LOCAL ARBOREAL REPRESENTATIONS

JACQUELINE ANDERSON, SPENCER HAMBLEN, BJORN POONEN, AND LAURA WALTON

Abstract. Let K be a field complete with respect to a discrete valuation v of residue characteristic p. Let $f(z) \in K[z]$ be a separable polynomial of the form $z^\ell - c$. Given $a \in K$, we examine the Galois groups and ramification groups of the extensions of K generated by the solutions to $f^n(z) = a$. The behavior depends upon $v(c)$, and we find that it shifts dramatically as $v(c)$ crosses a certain value: 0 in the case $p \nmid \ell$, and $-p/(p-1)$ in the case $p = \ell$.

1. Introduction

1.1. **Arboreal Galois representations.** Let K be a field. Choose an algebraic closure $\overline{K}$. Let $f(z)$ be a polynomial of degree ℓ over K. For $n \geq 0$, let f^n denote the nth iterate $f \circ f \circ \cdots \circ f$. Fix $a \in K$. For $n \geq 0$, let $f^{-n}(a)$ be the multiset of solutions to $f^n(z) = a$ in $\overline{K}$, so $\# f^{-n}(a) = \ell^n$; also let $K_n = K(f^{-n}(a)) \subseteq \overline{K}$. Let $K_\infty = \bigcup_{n \geq 1} K_n$. For $0 \leq n \leq \infty$, let $G(n) = \operatorname{Aut}(K_n/K)$ and let $I(n)$ be the inertia subgroup of $G(n)$.

Let $n \in \{0, 1, 2, \ldots, \infty\}$. Let T_n be the complete ℓ-ary rooted tree of height n (so there are ℓ^n leaves at the top); here T_∞ is the increasing union of $T_1 \subset T_2 \subset \cdots$. The disjoint union of the $f^{-m}(a)$ for $m \leq n$, with an edge from α to $f(\alpha)$ for each vertex α other than the root, is isomorphic to T_n. Suppose that the solutions to $f^n(z) = a$ are distinct. Then these solutions lie in the separable closure K_s of K in $\overline{K}$, and $\operatorname{Gal}(K_s/K)$ acts on this copy of T_n. This defines a continuous homomorphism $\rho_n \colon \operatorname{Gal}(K_s/K) \to \operatorname{Aut} T_n$. The image of ρ_n is isomorphic to $G(n)$. A continuous homomorphism $\operatorname{Gal}(K_s/K) \to \operatorname{Aut} T_\infty$ is called an arboreal Galois representation [BJ07, Definition 1.1].

There is a large literature studying the image of ρ_∞ for various polynomials over global fields [Odo85a, Odo85b, Sto92, Odo97, BJ07, Jon08, BJ09, Jon13, Hin16], and occasionally also for rational functions [JM14].

Example 1.1. Let $K = \mathbb{Q}$ and $f(z) = z^2 - z + 1$ and $a = 0$. Then ρ_∞ is surjective [Odo85a, Theorem 1].

Example 1.2. Let $K = \mathbb{Q}$. Let $b \in \mathbb{Z}$ be such that either $b > 0$ and $b \equiv 1, 2 \pmod 4$, or $b < 0$ and $b \equiv 0 \pmod 4$. Let $f(z) = z^2 + b$. Then ρ_∞ is surjective [Sto92].

1.2. **Local fields.** From now on, K is a field that is complete with respect to a discrete valuation v. Let k be the residue field. Let p be the characteristic of k. Extend v to K_s.

Consider $f(z) := z^\ell - c \in K[z]$ for some $\ell \geq 2$ and $c \in K^\times$. We assume that we are in one of the following cases:

Date: May 1, 2018.

2010 *Mathematics Subject Classification.* Primary 11S82; Secondary 11F80, 11S15, 37P05, 37P20.

Key words and phrases. Arboreal representation, ramification groups.

B.P. was supported in part by National Science Foundation grants DMS-1069236 and DMS-1601946 and grants from the Simons Foundation (#340694 and #402472 to Bjorn Poonen).

- ("Tame case") ℓ is not divisible by p;
- ("Wild case") $\ell = p$ and K is a finite extension of $\mathbb{Q}_p$.

In particular, f is separable.

In contrast with the situation over global fields in Examples 1.1 and 1.2, our Theorem 2.1 will imply that over a local field K with finite residue field, the arboreal representation associated to a separable polynomial $f(z) = z^\ell - c$ as above is *never* surjective, and never even of finite index. Ingram proved a related result when K is a finite extension of $\mathbb{Q}_p$. In this setting, he showed that if $f \in K[x]$ is a monic polynomial with good reduction and degree not divisible by p, and $a \in K$ is such that $f^n(a) \to \infty$ as $n \to \infty$, then the image of $\operatorname{Gal}(K_s/K)$ is of finite index in a particular infinite index subgroup of $\operatorname{Aut} T_\infty$ [Ing13, Theorem 1].

In this introduction, we describe our main results in the wild case. It turns out that in this case there is a dramatic shift of behavior as $v(c)$ crosses $-p/(p-1)$:

Theorem 1.3. *Suppose that K is a finite extension of $\mathbb{Q}_p$, and $\ell = p$.*
(a) *If $v(c) < -p/(p-1)$, then K_∞/K is a finite extension.*
(b) *If $v(c) = -p/(p-1)$, then K_∞/K is an infinite extension if k is finite, and K_∞/K is finitely ramified if and only if a lies within the closed unit disk centered at a fixed point of f.*
(c) *If $v(c) > -p/(p-1)$, then K_∞/K is infinitely ramified.*

In fact, our results are more precise. For example:

- If $v(c) < -p/(p-1)$ and $v(a) > v(c)/p$ and $\mu_p \subseteq K$, then there exists n depending on $v(c)$ and there exists $\alpha \in f^{-n}(a)$ such that $K_\infty = K(\alpha)$ (generated by one element!) and $G(\infty)$ is an elementary abelian p-group of order at most p^n (Theorems 4.2 and 4.3).
- If $v(c) = -p/(p-1)$, then some upper numbering ramification subgroup of $G(\infty)$ is trivial (Theorem 5.11; see also Example 5.12). This contrasts with Sen's filtration theorem: see Remark 5.13.
- If $v(c) = -p/(p-1)$ and $v(a) > v(c)$ and $\mu_p \subset K$, then $I(\infty)$ is either $\{1\}$ or $(\mathbb{Z}/p\mathbb{Z})^\infty$ (Theorem 5.1).
- If $v(c) < 0$, Theorem 6.2 provides a nontrivial upper bound on the asymptotic rate of growth of $[K_n : K]$.

We prove similar results in the tame case.

1.3. **Outline of the paper.** Section 2 shows that the image of an arboreal representation over a local field has infinite index, whether or not it arises from iterates of a polynomial. Section 3 proves some general lemmas used throughout the rest of the paper. The Galois groups $G(n)$ and $G(\infty)$ depend on whether $v(c)$ is negative, and in the wild case also on whether $v(c) < -p/(p-1)$. Sections 4 to 7 describe these groups; the section titles refer to the valuation of c. Finally, in Section 8, we determine K_∞ completely in the analogous situation with $K = \mathbb{R}$.

2. Images of local arboreal representations

Recall our assumptions on K and k from Section 1.2.

Theorem 2.1. *Assume that* $\operatorname{char} K \neq 2$ *and k is finite. Then the image of any continuous homomorphism $\rho_\infty\colon \operatorname{Gal}(K_s/K) \to \operatorname{Aut} T_\infty$ is of infinite index.*

Proof. Each $\tau \in \operatorname{Aut} T_\infty$ acts as a permutation of the set of the leaves of T_n; let $\operatorname{sgn}_n(\tau)$ be the sign of this permutation. We define a map $\operatorname{sgn}\colon \operatorname{Aut} T_\infty \to \prod_{n\geq 1}\{\pm 1\}$ by assigning $\tau \mapsto \prod_{n\geq 1} \operatorname{sgn}_n(\tau)$.

