). In particular, $\varphi(x)$ is a CFSR polynomial. These observations motivate the following.

Definition 2.7. A *normalized CFSR polynomial* $\varphi \in K[x]$ is a monic polynomial with $\varphi(x) - x = d^{-1}x\varphi'(x)$.

The above argument gives the following.

Lemma 2.8. If K is algebraically closed, then every CFSR polynomial is equivalent to a normalized CFSR polynomial. □

Next, we will show that over an algebraically closed field, there is, up to equivalence, a unique CFSR polynomial of each degree.

Assume $\varphi \in F[x]$ is a normalized CFSR polynomial of degree d. We rewrite $\varphi(x) - x = d^{-1}x\varphi'(x)$ as

$$\varphi(x) = x + d^{-1}x\varphi'(x). \tag{2.8}$$

By differentiating this equation we get $\varphi'(x) = 1 + d^{-1}\varphi'(x) + d^{-1}x\varphi''(x)$, so

$$\varphi' = \frac{d + x\varphi''(x)}{d-1}, \qquad \varphi = x + d^{-1}x\left(\frac{d + x\varphi''(x)}{d-1}\right) = \frac{d}{d-1}x + \frac{1}{d(d-1)}x^2\varphi''(x). \tag{2.9}$$

Differentiating the first of these gives $\varphi''(x) = (1/(d-1))(\varphi''(x) + x\varphi'''(x))$. So if $d > 2$, $\varphi''(x) = (1/(d-2))x\varphi'''(x)$. Thus

$$\varphi(x) = \frac{d}{d-1}x + \frac{1}{d(d-1)}x^2\left(\frac{1}{d-2}x\varphi'''(x)\right) = \frac{d}{d-1}x + \frac{(d-3)!}{d!}x^3\varphi'''(x). \tag{2.10}$$

Continuing in this manner, we get that the nth derivative $\varphi^{(n)}(x)$ is $(1/(d-n))x\varphi^{(n+1)}(x)$ if $n \leq d$. So, for $n \leq d$,

$$\varphi = \frac{d}{d-1}x + \frac{(d-n)!}{d!}x^n\varphi^{(n)}(x). \tag{2.11}$$

In particular, if $n = d$, then

$$\varphi(x) = \frac{d}{d-1}x + \frac{1}{d!}x^d\varphi^{(d)}(x) = \frac{d}{d-1}x + x^d. \tag{2.12}$$

This gives uniqueness. Existence follows from the fact that $\varphi(x) = (d/(d-1))x + x^d$ satisfies the equation $\varphi(x) - x = d^{-1}x\varphi'(x)$ and so is a normalized CFSR polynomial.

Proposition 2.9. The polynomial $(d/(d-1))x + x^d$ is the unique normalized CFSR polynomial of degree d. □

Remark 2.10. By Proposition 2.9, all CFSR polynomials over the complex numbers are equivalent to a monic polynomial with algebraic coefficients and the same is true for all critically fixed polynomials by a theorem of Tischler [23] (see Pakovich [15] for more on critically fixed polynomials). In fact, any post-critically finite rational function over the complex numbers is equivalent to one with algebraic coefficients (see [6, Theorem 3.17]).

(We are grateful to Pilgrim for the latter remark.)

3 Discriminant formulae

In this section, we prove Theorem 1.1 by giving an explicit formula in terms of branch points for the discriminant of $\Phi_n(x,t)$. We continue to assume that K is a number field; however, Propositions 3.1 and 3.2 are true for general K as long as the degrees (δ and d) are not divisible by the characteristic of K. Recall the formula

$$\operatorname{Res}(P,R) = (-1)^{\deg P \deg R}\operatorname{Res}(R,P) = (-1)^{\deg P \deg R}l(R)^{\deg P}\prod_j P(\theta_j), \tag{3.1}$$

for the resultant of two polynomials P, R in x, where $R = l(R)\prod_j(x-\theta_j)$. Also, for the discriminant of P, we have

$$\operatorname{disc}(P) = (-1)^{d(d-1)/2}l(P)^{-1}\operatorname{Res}(P,P'), \tag{3.2}$$

where $d = \deg P$. See, for example, Lang [13, Chapter V, Section 10].

Proposition 3.1. For $\psi \in K[x]$ of degree δ with leading coefficient $l(\psi) = \alpha$,

$$\operatorname{disc}_x\big(\psi(x) - t\big) = (-1)^{(\delta-1)(\delta-2)/2}\delta^\delta\alpha^{\delta-1}\prod_{\beta\in\mathcal{B}_\psi}(t-\beta)^{M_\beta(\psi)}. \tag{3.3}$$

□

Proof. By (3.2) and then (3.1), we have

$$\begin{aligned}
\operatorname{disc}_x\big(\psi(x)-t\big) &= (-1)^{\delta(\delta-1)/2}\alpha^{-1}\operatorname{Res}_x\big(\psi(x)-t,\psi'(x)\big)\\
&= (-1)^{\delta(\delta-1)/2}\alpha^{-1}\operatorname{Res}_x\left(\psi(x)-t,\delta\alpha\prod_{r\in\mathcal{R}_\psi}(x-r)^{m_r(\psi)}\right)\\
&= (-1)^{\delta(\delta-1)/2}\alpha^{-1}(-1)^{\delta(\delta-1)}(\delta\alpha)^{\delta}\prod_{r\in\mathcal{R}_\psi}\big(\psi(r)-t\big)^{m_r(\psi)} \qquad (3.4)\\
&= (-1)^{\delta(\delta-1)/2}(-1)^{\delta(\delta-1)}(-1)^{\delta-1}\delta^{\delta}\alpha^{\delta-1}\prod_{r\in\mathcal{R}_\psi}\big(t-\psi(r)\big)^{m_r(\psi)}\\
&= (-1)^{(\delta-1)(\delta-2)/2}\delta^{\delta}\alpha^{\delta-1}\prod_{\beta\in\mathcal{B}_\psi}(t-\beta)^{M_\beta(\psi)}.
\end{aligned}$$

■

Proposition 3.2. For $\varphi\in K[x]$ of degree d with $l(\varphi)=a$, and $n\geq 1$,

$$\operatorname{disc}_x\big(\Phi_n\big) = (-1)^{(d^n-1)(d^n-2)/2}d^{nd^n}a^{(d^n-1)^2/(d-1)}\prod_{\beta\in\mathcal{B}_{\varphi^{\circ n}}}(t-\beta)^{M_\beta(\varphi^{\circ n})}. \qquad (3.5)$$

□

Proof. We apply Proposition 3.1 with $\psi=\varphi^{\circ n}$, noting that $\deg\psi=d^n$ and $l(\psi)=a^{(d^n-1)/(d-1)}$. ■

Definition 3.3. Let v be a place of K. A polynomial $\varphi\in K[x]$ has *good reduction* at v if every coefficient of φ has nonnegative v-valuation and the leading coefficient of φ has zero v-valuation. In other words, φ has good reduction when it is v-integral with v-unital leading coefficient. Obviously, if φ has good reduction at v, then so does each iterate $\varphi^{\circ n}$. Also note that if a polynomial has good reduction at v, then the roots of φ are v-integral in the sense that they have nonnegative valuation (for extensions of v to the splitting field of φ).