The hypotheses on K imply that K has only finitely many quadratic extensions, so there are only finitely many continuous homomorphisms $\operatorname{Gal}(K_s/K) \to \prod_{n\geq 1}\{\pm 1\}$. Thus the composition $\operatorname{Gal}(K_s/K) \stackrel{\rho_\infty}{\to} \operatorname{Aut} T_\infty \stackrel{\operatorname{sgn}}{\to} \prod_{n\geq 1}\{\pm 1\}$ has finite image. On the other hand, the map $\operatorname{Aut} T_\infty \stackrel{\operatorname{sgn}}{\to} \prod_{n\geq 1}\{\pm 1\}$ is surjective. □

Remark 2.2. Without the assumption that k is finite, Theorem 2.1 can fail. For example, if $K = \mathbb{Q}((t))$, then any $f(x)$ as in Example 1.2 defines a surjective ρ_∞.

Remark 2.3. If k is finite but $\operatorname{char} K = 2$, then again Theorem 2.1 can fail, as we now explain. In this case, $K = \mathbb{F}_{2^e}((t^{-1}))$ for some e, and the maximal pro-2 quotient of $\operatorname{Gal}(K_s/K)$ is a free pro-2 group of infinite rank [Kat86, 1.4.4]. This implies that $\operatorname{Gal}(K_s/K)$ admits a continuous surjective homomorphism onto any inverse limit of a sequence of finite 2-groups. If T_∞ is a binary tree ($\ell = 2$), then $\operatorname{Aut} T_\infty$ is such an inverse limit.

3. General lemmas

For $n \geq 1$, let $\nu_n = -\frac{\ell^{n+1}}{(\ell^n-1)(\ell-1)} v(\ell)$. Let $\nu_\infty = -\frac{\ell}{\ell-1} v(\ell)$. It will turn out that there is a shift of behavior when $v(c)$ crosses these values. In the tame case, all these values collapse into one: $\nu_n = 0$ for all $n \leq \infty$. In the wild case, $\nu_n = -\frac{p^{n+1}}{(p^n-1)(p-1)}$ and their limit is $\nu_\infty = -\frac{p}{p-1}$.

Lemma 3.1. *Let $d, y \in \overline{K}$. Consider the ℓ solutions x to $f(x) - f(y) = d$, counted with multiplicity.*

(a) *If $v(d) \leq \ell v(y) - \nu_\infty$, then $v(x-y) = v(d)/\ell$ for each x.*
(b) *If $v(d) > \ell v(y) - \nu_\infty$, then the solution x that is closest to y satisfies $v(x-y) = v(d) - (\ell-1)v(y) - v(\ell)$ and the other $(\ell-1)$ solutions x satisfy $v(x-y) = v(y) + v(\ell)/(\ell-1)$. The first solution lies in $K(d,y)$.*
(c) *If $\ell = p$ and $v(d) = \ell v(y) - \nu_\infty$, then the solutions generate an unramified extension of $K(d,y)$.*

Proof.

(a,b) Let $z = x - y$. Let $K' = K(d,y)$. We need the valuations of the zeros of the polynomial

$$f(z+y) - f(y) - d = z^\ell + \binom{\ell}{1} y z^{\ell-1} + \binom{\ell}{2} y^2 z^{\ell-2} + \cdots + \binom{\ell}{\ell-1} y^{\ell-1} z - d \in K'[z].$$

Its Newton polygon is the lower convex hull of the points $(0, v(d))$, $(1, (\ell-1)v(y) + v(\ell))$, and $(\ell, 0)$. The slopes of the Newton polygon depend on whether the middle point lies above or below the line segment through $(0, v(d))$ and $(\ell, 0)$. These slopes determine the valuations of the zeros. A Newton polygon segment of width 1 corresponds to a solution in the ground field $K(d,y)$.

(c) The Newton polygon of $f(z+y) - f(y) - d$ is a line segment containing the three points above, while all other intermediate monomials correspond to points strictly above this line since the prime ℓ divides each binomial coefficient. Thus, if we scale the variable to make the first two points horizontal, and then divide by the leading coefficient, we obtain a polynomial $g(z)$ reducing to $\bar{g}(z) := z^\ell + u_1 z + u_2$ for some units u_1, u_2. We have $\bar{g}'(z) = u_1$, so $\bar{g}$ is separable, so the roots of g generate an unramified extension. □

Lemma 3.2. *Suppose that $v(c) < 0$. If n is sufficiently large, then every $\alpha \in f^{-n}(a)$ satisfies $v(\alpha) = v(c)/\ell$. If $v(a) > v(c)$, then this conclusion holds for all $n \geq 1$.*

Proof. Let $\alpha_0 = a$ and let $\alpha_{n+1} \in f^{-1}(\alpha_n)$ for $n \geq 1$. The equation $\alpha_{n+1}^\ell = \alpha_n + c$ implies that

$$v(\alpha_{n+1}) = \begin{cases} v(\alpha_n)/\ell, & \text{if } v(\alpha_n) < v(c); \\ v(c)/\ell \text{ or larger}, & \text{if } v(\alpha_n) = v(c); \\ v(c)/\ell, & \text{if } v(\alpha_n) > v(c). \end{cases}$$

Thus the first case holds at most finitely many times, and then the second case holds at most once, and then the third case holds from then on. □

Lemma 3.3. *If $\mu_\ell \subset K$, then $G(n)$ is an ℓ-group.*

Proof. Each extension K_{n+1}/K_n is a Kummer extension of exponent dividing ℓ. □

4. Sufficiently negative valuation

In this section, we consider the case $v(c) < \nu_\infty$.

Lemma 4.1. *Suppose that $v(c) < \nu_\infty$ and $v(a) > v(c)$. If $n \geq 0$ and $\alpha, \beta \in f^{-n}(a)$, then $v(\alpha - \beta) \geq v(c)/\ell + v(\ell)/(\ell - 1)$.*

Proof. We may assume that $n \geq 1$ and $\alpha \neq \beta$. We use induction on n. If $n = 1$, then $\beta^\ell = c + a$, so $v(\beta) = v(c + a)/\ell = v(c)/\ell$. Also $\alpha^\ell = c + a$, so $\alpha = \zeta\beta$ for some ℓth root of unity ζ. Then $v(\alpha - \beta) = v((\zeta - 1)\beta) = v(\ell)/(\ell - 1) + v(c)/\ell$.

Suppose that $n > 1$ and the result holds for $n - 1$. Let $d = f(\alpha) - f(\beta)$ and $y = \beta$. If $n > 1$, then by the inductive hypothesis, the hypothesis on c, and Lemma 3.2,

$$v(d) \geq v(c)/\ell + v(\ell)/(\ell - 1) > v(c) + \ell v(\ell)/(\ell - 1) = \ell v(y) - \nu_\infty, \tag{1}$$

so Lemma 3.1(b) shows that $v(\alpha - \beta) \geq v(y) + v(\ell)/(\ell - 1) = v(c)/\ell + v(\ell)/(\ell - 1)$. □

Theorem 4.2. *If $v(c) < \nu_\infty$ and $v(a) > v(c)$ and $\mu_\ell \subseteq K$, then*
(a) *The group $G(n)$ is isomorphic to a subgroup of $(\mathbb{Z}/\ell\mathbb{Z})^n$.*
(b) *The group $G(n)/I(n)$ is cyclic of order dividing ℓ.*
(c) *For any $\alpha_n \in f^{-n}(a)$, we have $K_n = K(\alpha_n)$.*

Proof.
(a) Let $\delta = v(c)/\ell + v(\ell)/(\ell - 1)$. Let $m \in \{1, \ldots, n\}$. For $x, y \in f^{-m}(a)$, write $x \sim y$ if $v(x - y) > \delta$; this defines an equivalence relation. Let $\mathcal{D}_m = f^{-m}(a)/\sim$. Suppose that $\alpha_{m-1}, \beta_{m-1} \in f^{-(m-1)}(a)$ and $\alpha_m \in f^{-1}(\alpha_{m-1})$. By Lemma 4.1, $v(\alpha_{m-1} - \beta_{m-1}) \geq \delta$. Lemma 3.1(b) with $(d, y) := (\alpha_{m-1} - \beta_{m-1}, \alpha_m)$ applies (by (1)), so for all but one $\beta_m \in f^{-1}(\beta_{m-1})$, we have $v(\alpha_m - \beta_m) = v(y) + v(\ell)/(\ell - 1) = \delta$, and for the other β_m, we have $v(\alpha_m - \beta_m) > \delta$. In other words, exactly one preimage of β_{m-1} is equivalent to α_m. Thus the map

$$\begin{aligned} f^{-m}(a) &\longrightarrow f^{-(m-1)}(a) \times \mathcal{D}_m \\ x &\longmapsto (f(x), \text{equivalence class of } x) \end{aligned}$$

is a bijection. The multiplication action of μ_ℓ on $f^{-m}(a)$ is compatible with the trivial action on $f^{-(m-1)}(a)$; on the other hand, it induces an action on $\mathcal{D}_m$. The action on $f^{-m}(a)$ is free (since the elements of $f^{-m}(a)$ are nonzero), so the action on $\mathcal{D}_m$ is free. But $\#\mathcal{D}_m = \ell^m/\ell^{m-1} = \ell = \#\mu_\ell$, so $\mathcal{D}_m$ is a μ_ℓ-torsor, and its automorphism group as a torsor is μ_ℓ. Each element of $G(n)$ acts trivially on μ_ℓ, and hence acts as an automorphism of the μ_ℓ-torsor $\mathcal{D}_m$. Combining the bijections for $m = 1, \ldots, n$ yields a Galois-equivariant bijection $f^{-n}(a) \xrightarrow{\sim} \prod_{i=1}^n \mathcal{D}_i$, so $G(n) \leq \prod_{i=1}^n \operatorname{Aut}_{\mu_\ell\text{-torsor}}(\mathcal{D}_i) = \mu_\ell^n \simeq (\mathbb{Z}/\ell\mathbb{Z})^n$.

(b) The group $G(n)/I(n)$ is isomorphic to the Galois group of the residue field extension, which is cyclic. Its order divides the exponent of $G(n)$, which by (a) is ℓ.

(c) If an element of $\prod_{i=1}^m \operatorname{Aut}_{\mu_\ell\text{-torsor}}(\mathcal{D}_i)$ fixes one element of $\prod_{i=1}^n \mathcal{D}_i$, it fixes all elements. Thus the subgroup of $G(n)$ fixing α_n is trivial. By Galois theory, $K(\alpha_n) = K_n$. □

Recall that $\nu_n = -\frac{\ell^{n+1}}{(\ell^n-1)(\ell-1)} v(\ell)$, which is 0 in the tame case.

Theorem 4.3. *Suppose that $v(a) \geq v(c)/\ell$. In the tame case, if $v(c) < 0$, then $K_\infty = K_1$. In the wild case, if $v(c) < \nu_n$, then $K_\infty = K_n$, and if $v(c) = \nu_n$, then $K_\infty = K_{n+1}$ and K_{n+1}/K_n is unramified.*

Proof. First suppose that $v(c) < \nu_n$. Let $\alpha_0 = a$, and for $m \geq 1$, let α_m be an element of $f^{-1}(\alpha_{m-1})$ minimizing the distance to α_{m-1}. Let $q_m = v(\alpha_m - \alpha_{m-1})$. By Lemma 3.2, $v(\alpha_m) = v(c)/\ell$ for all $m \geq 1$. Thus $q_1 \geq v(c)/\ell$. For $m \geq 1$, Lemma 3.1 applied to $d = \alpha_m - \alpha_{m-1}$ and $y = \alpha_m$ implies

$$q_{m+1} = \begin{cases} q_m/\ell, & \text{if } q_m \leq v(c) - \nu_\infty; \\ q_m - (\ell-1)v(c)/\ell - v(\ell), & \text{otherwise.} \end{cases} \tag{2}$$

If the first case in (2) holds for $m = 1, 2, \ldots, n-1$, then $q_{n-1} = \ell^{1-n} q_1 \geq \ell^{-n} v(c) > v(c) - \nu_\infty$ by definition of ν_n, so the second case holds for $m = n$. Moreover, if the second case holds for a given m, then we remain in the second case from then on, since $-(\ell-1)v(c)/\ell - v(\ell)$ is positive under the hypothesis $v(c) < \nu_n \leq \nu_\infty$. Thus the second case holds for all $m \geq n$, and we have $n = 1$ in the tame case. The final sentence of Lemma 3.1(b) implies that for all $m \geq n$, we have $\alpha_{m+1} \in K(d, y) \subseteq K_m$. By Theorem 4.2(c), this implies that $K_{m+1} = K_m$ for all $m \geq n$. Thus $K_\infty = K_n$.

Now suppose instead that we are in the wild case and $v(c) = \nu_n$. Then $v(c) < \nu_{n+1}$, so the previous paragraph shows that $K_\infty = K_{n+1}$. The arguments above show that if the first case holds for $m = 1, 2, \ldots, n-1$, then $q_{n-1} \geq v(c) - \nu_\infty$. Thus we obtain $K_{n+1} = K_n$ as before unless if $q_{n-1} = v(c) - \nu_\infty$, in which case Lemma 3.1(c) shows that α_{n+1} is unramified over K_n for each $\alpha_{n+1} \in f^{-(n+1)}(a)$. □

Corollary 4.4. *If $v(c) < \nu_\infty$, then K_∞ is a finite extension of K.*

Proof. Choose n such that $v(c) < \nu_n$. By Lemma 3.2, there exists an $m \geq 1$ such that every $\alpha \in f^{-m}(a)$ satisfies $v(\alpha) = v(c)/\ell$. Apply Theorem 4.3 over K_m with each α in place of a, and take the compositum of the resulting finite extensions. □

Theorem 4.5. *Suppose that $\ell = p$ and $\mu_\ell \subseteq K$.*

(a) *Suppose $\nu_{n-1} < v(c) < \nu_n$ and $v(a) > v(c)/\ell$. If $v(c) \notin \ell v(K^\times)$, then $G(\infty) = G(n) = I(\infty) = I(n) \simeq (\mathbb{Z}/\ell\mathbb{Z})^n$. More generally, if ℓ^r is the largest power of ℓ such that $v(c) \in \ell^r v(K^\times)$, then $\ell^{n-r} \leq \#I(n) \leq \#G(n) = \#G(\infty) \leq \ell^n$.*

(b) *If* $v(c) = \nu_n$ *and* $v(a) \geq v(c)/\ell$, *then* $G(\infty) = G(n+1) \leq (\mathbb{Z}/\ell\mathbb{Z})^{n+1}$, $I(\infty) = I(n) \leq (\mathbb{Z}/\ell\mathbb{Z})^n$, *and* $G(\infty)/I(\infty) \leq \mathbb{Z}/\ell\mathbb{Z}$.

Proof.

(a) In the proof of Theorem 4.3, we have $v(\alpha_1) = v(c)/\ell$, so $q_1 = v(\alpha_1 - a) = v(c)/\ell$. Then by (2), $q_m = v(c)/\ell^m$ for $m = 1, \dots, n$, since the hypothesis $\nu_{n-1} < v(c)$ implies that $v(c)/\ell^{m-1} \leq v(c) - \nu_\infty$ for $m \leq n$. In particular, $\alpha_n - \alpha_{n-1}$ is an element of K_n whose valuation is $q_n = v(c)/\ell^n$, so the ramification index $(v(K_n^\times) : v(K^\times))$ is at least ℓ^{n-r}. Thus $\#I(n) \geq \ell^{n-r}$. On the other hand, $I(n) \leq G(n) \leq (\mathbb{Z}/\ell\mathbb{Z})^n$ by Theorem 4.2(a). In particular, if $r = 0$, then equality holds. In any case, $K_\infty = K_n$ by Theorem 4.3.

(b) By Theorem 4.3, $K_\infty = K_{n+1}$, and K_{n+1}/K_n is unramified. Then $G(\infty) = G(n+1) \leq (\mathbb{Z}/\ell\mathbb{Z})^{n+1}$ by Theorem 4.2(a), and $I(\infty) = I(n+1) = I(n) \leq G(n) \leq (\mathbb{Z}/\ell\mathbb{Z})^n$. Finally, $G(\infty)/I(\infty) = G(n+1)/I(n+1) \leq \mathbb{Z}/\ell\mathbb{Z}$ by Theorem 4.2(b).