A basic result of algebraic number theory is the following.

Lemma 3.4. Let $K(\alpha)$ be an extension of K generated by a root of a polynomial $f\in K[x]$ where $\operatorname{disc} f\neq 0$ (but not necessarily irreducible). If f has good reduction at a place v of K, then $v(\operatorname{disc}K(\alpha)/K)\leq v(\operatorname{disc} f)$. □

Definition 3.5. Let $\varphi\in K[x]$ be a polynomial of degree d with leading coefficient $l(\varphi)=a$, v a place of K, and $t_0\in K\setminus\mathcal{P}_\varphi$ an element outside the postcritical set. The pair (v,t_0) is called φ-*exceptional* if either (i) φ has bad reduction at v, (ii) $v(t_0)<0$, (iii) $v(d)>0$, or (iv) $v(\operatorname{Norm}_{K'/K}(t_0-\nu))\neq 0$ for some $\nu\in\mathcal{P}_\varphi$ where K' is the extension of K generated by $\mathcal{P}_\varphi$. Define S_{φ,t_0} to be the set of real infinite places of K together with finite places v

such that (v, t_0) is φ-exceptional. Observe that S_{φ,t_0} is a finite set if φ is postcritically finite.

We now state and prove the following version of Theorem 1.1.

Theorem 3.6. Let $\varphi \in K[x]$ be a postcritically finite polynomial of degree d where K is a number field, and let $t_0 \in K$ be outside the postcritical set $\mathcal{P}_\varphi$. Then $K_{\varphi,t_0}/K$, and hence $\mathcal{K}_{\varphi,t_0}/K$, are unramified outside the set S_{φ,t_0}. □

Proof. Let v be a finite place of $\mathcal{O}_K$ outside S_{φ,t_0}. It is enough to show that $v(\operatorname{disc} K_{n,t_0}/K) = 0$ for general n. Since v is outside S_{φ,t_0}, the polynomial $\Phi_n(x, t_0)$ has good reduction at v. By Lemma 3.4, $v(\operatorname{disc} K_{n,t_0}/K) \le v(\operatorname{disc}_x \Phi_n(x, t_0))$, so it is enough to show that $v(\operatorname{disc}_x \Phi_n(x, t_0)) = 0$.

By the discriminant formula (3.2) and the matrix definition of resultant, the discriminant $\operatorname{disc}_x \Phi_n(x, t_0)$ is obtained by evaluating the t-polynomial $\operatorname{disc}_x \Phi_n(x, t)$ at $t = t_0$. So by Proposition 3.2,

$$\operatorname{disc}_x \Phi_n(x, t_0) = (-1)^{(d^n-1)(d^n-2)/2} d^{nd^n} a^{(d^n-1)^2/(d-1)} \prod_{\beta \in \mathcal{B}_{\varphi^{\circ n}}} (t_0 - \beta)^{M_\beta(\varphi^{\circ n})}. \tag{3.6}$$

Now extend v to a valuation v' of the extension K' of K generated by the ramification points of $\varphi^{\circ n}$. Since $\Phi_n(x, t_0)$ has good reduction at v, and $v(d) = 0$, it follows that its derivative, $(\varphi^{\circ n})'$, also has good reduction. So each ramification point r of $\varphi^{\circ n}$ has nonnegative v'-valuation. Thus the corresponding branch point $\beta = \varphi^{\circ n}(r)$ also has nonnegative v'-valuation. So, for each branch point β, the element $t_0 - \beta \in K'$ and its conjugates over K have nonnegative v'-valuation. Since v is outside S_{φ,t_0}, the norm of each such $t_0 - \beta$ has zero v-valuation, so $v'(t_0 - \beta) = 0$. In addition, $v(d) = v(a) = 0$ since v is outside S_{φ,t_0}. Thus $v(\operatorname{disc}_x \Phi_n(x, t_0)) = 0$. ■

Corollary 3.7. Let $\varphi \in K[x]$ be a postcritically finite polynomial of degree $d > 1$ where K is a number field. For $t_0 \in K \setminus \mathcal{P}_\varphi$, the action of $\operatorname{Gal}(\overline{K}/K)$ on $\mathcal{K}_{\varphi,t_0}$ induces an iterated monodromy representation $\rho_{\varphi,t_0} : G_{K,S} \twoheadrightarrow \mathcal{M}_{\varphi,t_0}$, where $S = S_{\varphi,t_0}$. □

4 Polynomials with good reduction

We are interested in the ramification behavior of $K_{n,t_0}/K$, and hence the valuation of $\operatorname{disc}(K_{n,t_0}/K)$, especially for places of K of residual characteristic dividing the degree d of φ. As in Lemma 3.4, if $\Phi_n(x, t_0)$ has good reduction at v, then the v-adic behavior of $\operatorname{disc}(\Phi_n(x, t_0))$ gives bounds, often sharp, for the v-adic behavior of $\operatorname{disc}(K_{n,t_0}/K)$.

Our aim here is to prove Theorem 1.2. Throughout this section, we suppose K is a characteristic 0 field equipped with an ultrametric valuation v having valuation ring $\mathcal{O}_v = \{\alpha \in K : v(\alpha) \geq 0\}$; we assume that $v(K^\times) = \mathbb{Z}$. The residue field of K with respect to v is denoted k_v. We assume that k_v has positive characteristic $p > 0$.

Lemma 4.1. Suppose K' is an algebraic extension of K and fix an extension v' of v to K'. Let $\varphi \in K[x]$ be a polynomial of degree $d \geq 2$ with good reduction at v. If $\alpha \in K'$ has $v'(\alpha) < 0$, then α is not preperiodic for φ. □

Proof. Suppose $\beta \in K'$ has $v'(\beta) < 0$. Since the leading coefficient of φ is a v-adic unit, there is a unique term in the sum $\varphi(\beta) = \sum_{j=0}^{d} a_j \beta^j$ with minimal valuation, namely $a_d \beta^d$. Since v' is ultrametric, we have $v'(\varphi(\beta)) = d \cdot v'(\beta) < v'(\beta)$. Applying this principle to $\alpha, \varphi(\alpha), \varphi^{\circ 2}(\alpha), \ldots$, we obtain $v'(\varphi^{\circ n}(\alpha)) = d^n v'(\alpha) \to -\infty$. Thus, the set $\{\varphi^{\circ n}(\alpha)\}$ cannot be finite since $\{v'(\varphi^{\circ n}(\alpha))\}$ is not finite. ■

Definition 4.2. For $f \in K[x]$, put $\mathrm{rd}_v(f) = (1/\deg f) v(\operatorname{disc} f)$ for the v-*root discriminant* of f.