□

5. Special negative valuation: $v(c) = -p/(p-1)$

In this section and the next, we consider the wild case.

5.1. **Galois groups and inertia groups.**

Theorem 5.1. *Suppose that* $\ell = p$ *and* $v(c) = -p/(p-1)$ *and* $0 \leq n < \infty$. *Let* $b \in \overline{K}$ *be a fixed point of* $f(z)$.

(a) *If* $\mu_p \subset K$, *then* $G(n)/I(n)$ *is a cyclic* p*-group.*
(b) *The group* $I(n)$ *is a* p*-group.*
(c) *If* $v(a) > v(c)$, *then* $I(n)$ *is an elementary abelian* p*-group of order dividing* p^n.
(d) *If* $\mu_p \subset K$, *then* $G(\infty)/I(\infty) \cong \mathbb{Z}_p$.
(e) *If* $v(a-b) < 0$, *then* $I(\infty)$ *is an infinite pro-*p *group; if, moreover,* $v(a) > v(c)$, *then* $I(\infty) \simeq (\mathbb{Z}/p\mathbb{Z})^\infty$.
(f) *If* $v(a-b) \geq 0$, *then* $I(\infty)$ *is finite; if, moreover,* $b \in K$, *then* $I(\infty) = \{1\}$.

Proof. Let k_n be the residue field of K_n.

(a) The group $G(n)/I(n)$ is isomorphic to the group $\mathrm{Gal}(k_n/k)$, a Galois group of an extension of finite fields, so it is cyclic. By Lemma 3.3, $G(n)$ is a p-group, so $G(n)/I(n)$ is a p-group too.
(b) Since $v(c) = -p/(p-1)$, the ramification index of K over $\mathbb{Q}_p$ is divisible by $p-1$. The extension $K(\mu_p)/K$ is tamely ramified with ramification index dividing $p-1$, so after replacing K by an unramified extension, we have $\mu_p \subset K$. Then Lemma 3.3 applies.
(c) By Lemma 3.2, if $m \geq 1$ and $\alpha \in f^{-m}(a)$, then $v(\alpha) = -1/(p-1)$.

Next we prove by induction that for $n \geq 1$, for any distinct $\alpha_n, \beta_n \in f^{-n}(a)$, we have $v(\alpha_n - \beta_n) = 0$. If $n = 1$, then $\alpha_1 = \zeta\beta_1$ for some pth root of unity, so $v(\alpha_1 - \beta_1) = v(\zeta - 1) + v(\beta_1) = 1/(p-1) - 1/(p-1) = 0$. Now suppose that $n > 1$ and the result holds for all $m < n$. Given distinct $\alpha_n, \beta_n \in f^{-n}(a)$, let $\alpha_{n-1} = f(\alpha_n)$ and $\beta_{n-1} = f(\beta_n)$. Let $d = \alpha_{n-1} - \beta_{n-1}$ and $y = \beta_n$, so $v(y) = -1/(p-1)$. If $\alpha_{n-1} \neq \beta_{n-1}$, then $v(d) = 0$ by the inductive hypothesis, and $pv(y) + p/(p-1) = 0$ too, so Lemma 3.1(a) implies that $v(\alpha_n - \beta_n) = v(d)/p = 0$. If $\alpha_{n-1} = \beta_{n-1}$, then $d = 0$, so Lemma 3.1(b) applies: the solution to $f(x) - f(\beta_n) = 0$ closest to β_n is β_n itself, and the other solutions satisfy

$v(x-\beta_n) = v(y) + 1/(p-1) = 0$; in particular, $v(\alpha_n - \beta_n) = 0$. In both cases, the inductive step is completed.

Let $n \geq 1$. Let $\mathcal{O}_n$ be the closed unit disk in K_n centered at 0; let $\mathfrak{m}$ be the open unit disk in K_n centered at 0. Let D_n be the closed unit disk in K_n containing $f^{-n}(a)$; by the previous paragraph, such a disk exists and the natural map $f^{-n}(a) \to D_n/\mathfrak{m}$ is injective. Injectivity implies that $G(n)$ acts faithfully on $D_n/\mathfrak{m}$. The simply transitive translation action of $\mathcal{O}_n/\mathfrak{m}$ on $D_n/\mathfrak{m}$ is $G(n)$-equivariant, and hence $I(n)$-equivariant. Since $I(n)$ acts trivially on the residue field $\mathcal{O}_n/\mathfrak{m}$, the previous sentence implies that each $\sigma \in I(n)$ acts on $D_n/\mathfrak{m}$ as a translation by some element of $\mathcal{O}_n/\mathfrak{m}$. This defines an injective homomorphism $I(n) \hookrightarrow \mathcal{O}_n/\mathfrak{m}$, so $I(n)$ is an elementary abelian p-group. The number of translations mapping $f^{-n}(a)$ mod $\mathfrak{m}$ to itself is at most $\#f^{-n}(a) = p^n$, so $\#I(n) \leq p^n$.

(d) Fix $\alpha_n \in f^{-n}(a)$. As β_n varies over $f^{-n}(a)$, the argument in the proof of (c) shows that the differences $\alpha_n - \beta_n$ have valuation 0 and have distinct residues. Thus $\#k_n \geq p^n$. Hence k_∞ is infinite, so $G(\infty)/I(\infty)$ is infinite. On the other hand, by (a), $G(\infty)/I(\infty)$ is an inverse limit of cyclic p-groups. Thus $G(\infty)/I(\infty) \simeq \mathbb{Z}_p$.

(e) By (b) and (c), it will suffice to show that $I(\infty)$ is infinite. In proving this, we may replace K by its finite extension $K(b)$. Conjugating $z \mapsto f(z)$ by the coordinate change $z = x + b$ yields $x \mapsto g(x)$, where

$$g(x) := f(x+b) - b = x^p + \binom{p}{1} b x^{p-1} + \cdots + \binom{p}{p-1} b^{p-1} x. \tag{3}$$

Examining the Newton polygon of $x^p - x - c$ shows that $v(b) = v(c)/p = -1/(p-1)$, so each coefficient of g is p-adically integral. If $\alpha \in \overline{K}$ satisfies $v(\alpha) < 0$, then any solution to $g(x) = \alpha$ has valuation $v(\alpha)/p$. Thus if we start at $z = a$, or equivalently at $x = a - b$, and if $v(a-b) < 0$, then every element of $f^{-n}(a)$ has x-coordinate of valuation $v(a-b)/p^n$. Thus the ramification index of $K(f^{-n}(a))$ over K tends to ∞ as $n \to \infty$.

(f) By adjoining b to K, we reduce to proving the second statement. Thus we assume that $b \in K$, and we need to prove that $I(\infty) = \{1\}$. The polynomial $g(x)$ in (3) has p-adically integral coefficients, and its reduction modulo the maximal ideal is separable (of the form $x^p + ux$ for some $u \in k^\times$, since $v(b) = -1/(p-1)$). Since $v(a-b) \geq 0$, conjugating $g(x)$ by the coordinate change $x = y + (a-b)$ yields another polynomial $h(y)$ with p-adically integral coefficients and with separable reduction. Moreover, $h(y)$ could be obtained directly from $f(z)$ by conjugating by $z = y + a$, so $h(y)$ has coefficients in K. Since $h(y)$ has separable reduction, adjoining solutions to $h(y) = e$ for any p-adically integral e yields an unramified extension. By induction, $K(h^{-n}(0))$ is unramified over K for every $n \geq 0$. Conjugating back shows that $K(f^{-n}(a))$ is unramified over K for every $n \geq 0$. Thus $I(\infty) = \{1\}$. □

Corollary 5.2. *If $\ell = p$ and $v(c) = -p/(p-1)$, then $[K_\infty : K] = \infty$.*

Proof. We may replace K by $K(\mu_p)$. Then Theorem 5.1(d) implies that $G(\infty)/I(\infty)$ is infinite, so $[K_\infty : K] = \#G(\infty) = \infty$. □

Example 5.3. Let $p = 2$ and $c = -1/4$, so $f(z)$ is $z^2 + 1/4$. If $a = 1/2$, then K_∞ is the unramified $\mathbb{Z}_2$-extension of $\mathbb{Q}_2$.

5.2. **Ramification group lemmas.** We will prove results about the ramification groups of $G(\infty)$, but first we need some lemmas about ramification groups in general. Let K be a local field, and let L be a Galois extension of K with Galois group G. For $u \in \mathbb{R}_{\geq 0}$, let $G_u \leq G$ be the uth ramification group in the lower numbering. For $w \in \mathbb{R}_{\geq 0}$, let $G^w \leq G$ be the wth ramification group in the upper numbering. (We use the definitions in [Ser79, IV].)

Lemma 5.4. *Let K be a local field, and let L be a Galois extension of K with Galois group G. Then $\bigcap_{w \in \mathbb{R}_{\geq 0}} G^w = \{1\}$.*

Proof. The intersection maps to the corresponding intersection for each finite Galois subextension L' over K, so we may assume that L is finite over K. Suppose that $\sigma \in \bigcap_{w \in \mathbb{R}_{\geq 0}} G^w$. The G^w are the same as the G_u, only renumbered, so $\sigma \in G_u$ for all $u \in \mathbb{R}_{\geq 0}$. Then for any $x \in \mathcal{O}_L$, we have $v({}^\sigma x - x) \geq u + 1$ for all u, so ${}^\sigma x = x$. The field generated by the elements of $\mathcal{O}_L$ is L, so $\sigma = 1$ in $\operatorname{Gal}(L/K)$. $\square$

Lemma 5.5. *Consider a tower of extensions $K \subseteq L \subseteq M$ of a local field K. Suppose that M is Galois over K and L is finite over K. Let $G = \operatorname{Gal}(M/K)$ and $H = \operatorname{Gal}(M/L)$. Then $G^w \cap H \leq H^w$ for all $w \in \mathbb{R}_{\geq 0}$.*

Proof. If the result holds for every finite Galois extension of K lying between L and M, then the result holds for M too. Thus we may assume that M is finite over K. Lower numbering ramification groups are compatible with subgroups; that is, $H_t = G_t \cap H$ for all $t \in \mathbb{R}_{\geq 0}$. Thus H_0/H_t injects into G_0/G_t, so the Herbrand functions defined in [Ser79, IV.§3] satisfy

$$\phi_{M/K}(u) := \int_0^u \frac{dt}{(G_0 : G_t)} \leq \int_0^u \frac{dt}{(H_0 : H_t)} =: \phi_{M/L}(u).$$

Thus for $s \in H$, we have

$$s \in G^{\phi_{M/L}(u)} \implies s \in G^{\phi_{M/K}(u)} \iff s \in G_u \iff s \in H_u \iff s \in H^{\phi_{M/L}(u)}.$$

Hence $G^{\phi_{M/L}(u)} \cap H \leq H^{\phi_{M/L}(u)}$. As u ranges over $[0, \infty)$, so does $\phi_{M/L}(u)$; thus $G^w \cap H \leq H^w$ for all $w \in \mathbb{R}_{\geq 0}$. $\square$

Corollary 5.6. *With notation as in Lemma 5.5, suppose in addition that L is Galois over K. Let $w \in \mathbb{R}_{\geq 0}$. If H^w and $(G/H)^w$ are $\{1\}$, then $G^w = \{1\}$.*

Proof. The surjection $G \twoheadrightarrow G/H$ maps G^w into $(G/H)^w = \{1\}$, so $G^w \leq H$. In particular, $G^w = G^w \cap H$, which by Lemma 5.5 is contained in $H^w = \{1\}$. $\square$

Corollary 5.7. *With notation as in Lemma 5.5, if $H^w = \{1\}$ for some $w \in \mathbb{R}_{\geq 0}$, then $G^{w'} = \{1\}$ for some $w' \in \mathbb{R}_{\geq 0}$.*

Proof. By Lemma 5.5, $G^w \cap H \leq H^w = \{1\}$. Thus G^w injects into the finite set G/H, so G^w is finite. The groups $G^{w'}$ are decreasing and their intersection is $\{1\}$ by Lemma 5.4, so $G^{w'} = \{1\}$ for some $w' \geq w$. $\square$

Lemma 5.8. *Let K be a local field. Let $L_1, \ldots, L_n$ be Galois extensions of K. Let $w \in \mathbb{R}_{\geq 0}$. If $\operatorname{Gal}(L_i/K)^w = \{1\}$ for all i, then $\operatorname{Gal}(L_1 \cdots L_n/K)^w = \{1\}$.*

Proof. The injection $\operatorname{Gal}(L_1 \cdots L_n/K) \hookrightarrow \prod_{i=1}^n \operatorname{Gal}(L_i/K)$ maps $\operatorname{Gal}(L_1 \cdots L_n/K)^w$ into each $\operatorname{Gal}(L_i/K)^w$. $\square$

Lemma 5.9. *Let $L \supseteq K$ be a finite Galois extension of local fields with Galois group G. Then for any $u \in \mathbb{R}_{\geq 0}$, the uth upper and lower numbering ramification groups satisfy $G^u \leq G_u$.*

Proof. The Herbrand function satisfies $\phi(u) := \int_0^u \frac{dt}{(G_0:G_u)} \leq \int_0^u dt = u$, so $G^u \leq G^{\phi(u)} = G_u$. □

Lemma 5.10. *Let v be a valuation on a field K. Let $x, y \in K$. If $v(x) = v(y) = -\epsilon$ for some $\epsilon > 0$, and $v(x-y) = 0$, then $v(x^{-1} - y^{-1}) = 2\epsilon$.*

Proof. This follows from $x^{-1} - y^{-1} = -\frac{x-y}{xy}$. □

5.3. **Ramification groups of iterates.** We now return to the study of the Galois groups of $f^n(z) - a$. The following theorem shows that when $v(c) = -p/(p-1)$, the ramification in K_∞/K is not very deep. Let $b \in \overline{K}$ be a fixed point of f. Let e be the ramification index of K over $\mathbb{Q}_p$.

Theorem 5.11. *Suppose that $\ell = p$. If $v(c) = -p/(p-1)$, then there exists $w \in \mathbb{R}_{\geq 0}$ such that $G(\infty)^w = \{1\}$.*

Proof. First suppose that $v(a) > v(c)$ and $b \in K$. If $v(a-b) \geq 0$, then Theorem 5.1(f) implies that $I(\infty) = \{1\}$, so the conclusion holds trivially, with $w = 0$. So assume that $v(a-b) < 0$. Let $n \geq 1$. Let v_n be the valuation on K_n normalized so that its value group is $\mathbb{Z}$. Thus $v_n = (e\#I(n))v$. By Theorem 5.1(c), we have $\#I(n) \leq p^n$. Let K' be the maximal unramified extension of K in K_n. Fix $\alpha \in f^{-n}(a)$, and let $\gamma = \alpha - b$. Let $\sigma \in I(n) = \operatorname{Gal}(K_n/K')$ be such that $\sigma \neq 1$. The proof of Theorem 5.1(c) shows that σ acts on $f^{-n}(a)$ without fixed points. In particular, ${}^\sigma\alpha \neq \alpha$, and the proof of Theorem 5.1(c) shows that $v({}^\sigma\alpha - \alpha) = 0$. Since σ fixes b, we obtain $v({}^\sigma\gamma - \gamma) = 0$. The proof of Theorem 5.1(e) shows that $v(\gamma) = v(a-b)/p^n$, so $|v_n(\gamma)| = (e\#I(n))|v(a-b)|/p^n \leq e|v(a-b)|$. Lemma 5.10 applied to $x = {}^\sigma\gamma$ and $y = \gamma$ shows that

$$v_n({}^\sigma\gamma^{-1} - \gamma^{-1}) \leq 2e|v(a-b)|.$$

Hence for any positive integer $w \geq 2e|v(a-b)|$, we have $G(n)_w = \{1\}$, so Lemma 5.9 shows that $G(n)^w = \{1\}$ too. This holds for all n, so $G(\infty)^w = \{1\}$ for such w.