We now state and prove the following version of Theorem 1.2.

Theorem 4.3. Let $\varphi \in K[x]$ be a postcritically finite polynomial of degree $d \geq 2$ with good reduction at v, and let $t_0 \in \mathcal{O}_v$. Then, for $n \geq 1$,

$$n v(d) \leq \mathrm{rd}_v\left(\Phi_n(x, t_0)\right) \leq n v(d) + \sum_{\nu \in \mathcal{P}_\varphi} v'(t_0 - \nu), \tag{4.1}$$

where v' is the extension of v to K', the field obtained by adjoining the elements of the postcritical set $\mathcal{P}_\varphi$ to K. In particular, the v-root discriminant of $\Phi_n(x, t_0)$ is bounded as n goes to infinity if and only if the residual characteristic p of v does not divide d. □

Proof. Proposition 3.2 yields the following:

$$\mathrm{rd}_v\left(\Phi_n(x, t_0)\right) = n v(d) + \sum_{\beta \in \mathcal{B}_{\varphi^{\circ n}}} \frac{M_\beta}{d^n} v'(t_0 - \beta). \tag{4.2}$$

By Lemma 4.1, $v'(t_0 - \beta) \geq 0$. The result now follows since $M_\beta = M_\beta(\varphi^{\circ n}) < d^n$. ■

Example 4.4. It is not difficult to write down polynomials $\varphi \in \mathbb{Z}[x]$ such that there is no wild ramification in the iterated tower of φ. If a strengthening of Theorem 1.2 for field discriminants (as opposed to polynomial discriminants) holds, then such a polynomial, if monic, will not be postcritically finite, so the resulting iterated tower of function fields will be infinitely ramified. Here is a quadratic example. Let $\varphi(x) = x^2 + x + \mu$ with $\mu \in \mathbb{Z}$. Then $\operatorname{disc}_x(\Phi_n(x, t))$ is *odd* for all $t \in \mathbb{Z}$ (for instance by Proposition 3.2). However, φ is

not postcritically finite. Indeed, its only critical point is $r = -1/2$. For $v = \mathrm{ord}_2$, the 2-adic valuation of $\mathbb{Z}$, $v(r) = -1$ is negative, hence by Lemma 4.1, φ is not postcritically finite.

5 Prime decomposition in towers

In this section, K is a number field. We now describe, in terms of certain graphs, how primes of K not dividing the discriminant of $\Phi_n(x, t_0)$ (assumed to be irreducible) decompose when we adjoin a root of this polynomial. A simple consequence of this description is that no finite prime of K splits completely in $K_{\varphi,t_0}/K$.

We first set up some notation. We assume $\varphi \in \mathcal{O}_K[x]$ is postcritically finite. Recall the notation from Section 1 regarding $F_n = F(\xi_n)$. Fixing $t_0 \in \mathcal{O}_K$, we assume that $\Phi_n(x, t_0)$ is irreducible over K for all $n \geq 1$ and choose a coherent system $(\xi_n|_{t_0})$ of their roots so that $K_{n,t_0} = K(\xi_n|_{t_0})$. For the rest of this section, we assume $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ which is not in S_{φ,t_0} (see Definition 3.5). For such $\mathfrak{p}$, the splitting of $\mathfrak{p}$ in the ring of integers of K_{n,t_0} coincides with the splitting of $\mathfrak{p}$ in the ring $\mathcal{O}_K[\xi_n|_{t_0}]$; the latter factorization mirrors exactly the factorization of the polynomial $\Phi_n(x, t_0)$ over the residue field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$.

For example, the primes of degree 1 in $\mathcal{O}_K[\xi_n|_{t_0}]$ which lie over $\mathfrak{p}$ correspond to the roots of $\varphi^{\circ n}(x) - t_0$ over $\mathbb{F}_\mathfrak{p}$, that is, the points in $\mathbb{F}_\mathfrak{p}$ whose image under the nth iterate of φ is the image $\overline{t}_0$ of t_0 in $\mathbb{F}_\mathfrak{p}$. A prime of degree k lying over $\mathfrak{p}$ corresponds to a Galois orbit of k points defined over a degree k extension of $\mathbb{F}_\mathfrak{p}$ mapping to $\overline{t}_0$ by $\varphi^{\circ n}$. Such data is conveniently summarized in terms of certain directed graphs we now define.

For $k \geq 1$, let $\mathbb{F}_{\mathfrak{p},k}$ be a degree k extension of the residue field $\mathbb{F}_\mathfrak{p}$. We denote by $\Gamma_{\varphi,\mathfrak{p},k}$ the following directed graph: the vertices are the elements of $\mathbb{F}_{\mathfrak{p},k}$ and the graph has a directed edge $v \to w$ if and only if $\varphi(v) = w$. After we choose an ordering $\lambda_1, \ldots, \lambda_q$ of the elements of $\mathbb{F}_{\mathfrak{p},k}$, the adjacency matrix $A_{\varphi,\mathfrak{p},k}$ of $\Gamma_{\varphi,\mathfrak{p},k}$ has ij entry 1 if $\varphi(\lambda_i) = \lambda_j$ and 0 otherwise. We write $\Gamma_{\varphi,\mathfrak{p}}$, $A_{\varphi,\mathfrak{p}}$ for $\Gamma_{\varphi,\mathfrak{p},1}$ and $A_{\varphi,\mathfrak{p},1}$.

For calculations, it is useful to note that $A_{\varphi^{\circ n},\mathfrak{p},k} = A^n_{\varphi,\mathfrak{p},k}$. In other words, the in-degree of a vertex v in $\Gamma_{\varphi^{\circ n},\mathfrak{p},k}$ is the number of length n paths on $\Gamma_{\varphi,\mathfrak{p},k}$ ending at v. For example, let $\overline{t}_0 = t_0 + \mathfrak{p}$ be the vertex corresponding to the reduction of t_0 modulo $\mathfrak{p}$. Then the following quantities all coincide:

(a) the number of degree 1 primes of $\mathcal{O}_K[\xi_n|_{t_0}]$ over $\mathfrak{p}$,

(b) the in-degree of $\overline{t}_0$ on $\Gamma_{\varphi^{\circ n},\mathfrak{p}}$,

(c) the sum of the entries in the column of $A^n_{\varphi,\mathfrak{p}}$ corresponding to $\overline{t}_0$,

(d) the number of length n paths on $\Gamma_{\varphi,\mathfrak{p}}$ ending at $\overline{t}_0$.