Now we consider the general case. By Lemma 3.2, we can find $m \geq 1$ such that all $\alpha \in f^{-m}(a)$ satisfy $v(\alpha) = v(c)/p$, so $v(\alpha) > v(c)$. Let L be a finite Galois extension of K containing $f^{-m}(a)$ and b. For each α, the previous paragraph yields $w \in \mathbb{R}_{\geq 0}$ such that $\operatorname{Gal}(L(f^{-\infty}(\alpha))/L)^w = \{1\}$; by taking the maximum of the w's, we find one w for which $\operatorname{Gal}(L(f^{-\infty}(\alpha))/L)^w = \{1\}$ for all $\alpha \in f^{-m}(a)$. Taking the compositum over α yields $\operatorname{Gal}(L(f^{-\infty}(a))/L)^w = \{1\}$ by Lemma 5.8. By Corollary 5.7, $\operatorname{Gal}(L(f^{-\infty}(a))/K)^{w'} = \{1\}$ for some $w' \in \mathbb{R}_{\geq 0}$. Taking the image in the quotient $G(\infty)$ of $\operatorname{Gal}(L(f^{-\infty}(a))/K)$ shows that $G(\infty)^{w'} = \{1\}$. □

Example 5.12. Suppose that $\ell = p$ and $e = p-1$ and $v(c) = -p/(p-1)$ and $b \in K$ and $v(a-b) = -1/(p-1)$ (this implies $v(a) \geq -1/(p-1) > v(c)$). Then the first paragraph of the proof of Theorem 5.11 shows that $G(n)_2 = \{1\}$ for all n. On the other hand, $G(n)_0 = G(n)_1$ since the inertia group is of p-power order. Thus the only break in the ramification filtration (in either the lower or upper numbering) occurs at 1, and for the upper numbering this holds also for $I(\infty)$.

Remark 5.13. Let K be a characteristic 0 local field with perfect residue field of characteristic p. For a continuous homomorphism ρ from $\operatorname{Gal}(K_s/K)$ to a p-adic Lie group G, Sen's theorem [Sen72, §4] relates the ramification filtration to the "Lie filtration" of G. Theorem 5.11 and Example 5.12 show that the analogue for arboreal representations does not hold.

6. Insufficiently negative valuation

Theorem 6.1. *If $\ell = p$ and $-p/(p-1) < v(c) < 0$, then K_∞/K is infinitely wildly ramified.*

Proof. By Lemma 3.2, we may replace a by some iterated preimage to assume that $v(\alpha) = v(c)/p$ for every $\alpha \in f^{-n}(a)$ for every $n \geq 0$. Let $\alpha_0 = a$, and inductively choose $\alpha_n \in f^{-1}(\alpha_{n-1})$ for $n \geq 1$. Let $\beta_0 = a$, and inductively choose $\beta_n \in f^{-1}(\beta_{n-1})$ such that $\beta_1 \neq \alpha_1$. Let $d_n = \beta_n - \alpha_n$. By Lemma 3.1(b) with $d = 0$ and $y = \alpha_1$, we have $v(d_1) = v(c)/p + 1/(p-1) > 0$.

We prove by induction that $v(d_n) = v(d_1)/p^{n-1}$ for all $n \geq 1$. The base case $n = 1$ is trivial. Suppose that $n \geq 2$ and the result holds for $n-1$. Let $d = d_{n-1}$ and $y = \alpha_n$. By the inductive hypothesis,

$$v(d) = v(d_1)/p^{n-2} \leq v(d_1) = v(c)/p + 1/(p-1) < p(v(c)/p + 1/(p-1)) = pv(y) + p/(p-1).$$

By Lemma 3.1(a), $v(d_n) = v(d)/p = v(d_{n-1})/p = v(d_1)/p^{n-1}$.

Thus the exponent of p in the denominator of $v(d_n)$ eventually grows with n, so K_∞/K is infinitely wildly ramified. □

We next bound the growth rate of $[K_n : K]$. We have $\mu_p \subseteq K_1$. For $r \geq 1$, the field K_{r+1} is obtained from K_r by adjoining the pth roots of the p^r numbers $\alpha_r + c$ as α_r ranges over the elements of $f^{-r}(a)$. By Kummer theory, $[K_{r+1} : K_r]$ equals the order of the subgroup generated by these p^r numbers in $K_r^\times/K_r^{\times p}$. In particular, $[K_{r+1} : K_r] \leq p^{p^r}$ for all $r \geq 1$. Similarly, $[K_1 : K(\mu_p)] \leq p$. Also, $[K(\mu_p) : K] \leq p-1$. Taking the product yields the "trivial" bound

$$[K_n : K] \leq B_n := (p-1) \prod_{m=1}^{n} p^{p^m}.$$

(If $p = 2$, then $B_n = \#\operatorname{Aut} T_n$.) The next theorem shows that when $v(c) < 0$, we can do better.

Theorem 6.2. *Suppose that $\ell = p$ and $v(c) < 0$. Let $r \in \mathbb{Z}_{\geq 1}$ be such that $v(c) < -p/((p^r - 1)(p-1))$. Then there exists a constant C depending on p, r, and $v(a)$ such that*

$$[K_n : K] \leq C B_n^{1-p^{-r}}.$$

We will need the following lemma in the proof of Theorem 6.2.

Lemma 6.3. *Let $\epsilon \in K$. If $v(\epsilon) > p/(p-1)$, then $1 + \epsilon \in K^{\times p}$.*

Proof. The hypothesis implies that the Newton polygon of $(1+x)^p - (1+\epsilon)$ has vertices at $(0, v(\epsilon))$, $(1,1)$, and $(p, 0)$. The width 1 segment at the left corresponds to a root in K. □

Proof of Theorem 6.2. By Lemma 3.2, there exists $m_0 \geq 1$ such that if $m \geq m_0$ and $\alpha_m \in f^{-m}(a)$, then $v(\alpha_m) \geq v(c)$.

We will show that if $m \geq m_0$ and $\alpha_m \in f^{-m}(a)$, then

$$\prod_{\alpha_{m+r} \in f^{-r}(\alpha_m)} (\alpha_{m+r} + c) \in K_{m+r}^{\times p}. \tag{4}$$

The numbers $\alpha_{m+r} + c$ in the product are the zeros of the polynomial $f^r(x-c) - \alpha_m$. Their product is $(-1)^{p^r}$ times the constant term, so the product is

$$(-1)^{p^r}(f^r(-c) - \alpha_m) = (-1)^{p^r}(t^p - c - \alpha_m) = ((-1)^{p^{r-1}} t)^p \left(1 - \frac{c + \alpha_m}{t^p}\right), \tag{5}$$

where $t := f^{r-1}(-c)$. We have $v(t) = p^{r-1}v(c)$, and $v(c + \alpha_m) \geq v(c)$, so $v((c + \alpha_m)/t^p) \geq v(c) - p^r v(c) > p/(p-1)$. Thus, by Lemma 6.3 over K_{m+r}, the second factor on the right of (5) is a pth power in K_{m+r} (as is the first). This proves (4).

Applying (4) to the p^m numbers $\alpha_m \in f^{-m}(a)$ shows that K_{m+r+1} is obtained from K_{m+r} by adjoining at most $p^m(p^r - 1)$ roots, so

$$[K_{m+r+1} : K_{m+r}] \leq p^{p^m(p^r-1)} = p^{p^{m+r}(1-p^{-r})}.$$

Thus if $n \geq m_0 + r$,

$$[K_n : K] \leq [K_{m_0+r} : K] \prod_{s=m_0+r}^{n-1} p^{p^s(1-p^{-r})} \leq C B_n^{1-p^{-r}}$$

for some C. □

7. Nonnegative valuation

In this section, we treat the tame and wild cases in which $v(c) \geq 0$. Fix an arbitrary sequence of preimages $(\alpha_n)_{n \geq 0}$ defined by $\alpha_0 := a$ and $\alpha_{n+1} \in f^{-1}(\alpha_n)$ for $n \geq 0$. Let $(\beta_n)_{n \geq 0}$ be another such sequence; if $a + c \neq 0$, we may assume that $\beta_1 \neq \alpha_1$. For $n \geq 0$, let $d_n = \alpha_n - \beta_n$.