Note that, by (c), for example, there are at most $|\mathbb{F}_\mathfrak{p}| = \mathbb{N}\mathfrak{p}$ degree 1 primes of K_{n,t_0} lying over $\mathfrak{p}$, hence $\mathfrak{p}$ does not split completely in $K_{\varphi,t_0}/K$.

More generally, we can count the number of primes of any given degree over $\mathfrak{p}$ by taking into account the action of $\mathrm{Gal}(\overline{\mathbb{F}}_\mathfrak{p}/\mathbb{F}_\mathfrak{p})$. Namely, the graph $\Gamma_{\varphi,\mathfrak{p},k}$ has the following additional structure: each vertex is "colored," we will say *weighted*, by a positive divisor m of k where m is the exact degree of that vertex over $\mathbb{F}_\mathfrak{p}$. Furthermore, every directed edge has the property that the weight of the initial vertex is a multiple of the weight of the terminal vertex. Also $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p},k}/\mathbb{F}_\mathfrak{p})$ acts on the graph and the weight of a vertex equals the size of its orbit under this action.

Summarizing the discussion, we have the following proposition describing prime decomposition in $K_{n,t_0}/K$ in terms of graphs.

Proposition 5.1. Suppose $\varphi \in \mathcal{O}_K[x]$ is postcritically finite and that $t_0 \in \mathcal{O}_K$ is such that $\Phi_n(x, t_0)$ is irreducible over K for all $n \geq 1$. Suppose $\mathfrak{p} \subset \mathcal{O}_K$ is not in S_{φ,t_0}. Then, for $k \geq 1$, the number of degree k primes of K_{n,t_0} lying over $\mathfrak{p}$ is N/k, where N is the number of paths of length k on $\Gamma_{\varphi,\mathfrak{p},k}$ which start with a vertex of weight k and end at $\overline{t}_0$, the weight 1 vertex corresponding to the image of t_0 in $\mathbb{F}_\mathfrak{p}$. □

Remark 5.2. Alternatively, one could take the quotient graph of $\Gamma_{\varphi,\mathfrak{p},k}$ by identifying vertices which are in the same orbit of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p},k}/\mathbb{F}_\mathfrak{p})$, and give a vertex in the new graph the weight equal to the number of points identified. Then the degree k primes of K_{n,t_0} lying over $\mathfrak{p}$ are in bijective correspondence with the paths of length n on the quotient graph starting with a vertex of weight k and ending at $\overline{t}_0$. We should note that as long as $\mathfrak{p} \notin S_{\varphi,t_0}$, the decomposition of $\mathfrak{p}$ in K_{n,t_0} depends only on the residue of t_0 modulo $\mathfrak{p}$.

For a fixed pair $(\mathfrak{p}, k)$ and n tending to infinity, each graph $\Gamma_{\varphi^{\circ n},\mathfrak{p},k}$ has $\mathbb{N}\mathfrak{p}^k$ vertices and an equal number of edges, hence is one of a finite number of graphs. Therefore, the sequence $\Gamma_{\varphi^{\circ n},\mathfrak{p},k}$, $n = 1, 2, \ldots$ is always eventually periodic. In fact, it is relatively simple to describe exactly what happens to the sequence of graphs in our situation. Each connected component of $\Gamma_{\varphi,\mathfrak{p},k}$ consists of a unique cycle or "loop" with a number of "arms" emanating from it. The minimal period of the sequence $(\Gamma_{\varphi^{\circ n},\mathfrak{p},k})$ is the lowest common multiple of the length of the unique loop in each connected component of $\Gamma_{\varphi,\mathfrak{p},k}$ and the preperiod is the least common multiple of the length of the longest arm in each connected component of $\Gamma_{\varphi,\mathfrak{p},k}$. All of these facts are easily verified and left as amusing exercises for the reader. A highly interesting question is whether one can capture the graph-theoretical description of prime decomposition in iterated extensions via appropriate zeta and L-functions. Here, we settle for a typical example as an illustration.

Example 5.3. Let $\varphi(x) = x^2 + i \in \mathbb{Z}[i]$. Let $\mathfrak{p} = (3 + 2i)$ be a prime of norm 13. We map $\mathbb{Z}[i] \to \mathbb{F}_\mathfrak{p} \simeq \mathbb{F}_{13}$ by sending $i \mapsto 8$, and list the elements of $\mathbb{F}_{13}$ as $0, 1, 2, \ldots, 12$. We write

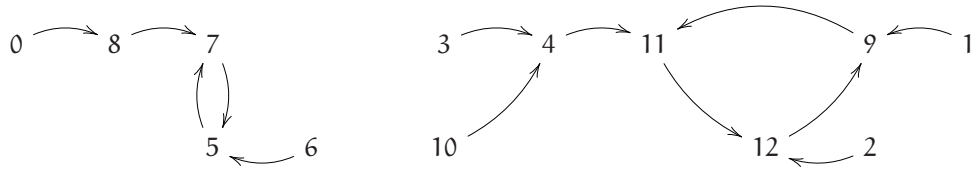

Figure 5.1 The graph $\Gamma_{\varphi,\mathfrak{p}}$.

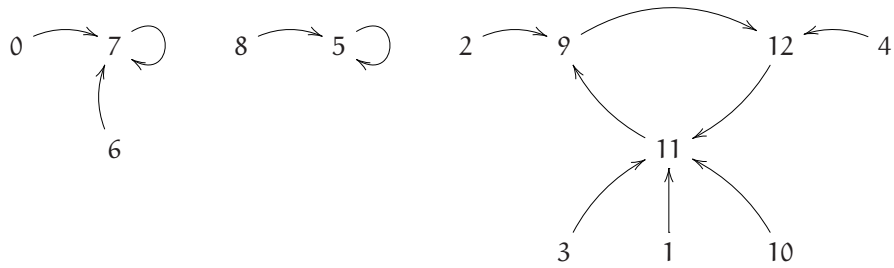

Figure 5.2 The graph $\Gamma_{\varphi^{\circ 2},\mathfrak{p}}$.

down the adjacency matrix $A_{\varphi,\mathfrak{p}}$:

$$A_{\varphi,\mathfrak{p}} = \begin{pmatrix} 0&0&0&0&0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&1&0\\ 0&0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0&0&0&1&0&0&0 \end{pmatrix}. \tag{5.1}$$

The graphs for φ and $\varphi^{\circ 2}$ are drawn in Figures 5.1 and 5.2, respectively.

Note that $\Gamma_{\varphi,\mathfrak{p}}$ has two connected components, one with a loop of length 2 and the other with a loop of length 3. The longest arm in each component has length 2. The reader can check either by taking powers of the adjacency matrix or by drawing the graphs that

Table 5.1

n	Degrees of irreducible factors of $\varphi^{\circ n}(x) - 11/\mathbb{F}_{13}$	Number of degree 1 factors
1	1; 1	2
2	1; 1; 1; 1	4
3	1; 1; 2; 2; 2	2
4	1; 1; 2; 2; 2; 2; 2; 4	2
5	1; 1; 1; 1; 2; 2; 2; 2; 4; 4; 4; 4; 4	4
6	1; 1; 2; 2; 2; 2; 2; 2; 2; 2; 4; 4; 4; 4; 4; 4; 8; 8; 8	2
7	1; 1; 2; 2; 2; 2; 2; 2; 2; 2; 2; 2; 4; 4; 4; 4; 4; 4; 4; 4; 4; 8; 8; 8; 8; 8; 8; 8; 8; 8	2

$\Gamma_{\varphi,\mathfrak{p}}$ occurs only once in the sequence $\Gamma_{\varphi^{\circ n},\mathfrak{p}}$, but starting with $n = 2$, the sequence has period 6. Note that 6 is the product of the lengths of the loops in the connected components of $\Gamma_{\varphi,\mathfrak{p}}$. With base field $K = \mathbb{F}_{\mathfrak{p}}$, the number of degree 1 places in F_n over the prime $(t - 11)$ for $n = 1, 2, 3, \ldots$ is the periodic sequence $2, 4, 2, 2, 4, 2, \ldots$ of period 3. As a check on the calculations, we verified using GP-PARI that with $\varphi(x) = x^2 + 8$, the polynomials $\varphi^{\circ n}(x) - 11$ for $n = 1, 2, \ldots, 7$, factor over $\mathbb{F}_{13}$ into distinct irreducible factors of the degrees listed in Table 5.1.

6 Quadratic polynomials

In this section, we make a few remarks and give some examples concerning quadratic polynomials. By applying automorphisms of $\mathbb{P}^1$, we bring each quadratic polynomial to a standard form $\varphi(x) = x^2 - r$. We then write down recurrence conditions for postcriticality of φ. The minimal number fields over which preperiodic points of prescribed preperiod m and period n for such quadratic polynomials are defined form an interesting family of number fields in their own right.

6.1 Normal form

Put

$$\varphi(x) = ax^2 + bx + c \in K[x]. \tag{6.1}$$

Let $\delta_\varphi = -b^2/(4a) + c$. It is the unique branch point for the cover of $\mathbb{P}^1$ given by the polynomial $\varphi(x)$, that is, $\mathcal{B}_\varphi = \{\delta_\varphi\}$. Theorem 1.1 now simplifies as follows: $\mathcal{F}_\varphi/F$ is finitely ramified if and only if δ_φ is preperiodic for φ.

If $\psi(x) = ax^2 + bx + c$ is quadratic, we take $\gamma(x) = x/a$, so that $\gamma^{-1}(x) = ax$. We then have that

$$\gamma^{-1}\psi\gamma(x) = x^2 + bx + ac \tag{6.2}$$

is monic. Note that γ fixes 0. Since an isomorphism from φ to ψ carries $\mathcal{B}_\varphi$ to $\mathcal{B}_\psi$, applying a K-automorphism taking δ_φ to 0, we see that ψ is conjugate to φ, where

$$\varphi(x) = \left(x + \frac{b}{2}\right)^2. \tag{6.3}$$

We leave to the reader the exercise that for each quadratic $\psi \in K[x]$, there is a unique $r \in \overline{K}$ such that ψ is conjugate to $(x-r)^2$. Note that via the automorphism $\gamma(x) = x + r$, the maps $x^2 - r$ and $(x-r)^2$ are K-isomorphic.

Now consider a normalized quadratic polynomial $\varphi(x) = x^2 - r$. We have

$$\begin{aligned} &\varphi^{\circ 0}(0) = 0, \qquad \varphi^{\circ 1}(0) = -r, \\ &\varphi^{\circ 2}(0) = r(r-1), \qquad \varphi^{\circ 3}(0) = r\left(r^3 - 2r^2 + r - 1\right), \ldots. \end{aligned} \tag{6.4}$$

For $n \geq 0$, consider the recurrence $g_{n+1} = rg_n^2 - 1$ with initial condition $g_0 = 0$. Then φ is postcritically finite if and only if r is a root of $g_m - g_n$ for some $m \neq n$.

Exercises. (i) If $r \in \mathbb{Z}$ and $\varphi(x) = (x-r)^2$ has periodic branch points, then $r \in \{0, 1, 2\}$.

(ii) If $\varphi(x) = ax^2 + bx + c \in \overline{\mathbb{Q}}[x]$ has preperiodic branch point, then $b/2$ is an algebraic integer.

6.2 The polynomial $\varphi(x) = x^2 - 2$

In this subsection, we turn to an example which was the starting point of this paper. We learned from Lemmermeyer the classical fact that the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$ can be written as $\mathbb{Q}(\theta_n)$, where $\theta_n = \sqrt{2 + \sqrt{2 + \cdots + \sqrt{2}}}$. Indeed, using the half-angle formula for cosines, one easily establishes that the nested square root expression given above evaluates $2\cos(\pi/2^{n+1})$. What attracted our attention here was that in the resulting recurrence-tower, the number of ramified primes is finite (indeed only 2 ramifies, and it does so totally and deeply). Since the θ_n are roots of the nth-iterate equation $\Phi_n(x, 0) = \varphi^{\circ n}(x) - 0$, where $\varphi(x) = x^2 - 2$, it was natural to wonder whether for every

$t \in K = \mathbb{Q}$, $\varphi^{\circ n}(x) - t = 0$ cuts out a finitely ramified tower. That this is so is guaranteed by Theorem 1.1 since $x^2 - 2$ is postcritically finite. Indeed, it is the first member of the Chebyshev family of postcritically finite polynomials. For more details see [1, Proposition 5.6] where the iterated monodromy group of any Chebyshev polynomial of degree $d > 1$ is shown to be infinite dihedral.