Lemma 7.1. *If $v(c) \geq 0$ and $\min\{v(a), v(c)\} \neq 0$ and $v(a) \neq v(c)$, then K_∞/K is infinitely ramified.*

Proof. We prove $v(\alpha_n) = \min\{v(a), v(c)\}/\ell^n < v(c)$ for $n \geq 1$ by induction. The equation $\alpha_1^\ell - c = a$ implies that $v(\alpha_1) = \min\{v(a), v(c)\}/\ell < v(c)$. If the statement is true for a given $n \geq 1$, then the equation $\alpha_{n+1}^\ell - c = \alpha_n$ implies $v(\alpha_{n+1}) = v(\alpha_n)/\ell$, so $v(\alpha_{n+1}) = \min\{v(a), v(c)\}/\ell^{n+1} < v(c)$. Thus the denominator of $v(\alpha_n)$ tends to infinity, so K_∞/K is infinitely ramified. □

7.1. **Wild case.**

We now assume that $\ell = p$ (and $v(c) \geq 0$). The following will be used to prove the main result of this section, Theorem 7.3.

Lemma 7.2. *If $\ell = p$ and $v(c) > 0$ and $v(a) = 0$, then K_∞/K is infinitely wildly ramified.*

Proof. First, $v(d_1) = 1/(p-1)$ by Lemma 3.1(b) with $d = d_0$ and $y = \alpha_1$. Then $v(d_n) = v(d_1)/p^{n-1}$ by induction on n, by Lemma 3.1(a) with $d = d_{n-1}$ and $y = \alpha_n$. Thus the denominator of $v(d_n)$ tends to infinity, so K_∞/K is infinitely ramified. □

Theorem 7.3. *If $\ell = p$ and $v(c) \geq 0$, then K_∞/K is infinitely wildly ramified.*

Proof. Lemmas 7.1 and 7.2 apply unless $v(a) > v(c) = 0$ or $v(a) = v(c) \geq 0$. If $v(a) > v(c) = 0$, then $v(\alpha_1) = 0$. So by replacing a by α_1 if necessary, we may assume that $v(a) = 0$. Thus it remains to consider the case $v(a) = v(c) \geq 0$. If any iterated preimage of a has valuation not $v(c)$, then we reduce to a previous case.

So assume that $v(\alpha_n) = v(c)$ for all $n \geq 1$. We now prove $v(d_n) = (v(c) + 1/(p-1))/p^{n-1}$ for $n \geq 1$ by induction. First, $v(d_0) = \infty > \ell v(\alpha_1) - \nu_\infty$, so Lemma 3.1(b) implies $v(d_1) = v(\alpha_1) + 1/(p-1) = v(c) + 1/(p-1) > 0$. Next, for $n \geq 2$, by the inductive hypothesis, $v(d_{n-1}) \leq v(d_1) \leq pv(c) + p/(p-1) = pv(\alpha_n) - \nu_\infty$, so Lemma 3.1(a) implies $v(d_n) = v(d_{n-1})/p = (v(c)+1/(p-1))/p^{n-1}$. Thus the denominator of $v(d_n)$ tends to infinity, so K_∞/K is infinitely ramified. □

7.2. **Tame case.** We now assume that $p \nmid \ell$ (and $v(c) \geq 0$). Lemma 7.1 handles the case where $v(a) < 0$, and Theorem 7.4 below will handle the case where $v(a) \geq 0$. Let $\mathfrak{m}$ (resp. $\mathfrak{m}_s$) be the maximal ideal of the valuation ring in K (resp. K_s).

Theorem 7.4. *Suppose that $v(c) \geq 0$ and $v(a) \geq 0$.*

(a) *If $a \bmod \mathfrak{m}$ is not in the forward orbit of $0 \bmod \mathfrak{m}$, then K_∞/K is unramified.*
(b) *If $0 \bmod \mathfrak{m}$ is strictly preperiodic mod $\mathfrak{m}$, then the ramification index of K_∞/K divides ℓ.*
(c) *If 0 and a are in a single cycle, then K_∞/K is unramified.*
(d) *If $0 \bmod \mathfrak{m}$ and $a \bmod \mathfrak{m}$ are in a single cycle mod $\mathfrak{m}$, but 0 and a are not both in a single cycle, then K_∞/K is infinitely ramified.*

Parts (a) and (b) cover the cases where $0 \bmod \mathfrak{m}$ and $a \bmod \mathfrak{m}$ are *not* in a single cycle mod $\mathfrak{m}$. Parts (c) and (d) cover the cases where $0 \bmod \mathfrak{m}$ and $a \bmod \mathfrak{m}$ *are* in a single cycle mod $\mathfrak{m}$.

Proof.

(a) In taking preimages, we are taking ℓth roots of units only, so the extensions are unramified.
(b) For any sequence of preimages $(\alpha_n)_{n\geq 0}$ with $\alpha_0 = a$ and $f(\alpha_{n+1}) = \alpha_n$ for all n, the extension $K(\alpha_0, \alpha_1, \ldots)$ is tamely ramified of ramification index dividing ℓ, since the sequence is obtained by adjoining ℓth roots of elements such that at most one of them is a non-unit (otherwise $0 \bmod \mathfrak{m}$ would have been periodic). The field K_∞ is the compositum of these extensions, so it too is tamely ramified of ramification index dividing ℓ.
(c) Let C_0 be the cycle containing 0 and a. Let n be the length of C_0. Let $\alpha \in C_0$. Then $(f^n)'(\alpha) = \prod_{\beta \in C_0} f'(\beta) = 0$, since $f'(0) = 0$. Thus the derivative of $f^n(x) - x$ at α is -1. By Hensel's lemma, $f^n(x) - x$ has a unique solution in K congruent to α modulo $\mathfrak{m}$. This applies to every $\alpha \in C_0$, so the elements of C_0 are distinct modulo $\mathfrak{m}$.

    Suppose that $\beta \in K_s$ is an iterated preimage of a. Since $a \in C_0$, there exists $r \geq 0$ such that $f^r(\beta) \in C_0$. We claim that if $\beta \equiv \alpha \pmod{\mathfrak{m}_s}$ for some $\alpha \in C_0$, then $\beta = \alpha$. We use induction on r. If $r = 0$, then $\beta \in C_0$, so the previous paragraph implies that $\beta = \alpha$. If $r \geq 1$, then the inductive hypothesis applied to $f(\beta) \equiv f(\alpha) \pmod{\mathfrak{m}_s}$ shows that $f(\beta) = f(\alpha)$. Then $\beta = \zeta\alpha$ for some ℓth root of unity ζ. Thus $\zeta\alpha \equiv \alpha \pmod{\mathfrak{m}_s}$. If $\alpha \equiv 0 \pmod{\mathfrak{m}_s}$, then $\alpha = 0$ by the previous paragraph, so $\beta = \zeta\alpha = 0 = \alpha$. Otherwise, $\zeta \equiv 1 \pmod{\mathfrak{m}_s}$. Since $\ell \neq \operatorname{char} k$, this implies $\zeta = 1$, so $\beta = \alpha$.

The claim shows that all iterated preimages of a that are 0 mod $\mathfrak{m}_s$ are equal to 0. Thus in taking preimages, we are taking ℓth roots of units and 0 only, so the extensions are unramified.

(d) Let m be the period of 0 mod $\mathfrak{m}$. The derivative of $f^m(x)-x$ mod $\mathfrak{m}$ at 0 is -1, a unit, so by Hensel's lemma, there is a unique solution to $f^m(x)-x=0$ that reduces to 0 mod $\mathfrak{m}$; call it b.