For the rest of this subsection, let $\varphi(x) = x^2 - 2$. Here we will verify that another property of the cyclotomic $\mathbb{Z}_2$-tower (the specialization of the tower at $t = 0$) holds for many values of $t_0 \in \mathbb{Z}$, namely that a root of $\Phi_n(x, t_0)$ generates over $\mathbb{Z}$ the ring of integers of the number field it cuts out.

Lemma 6.1. For $t_0 \in \mathbb{Z}$, $t_0 \equiv 0, 1 \bmod 4$, the polynomial $\varphi^{\circ n}(x) - t_0$ is irreducible over $\mathbb{Q}$. □

Proof. We note that $\varphi^{\circ n}(0) = -2$, $\varphi^{\circ n}(\pm 1) = -1$. If $t_0 \equiv 0 \bmod 4$, we apply the Eisenstein criterion to $\varphi^{\circ n}(x)$ at the prime 2. If $t_0 \equiv 1 \bmod 4$, we use $\varphi^{\circ n}(x + 1)$ instead. ■

Proposition 6.2. If $t_0 \in \mathbb{Z}$ is congruent to 0, 1 modulo 4, and if $t_0 + 2$ and $t_0 - 2$ are square-free, then for $n \geq 1$, the stem field $K_n = \mathbb{Q}[x]/(\Phi_n(x, t_0))$ of the polynomial $\Phi_n(x, t_0) = \varphi^{\circ n}(x) - t_0$ is monogène, as $\operatorname{disc} K_n = \operatorname{disc} \Phi_n(x, t_0)$. □

Proof. Letting $D_n = \operatorname{disc}(\Phi_n(x, t_0))$, a simple calculation from Proposition 3.2 gives for $n \geq 1$,

$$D_{n+1} = 4^{2^n} D_n^2 \Phi_n(-2) \tag{6.5}$$

or

$$D_{n+1} = 4^{2^n} D_n^2 (2 - t_0) \tag{6.6}$$

since $\varphi^{\circ n}(\pm 2) = 2$. Also, for $n = 1$, we have $D_1 = 4(t_0 + 2)$.

We need to compare D_n with the discriminant d_n of the ring of integers of K_n. For $n = 1$, we clearly have $d_n = D_n$, since $t_0 + 2$ is square-free. For $n \geq 1$, we now determine the ramification for each extension K_{n+1}/K_n.

We first remark that $K_{n+1} = K_n(\sqrt{\theta_n + 2})$, with $\Phi_n(\theta_n) = 0$. Next we observe that $N_{K_n/\mathbb{Q}}(\theta_n + 2) = \Phi_n(-2, t_0) = \varphi^{\circ n}(-2) - t_0 = 2 - t_0$. Hence, for $n \geq 1$, in the extension K_{n+1}/K_n, only the places dividing $2(2 - t_0)$ are allowed to ramify. We first examine the tame ramification. Suppose l is a prime divisor of $2 - t_0$. Then $2 + t_0 \equiv 4 \bmod l$ and so l is split in $K_1/\mathbb{Q}$. Let l be an odd prime divisor of $t_0 - 2$. Since $N_{K_n/\mathbb{Q}}(\theta_n + 2) = 2 - t_0$, there exists a prime l_n of K_n lying over l which is ramified in K_{n+1}/K_n. In fact, there are two primes over l in K_1. One of them is totally ramified in K_n/K_1. The other is unramified.

Therefore, the valuation $v_{\mathfrak{l}_n}$ at the prime ideal $\mathfrak{l}_n$ of the different of the extension K_{n+1}/K_n is precisely $2-1=1$.

It remains to study the wild ramification. For $n \geq 1$, we put

$$\pi_n = \begin{cases} \theta_n & \text{if } t_0 \equiv 0 (\mathrm{mod}\, 4), \\ 1+\theta_n & \text{if } t_0 \equiv 1 (\mathrm{mod}\, 4). \end{cases} \tag{6.7}$$

We note that 2 is ramified in $K_1/\mathbb{Q}$ and that π_1 is a uniformizer for the unique place $\mathfrak{p}_1$ of K_1 lying over 2. We will proceed by induction. Suppose, for some $n \geq 1$, that 2 is totally ramified in $K_n/\mathbb{Q}$ and that π_n is a uniformizer of the unique place $\mathfrak{p}_n$ of K_n lying over 2. We claim that $1+\pi_n$ is not a square modulo $\pi_n^{2^{n+1}+1}$. To see this, we suppose that $1+\pi_n$ is a square modulo $\pi_n^{2^{n+1}+1}$. Since the residue field is $\mathbb{F}_2$, we get, in the case $t_0 \equiv 1 (\mathrm{mod}\, 4)$,

$$2+\theta_n = 1+\pi_n = \left(1+a\pi_n\right)^2 \left(\mathrm{mod}\, \pi_n^{2^{n+1}}\right), \tag{6.8}$$

with $a \in \mathbb{Z}_2$, which is impossible. Thus, for $t_0 \equiv 1 \bmod 4$, the Kummer theory tells us that K_{n+1}/K_n is ramified at the unique place above 2. For $t_0 \equiv 0 \bmod 4$, the argument is simpler, since, in that case, the valuation of $2+\theta_n$ at π_n is the same as that of θ_n, namely 1. By Kummer theory, K_{n+1}/K_n is ramified at the unique place above 2. In conclusion, $K_{n+1}/\mathbb{Q}$ is totally ramified at 2.

If $t_0 \equiv 0 \bmod 4$, it is clear that θ_{n+1} is a uniformizer of the unique place of K_{n+1} lying over 2. The same holds for $1+\theta_{n+1}$ when $t_0 \equiv 1 \bmod 4$; note that $N_{K_{n+1}/K_n}(1+\theta_{n+1}) = -(\theta_n+1)$. This completes the induction step.

Next, we calculate conductors. Let σ be a generator of the Galois group $\mathrm{Gal}(K_{n+1}/K_n)$. Assume $t_0 \equiv 0 \bmod 4$. Then $\theta_{n+1} = \pi_{n+1}$ and

$$\left(\sqrt{2+\theta_n}\right)^{\sigma-1} - 1 = -2. \tag{6.9}$$

The valuation at $\mathfrak{p}_{n+1}$ of 2 is 2^{n+1}. Hence, the element σ belongs to $G_{2^{n+1}}$, but not to $G_{2^{n+1}+1}$ (we are using the higher ramification groups in the lower numbering). Consequently,

$$v_{\mathfrak{p}_{n+1}}\left(\mathfrak{d}\left(K_{n+1}/K_n\right)\right) = \sum_i \left(\#G_i - 1\right) = 2^{n+1}+1, \tag{6.10}$$

where $v_{\mathfrak{p}_{n+1}}$ is the valuation at $\mathfrak{p}_{n+1}$ and $\mathfrak{d}(K_{n+1}/K_n)$ is the different of the extension K_{n+1}/K_n.

Assume now $t_0 \equiv 1 \bmod 4$. Then $\pi_n = 1 + \theta_n$ and

$$(1+\theta_n)^{\sigma-1} - 1 = \frac{2\theta_{n+1}}{1-\theta_{n+1}}. \tag{6.11}$$

Hence, the element σ belongs to $G_{2^{n+1}-1}$, but not to $G_{2^{n+1}}$. Consequently,

$$v_{\mathfrak{p}_{n+1}}\left(\mathfrak{d}(K_{n+1}/K_n)\right) = \sum_i \left(\#G_i - 1\right) = 2^{n+1}. \tag{6.12}$$

Now we are able to determine the discriminant of $K_n/\mathbb{Q}$. First note that for $t_0 \equiv 0 \bmod 4$, $(t_0-2)/2$ (which is odd) is the tame part of $N_{K_{n+1}/\mathbb{Q}}\mathfrak{d}(K_{n+1}/K_n)$. If $t_0 \equiv 1 \bmod 4$, then $t_0 - 2$ (which is odd) is the tame part of $N_{K_{n+1}/\mathbb{Q}}\mathfrak{d}(K_{n+1}/K_n)$. Thus, we have the recurrence formula

$$\begin{aligned} \pm d_{n+1} &= d_n^2 N_{K_{n+1}/\mathbb{Q}}\mathfrak{d}(K_{n+1}/K_n) \\ &= d_n^2 (t_0-2) 2^{2^{n+1}} \\ &= d_n^2 (t_0-2) 4^{2^n}, \end{aligned} \tag{6.13}$$

which coincides up to sign with the recurrence (6.6) for D_n. We also have the coincidence of initial conditions, $d_1 = D_1$. Since D_n/d_n is a square, we conclude that $d_n = D_n$ for all n, and so $\mathcal{O}_{K_n} = \mathbb{Z}[\theta_n]$. ■

7 Iterated monodromy representations: questions

In this section, we discuss in a bit more detail conjectural and known properties of iterated monodromy representations, especially as compared with those of p-adic representations. We also list a number of open problems.

We first recall a conjecture of Fontaine and Mazur: if K is a number field and S is a finite set of places of K none of which has residue characteristic p, then all finite-dimensional p-adic representations of $G_{K,S}$ factor through a finite quotient (see [10, Conjecture 5a] as well as Kisin and Wortmann [12]). On the other hand, infinite tamely and finitely ramified extensions of number fields do exist (and are in plentiful supply) thanks to the criterion of Golod and Shafarevich, see, for example, Roquette [19]. Thus, at least for certain pairs K, S, there is a sizeable portion of $G_{K,S}$ which is predicted to be invisible to finite-dimensional p-adic representations.

When S contains all places above p, it is also expected, by a conjecture of Boston [5] (which we recall below), that p-adic representations do not capture all of $G_{K,S}$. Suppose $\bar{\rho} : G_{K,S} \to GL_m(\mathbb{F}_p)$ is a residual representation of $G_{K,S}$. By Mazur's theory of

deformations, there exist a universal ring $R(\rho)$ (local, Noetherian, and complete) and a versal deformation $\rho : G_{K,S} \to GL_m(R(\rho))$ such that $\bar{\rho}$ is the restriction of ρ. Let $L = L_{\bar{\rho}}$ be the subfield of K_S fixed by $\ker \bar{\rho}$. We put $H = H_{\bar{\rho}} = \mathrm{Gal}(M/L)$ where M is the maximal pro-p extension of L inside K_S. If S contains all place above p (p odd, or for p even we assume K is totally complex), then the cohomological dimension of H is at most 2. If L is not totally real, the purely group-theoretical Conjecture B of Boston [5] concerning the rank-growth of subgroups of $GL_m(R(\rho))$ then implies the *noninjectivity conjecture* (see [5, page 91]): ρ forgets a nontrivial part of H.

How can one shed light on those sides of arithmetic fundamental groups which are apparently not illuminated by the theory p-adic representations? As a counterpoint to the Fontaine-Mazur conjecture, a conjecture of Boston [4] asserts that infinite tame quotients of $G_{K,S}$ possess faithful actions on rooted trees. Iterated monodromy groups are canonically equipped with such an action [14]. It is therefore natural to seek such representations via specializations of iterated towers of postcritically finite polynomials, in the wild case as well as in the tame case. In the wild case, it would be interesting to produce iterated monodromy representations whose image does not have any infinite p-adic analytic quotients. Since very little is known about the structure of infinite tamely and finitely ramified extensions of number fields, the following question is of particular interest.

Question 7.1. Are there a number field K and a rational function φ on $\mathbb{P}^1/K$ of degree $d > 1$ as well as a specialization at $t_0 \in K$ of (1.1) such that

(i) for each $n \geq 1$, $\Phi_n(x, t_0)$ is irreducible over K (i.e., $K_{n,t_0} = K(\xi_n|_{t_0})$ is a field of degree d^n over K),

(ii) there is a finite set S of places of K such that $K_{n,t_0}/K$ is unramified outside S for all $n \geq 1$, and such that

(iii) S does not contain any primes dividing d?

By Theorem 1.1, it is possible to fulfill (ii) by taking φ to be a postcritically finite polynomial. Satisfying (i) is not too difficult either, since we can arrange a place of K to ramify totally in K_n (essentially an Eisenstein condition, see, e.g., Lemma 6.1). Condition (iii) asks that K_φ/K be *tamely ramified*. It is not difficult to arrange (i) and (iii) simultaneously by imposing congruence conditions (e.g., see Example 5.3). However, satisfying all conditions together appears to be quite difficult.

A positive answer to Question 7.1 would provide, for the first time, an explicit step-by-step method for constructing an infinite tamely and finitely ramified extension of a number field. The only method for producing such towers, the Golod-Shafarevich criterion, is effective but not constructive. On the other hand, a negative answer would

assert that an analogue of the Fontaine-Mazur conjecture holds for finitely ramified iterated extensions. We should mention that for the function field of a curve over a finite field with a square number of elements, recursive constructions of Garcia-Stichtenoth (see, e.g., [11]) for tamely and finitely ramified extensions exist; that such constructions always arise from modular curves is a conjecture of Elkies [9].

The root discriminant of a number field of degree n over $\mathbb{Q}$ is the nth root of the absolute value of its discriminant. Recall that an algebraic extension L over a number field K is called *asymptotically good* if (i) L/K is infinite, and (ii) for every sequence of distinct intermediate subfields of L/K, the root discriminant remains bounded. A more general and more concise version of Question 7.1 is the following.