Since 0 mod $\mathfrak{m}$ and a mod $\mathfrak{m}$ are in a single cycle mod $\mathfrak{m}$, we may choose a sequence of preimages (α_n) (with $\alpha_0 = a$ and $f(\alpha_{n+1}) = \alpha_n$ for all n) such that $\alpha_n \equiv 0 \bmod \mathfrak{m}_s$ for infinitely many n. We may assume that no α_n is equal to b: choose the α_i one at a time, and if one of them is b, multiply it by a nontrivial ℓth root of unity before proceeding; this changes it because if $\alpha_i = b = 0$, then 0 is periodic (since b is) and a is in the forward orbit of 0 (since a is in the forward orbit of α_i, but then 0 and a would belong to a single cycle, contradicting our hypothesis). Let $\beta_0, \beta_1, \ldots$ be all the numbers in the sequence (α_n) that are 0 mod $\mathfrak{m}_s$. Thus $f^m(\beta_{i+1}) = \beta_i$ for all i.

We now prove that $0 < v(\beta_{i+1} - b) < v(\beta_i - b)$ for all i. Let $\epsilon = \beta_{i+1} - b$, so $v(\epsilon) > 0$. We have $f^m(b+x) = b + (f^m)'(b)x + x^2R(x)$ for some $R(x) \in \mathcal{O}[x]$. Substituting $x = \epsilon$ yields $\beta_i = b + (f^m)'(b)\epsilon \pmod{\epsilon^2}$. Since $v(\epsilon) > 0$ and $v((f^m)'(b)) > 0$, we obtain $v(\beta_i - b) > v(\epsilon) = v(\beta_{i+1} - b) > 0$.

This holds for all i, so K_∞/K is infinitely ramified. □

8. Real case

Theorem 8.1. *Let $f(z) = z^k - c \in \mathbb{R}[z]$ for some $k \geq 2$ and $c \in \mathbb{R}^\times$. Given $a \in \mathbb{R}$, define K_n and K_∞ as before.*

(a) *If $k > 2$, then $K_\infty = \mathbb{C}$.*
(b) *If $k = 2$ and $c < 2$, then $K_\infty = \mathbb{C}$.*
(c) *If $k = 2$ and $c \geq 2$, then K_∞ is $\mathbb{R}$ or $\mathbb{C}$ according to whether $a \in [-c, c^2 - c]$ or not, respectively.*

Proof.

(a) There exists a nonzero $\beta \in f^{-n}(c)$ for some $n \geq 1$, since otherwise $c = 0$. Then for every kth root of unity ζ, we have $\zeta\beta \in f^{-n}(c)$ too, so $\zeta = (\zeta\beta)/\beta \in K_\infty$. Thus $K_\infty = \mathbb{C}$.

(b) Let $h(x) := \sqrt{c+x}$; if $x \geq -c$, take the nonnegative square root. Thus $h(x)$ is strictly increasing on $[-c, \infty)$.

Suppose that $K_\infty = \mathbb{R}$. Then all iterated preimages are real, and in particular, $h^n(a) \in \mathbb{R}_{\geq 0}$ for all $n \geq 0$. Also $c - h^n(a) \geq 0$ for all $n \geq 1$, since $-h^n(a)$ is a preimage of $h^{n-1}(a)$, and $h(-h^n(a)) = \sqrt{c - h^n(a)}$. In particular, $c \geq c - h(a) \geq 0$. We assumed $c \neq 0$, so $c > 0$.

The fixed points of $f(z)$ are $L := (1 + \sqrt{1+4c})/2 > 0$ and $L' := (1 - \sqrt{1+4c})/2 < 0$. The only solution to $h(x) = x$ in $[0, \infty)$ is L, and h is strictly increasing, and $h(0) > 0$ and $h(x) < x$ for large positive x; thus $x < h(x) \leq L$ for $x \in [0, L]$, and $L \leq h(x) < x$ for $x \in [L, \infty)$. In particular, $(h^n(a))_{n \geq 1}$ is a bounded monotonic sequence, so it converges. The limit is a nonnegative fixed point of hh, so the limit is L.

On the other hand, the hypothesis $c < 2$ implies that $L > c$, so $h^n(a) > c$ for sufficiently large n. This contradicts $c - h^n(a) \geq 0$.

(c) The hypothesis $c \geq 2$ implies that $L \leq c$. If $x \in [-c, c^2 - c]$, then $c + x \geq 0$, and $\sqrt{c+x} \leq \sqrt{c^2} = c$; also, $c \leq c^2 - c$, so $h(x), -h(x) \in [-c, c^2 - c]$. Iterating shows that if $a \in [-c, c^2 - c]$, then all iterated preimages are real, so $K_\infty = \mathbb{R}$.

If $a < -c$, then $h(a) \notin \mathbb{R}$, so $K_\infty = \mathbb{C}$.

If $a > c^2 - c$, then $h(a) > c$, contradicting the inequality $c - h(a) \geq 0$ derived in the proof of (b), so $K_\infty = \mathbb{C}$. □

Acknowledgements

We thank Robert L. Benedetto, Robert Harron, and Yevgeny Zaytman. This research began at the workshop "The Galois theory of orbits in arithmetic dynamics" organized by Rafe Jones, Michelle Manes, and Joseph Silverman at the American Institute of Mathematics.

References

[BJ07] Nigel Boston and Rafe Jones, *Arboreal Galois representations*, Geom. Dedicata **124** (2007), 27–35, DOI 10.1007/s10711-006-9113-9. MR2318536

[BJ09] Nigel Boston and Rafe Jones, *The image of an arboreal Galois representation*, Pure Appl. Math. Q. **5** (2009), no. 1, 213–225, DOI 10.4310/PAMQ.2009.v5.n1.a6. MR2520459

[Hin16] Wade Hindes, *Average Zsigmondy sets, dynamical Galois groups, and the Kodaira–Spencer map*, March 14, 2016. Preprint, `arXiv:1603.04459v1`.

[Ing13] Patrick Ingram, *Arboreal Galois representations and uniformization of polynomial dynamics*, Bull. Lond. Math. Soc. **45** (2013), no. 2, 301–308, DOI 10.1112/blms/bds088. MR3064415

[Jon08] Rafe Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. Lond. Math. Soc. (2) **78** (2008), no. 2, 523–544, DOI 10.1112/jlms/jdn034. MR2439638

[Jon13] Rafe Jones, *Galois representations from pre-image trees: an arboreal survey*, Actes de la Conférence "Théorie des Nombres et Applications", Publ. Math. Besançon Algèbre Théorie Nr., Presses Univ. Franche-Comté, Besançon, 2013, pp. 107–136 (English, with English and French summaries). MR3220023

[JM14] Rafe Jones and Michelle Manes, *Galois theory of quadratic rational functions*, Comment. Math. Helv. **89** (2014), no. 1, 173–213, DOI 10.4171/CMH/316. MR3177912

[Kat86] Nicholas M. Katz, *Local-to-global extensions of representations of fundamental groups*, Ann. Inst. Fourier (Grenoble) **36** (1986), no. 4, 69–106 (English, with French summary). MR867916

[Odo85a] R. W. K. Odoni, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc. (2) **32** (1985), no. 1, 1–11, DOI 10.1112/jlms/s2-32.1.1. MR813379

[Odo85b] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414, DOI 10.1112/plms/s3-51.3.385. MR805714

[Odo97] R. W. K. Odoni, *On the Galois groups of iterated generic additive polynomials*, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 1, 1–6, DOI 10.1017/S0305004196001168. MR1418355

[Sen72] Shankar Sen, *Ramification in p-adic Lie extensions*, Invent. Math. **17** (1972), 44–50. MR0319949

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[Sto92] Michael Stoll, *Galois groups over* $\mathbf{Q}$ *of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244, DOI 10.1007/BF01197321. MR1174401

Mathematics Department, Bridgewater State University, Bridgewater, MA 02325, USA
E-mail address: jacqueline.anderson@bridgew.edu

McDaniel College, 2 College Hill, Westminster, MD 21157
E-mail address: shamblen@mcdaniel.edu

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
E-mail address: poonen@math.mit.edu
URL: http://math.mit.edu/~poonen/

Mathematics Department, Brown University, Providence, RI 02912, USA
E-mail address: laura@math.brown.edu