Question 7.2. Are there a rational function φ on $\mathbb{P}^1$ defined over a number field K, and a $t_0 \in K$ such that the resulting specialized iterated tower $K_{\varphi,t_0}/K$ is asymptotically good?

Under the assumption of good reduction of the polynomial φ, the analogue of this question where we replace the number field discriminant with the polynomial discriminant, has a negative answer by Theorem 1.2. Namely, for a polynomial $P \in \mathbb{Q}[x]$ of degree $d \geq 1$, define its root discriminant by $\mathrm{rd}(P) = |\operatorname{disc}(P)|^{1/d}$. An immediate consequence of Theorem 1.2 is the following.

Corollary 7.3. If $\varphi \in \mathbb{Q}[x]$ is postcritically finite, has degree divisible by p, and has good reduction at p, then for any $t_0 \in \mathbb{Z}$, the sequence of polynomials $(\Phi_n(x, t_0))$ is asymptotically bad in the sense that $\mathrm{rd}_p(\Phi_n(x, t_0))$ tends to infinity with n. □

This result is in agreement with a conjecture of Simon [22], to the effect that any infinite sequence of distinct polynomials over $\mathbb{Z}$ is asymptotically bad. Thus, to tackle Questions 7.1 and 7.2, one would very likely have to understand the index of the order $\mathcal{O}_K[\xi_n|_{t_0}]$ in $\mathcal{O}_{K_{n,t_0}}$.

Acknowledgments

The work on this project began in June 2003 during visits by W. Aitken and C. Maire to Amherst, partially supported by the NSF Grant DMS-0226869. A few months later, the paper [14] of V. Nekrashevych appeared as a preprint on arxiv.org; in it, iterated monodromy groups from a more general perspective are studied. We learned from [14] that the construction (1.1) we had been studying had earlier been suggested by R. Pink (private communication). A special case also occurs in Boston [4]. C. Maire thanks R. Pink for a helpful conversation. C. Maire and F. Hajir would like to thank E. Bayer-Fluckiger for financial support of their visits to EPFL, Lausanne, in 2004 where a portion of this work was completed. We are grateful to R. Benedetto, P. Gunnells, and K. Pilgrim for useful discussions. Hajir's work was partially supported by the NSF under Grant DMS-0226869.

References

[1] L. Bartholdi, R. Grigorchuk, and V. Nekrashevych, *From fractal groups to fractal sets*, Fractals in Graz 2001: Analysis—Dynamics—Geometry—Stochastics (P. Grabner and W. Woess, eds.), Trends in Mathematics, Birkhäuser, Basel, 2003, pp. 25–118.

[2] H. Bass, M. V. Otero-Espinar, D. Rockmore, and C. Tresser, *Cyclic Renormalization and Automorphism Groups of Rooted Trees*, Lecture Notes in Mathematics, vol. 1621, Springer-Verlag, Berlin, 1996.

[3] B. Bielefeld, Y. Fisher, and J. Hubbard, *The classification of critically preperiodic polynomials as dynamical systems*, J. Amer. Math. Soc. **5** (1992), no. 4, 721–762.

[4] N. Boston, *Tree representations of Galois groups*, preprint, 2001, http://www.math.wisc.edu/~boston/.

[5] ———, *Explicit deformation of Galois representations*, Invent. Math. **103** (1991), no. 1, 181–196.

[6] E. Brezin, R. Byrne, J. Levy, K. Pilgrim, and K. Plummer, *A census of rational maps*, Conform. Geom. Dyn. **4** (2000), 35–74.

[7] K.-U. Bux and R. Perez, *On the growth of iterated monodromy groups*, preprint, 2004, http://arxiv.org/abs/math.GR/0405456.

[8] A. Douady and J. H. Hubbard, *A proof of Thurston's topological characterization of rational functions*, Acta Math. **171** (1993), no. 2, 263–297.

[9] N. Elkies, *Explicit modular towers*, Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing (Urbana-Champaign, Ill, 1997) (T. Basar and A. Vardy, eds.), University of Illionois, Urbana-Champaign, 1998, pp. 23–32.

[10] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic Curves, Modular Forms, & Fermat's Last Theorem (Hong Kong, 1993), Ser. Number Theory, I, International Press, Massachusetts, 1995, pp. 41–78.

[11] A. Garcia, H. Stichtenoth, and H.-G. Rück, *On tame towers over finite fields*, J. reine angew. Math. **557** (2003), 53–80.

[12] M. Kisin and S. Wortmann, *A note on Artin motives*, Math. Res. Lett. **10** (2003), no. 2-3, 375–389.

[13] S. Lang, *Algebra*, Springer, New York, 2000.

[14] V. Nekrashevych, *Iterated monodromy groups*, preprint, 2003, http://arxiv.org/abs/math.DS/0312306.

[15] F. Pakovich, *Arithmetics of conservative polynomials and yet another action of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *on plane trees*, preprint, 2004, http://arxiv.org/abs/math.NT/0404478.

[16] K. M. Pilgrim, *Dessins d'enfants and Hubbard trees*, Ann. Sci. École Norm. Sup. (4) **33** (2000), no. 5, 671–693.

[17] ———, *On postcritically finite polynomials. Part 1: critical portraits*, preprint, 1993, http://arxiv.org/abs/math.DS/9305207.

[18] A. Poirier, *On postcritically finite polynomials. Part 2: Hubbard trees*, preprint, 1993, http://arxiv.org/abs/math.DS/9307235.

[19] P. Roquette, *On class field towers*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 231–249.

[20] G. Shabat and A. Zvonkin, *Plane trees and algebraic numbers*, Jerusalem Combinatorics '93, Contemp. Math., vol. 178, American Mathematical Society, Rhode Island, 1994, pp. 233–275.

[21] J. H. Silverman, *The field of definition for dynamical systems on* $\mathbf{P}^1$, Compositio Math. **98** (1995), no. 3, 269–304.

[22] D. Simon, *Équations dans les corps de nombres et discriminants minimaux*, Ph.D. thesis, University of Bordeaux I, Talence, 1998.

[23] D. Tischler, *Critical points and values of complex polynomials*, J. Complexity **5** (1989), no. 4, 438–456.

Wayne Aitken: Department of Mathematics, California State University San Marcos, San Marcos, CA 92096, USA
E-mail address: waitken@csusm.edu

Farshid Hajir: Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003-9318, USA
E-mail address: hajir@math.umass.edu

Christian Maire: GRIMM, UFR SES, Université Toulouse 2, 5 Allées Antonio Machado, 31058 Toulouse Cedex, France
E-mail address: christian.maire@univ-tlse2.fr