Algebra & Number Theory

Volume 14
2020
No. 7

Abelian extensions in dynamical Galois theory

Jesse Andrews and Clayton Petsche

msp

msp

ALGEBRA AND NUMBER THEORY 14:7 (2020)
https://doi.org/10.2140/ant.2020.14.1981

Abelian extensions in dynamical Galois theory

Jesse Andrews and Clayton Petsche

We propose a conjectural characterization of when the dynamical Galois group associated to a polynomial is abelian, and we prove our conjecture in several cases, including the stable quadratic case over $\mathbb{Q}$. In the postcritically infinite case, the proof uses algebraic techniques, including a result concerning ramification in towers of cyclic p-extensions. In the postcritically finite case, the proof uses the theory of heights together with results of Amoroso and Zannier and Amoroso and Dvornicich, as well as properties of the Arakelov–Zhang pairing.

1. Introduction

Let K be a number field with algebraic closure $\overline{K}$. Let $\phi(x) \in K[x]$ be a polynomial of degree $d \geq 2$, and denote by $\phi^n = \phi \circ \cdots \circ \phi$ the n-fold composition of ϕ with itself. Let $\alpha \in K$ be a nonexceptional point for ϕ; that is, assume that the backward orbit $\{\beta \in \overline{K} \mid \phi^n(\beta) = \alpha \text{ for some } n \geq 0\}$ of α is an infinite set.

For each $n \geq 1$, define the n-th inverse image set of the pair (ϕ, α) by

$$\phi^{-n}(\alpha) = \{\beta \in \overline{K} \mid \phi^n(\beta) = \alpha\},$$

and let $K_n = K_n(\phi, \alpha)$ be the field generated over K by $\phi^{-n}(\alpha)$. Since the generators of K_n are ϕ-images of generators of K_{n+1}, we obtain a tower $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots$ of Galois extensions of K. Set $K_\infty = \bigcup_{n \geq 0} K_n$.

As described for example in [Jones 2013], $\mathrm{Gal}(K_n/K)$ acts faithfully on the n-th preimage tree $T_n = T_n(\phi, \alpha)$ associated to the pair (ϕ, α), which can be described as follows. For each $0 \leq m \leq n$, the level-m vertices of T_n are indexed by the elements of $\phi^{-m}(\alpha)$, and edge relations on T_n are determined by ϕ-evaluation. In the limit as $n \to +\infty$, $\mathrm{Gal}(K_\infty/K)$ acts faithfully on $T_\infty = \bigcup T_n$, and we obtain the arboreal Galois representations

$$\begin{aligned} \rho_n &: \mathrm{Gal}(K_n/K) \hookrightarrow \mathrm{Aut}(T_n) \\ \rho &: \mathrm{Gal}(K_\infty/K) \hookrightarrow \mathrm{Aut}(T_\infty). \end{aligned} \tag{1}$$

The study of the representations (1) goes back to Odoni [1985a; 1985b; 1988; 1997] and Stoll [1992], and has found renewed interest due to a series of papers by Boston [2000], Boston and Jones [2007; 2009] and Jones [2005; 2007; 2008; 2013]. Much of the current research in this area focuses on identifying

MSC2010: primary 11R32; secondary 11G50, 11R18, 37P30.

Keywords: arithmetic dynamics, dynamical Galois theory, arboreal representations, Weil height, small points, Arakelov–Zhang pairing.

cases in which $\mathrm{Gal}(K_\infty/K)$ is large in the sense that the arboreal Galois representation ρ is surjective, or has image with finite index in $\mathrm{Aut}(T_\infty)$.

Assume for now that the pair (ϕ, α) is *stable*, that is that the $\mathrm{Gal}(K_n/K)$-action on $\phi^{-n}(\alpha)$ is transitive for each $n \geq 1$; this is equivalent to the irreducibility of $\phi^n(x) - \alpha$ for all $n \geq 1$. In this case, each T_n is the complete d-ary rooted tree of level n, so using transitivity and comparing with the size of $\mathrm{Aut}(T_n)$, it follows from the injectivity of (1) that

$$d^n \leq |\mathrm{Gal}(K_n/K)| \leq d!^{(d^n-1)/(d-1)} \tag{2}$$

for all n. Examples in which the upper bound in (2) is achieved for all $n \geq 1$ have been identified by Odoni [1985b] and Stoll [1992] in degree $d = 2$, by Looper [2019] in every prime degree, and by Specter [2018] in arbitrary degree.

In the opposite direction, let us say that a pair (ϕ, α) is *minimally stable* if it is stable, and the lower bound in (2) is achieved for all $n \geq 1$. For example, let $K = \mathbb{Q}$, $\phi(x) = x^2$, and $\alpha = -1$. This pair (ϕ, α) is stable, indeed $\phi^n(x) - \alpha = x^{2^n} + 1$ is the 2^{n+1}-th cyclotomic polynomial and hence is irreducible over $\mathbb{Q}$, and $|\mathrm{Gal}(K_n/\mathbb{Q})| = [K_n : \mathbb{Q}] = 2^n$. Since $K_\infty/\mathbb{Q}$ is cyclotomic, $\mathrm{Gal}(K_\infty/\mathbb{Q})$ is abelian. (In fact $\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \mathbb{Z}_2^\times \simeq \{\pm\} \times \mathbb{Z}_2$.)

More generally, an elementary argument shows that if the pair (ϕ, α) is stable and $\mathrm{Gal}(K_\infty/K)$ is abelian, then (ϕ, α) is minimally stable; see Lemma 2. We do not know whether the converse is true; i.e., whether the only minimally stable pairs (ϕ, α) are those for which $\mathrm{Gal}(K_\infty/K)$ is abelian. We do not directly address this question here. Instead, in this paper we consider the following question: for precisely which pairs (ϕ, α) is $\mathrm{Gal}(K_\infty/K)$ abelian? In the stable case, this is closely related to the question of characterizing minimally stable pairs (ϕ, α), but the question makes sense even in the absence of a stability hypothesis. We conjecture that in general, $\mathrm{Gal}(K_\infty/K)$ is abelian only in cases related to the powering map example described above, or to similar examples arising from Chebyshev polynomials.

Given a field extension L/K, we say the pair (ϕ, α) is *conjugate* over L to the pair (ψ, β) if there exists an affine transformation $\gamma(x) = ax + b$ defined over L such that $\psi = \gamma \circ \phi \circ \gamma^{-1}$ and $\beta = \gamma(\alpha)$. It is not hard to see that if (ϕ, α) and (ψ, β) are conjugate over K, then $K_\infty(\phi, \alpha) = K_\infty(\psi, \beta)$. But for us, the more important fact is that whether or not $\mathrm{Gal}(K_\infty(\phi, \alpha)/K)$ is abelian is an invariant of the K^{ab}-conjugacy class of the pair (ϕ, α), where K^{ab} is the maximal abelian extension of K in $\overline{K}$; see Proposition 11.

Conjecture. *Let K be a number field, let $\phi(x) \in K[x]$ be a polynomial of degree $d \geq 2$, let $\alpha \in K$, and assume that α is not an exceptional point for ϕ. Then $K_\infty(\phi, \alpha)/K$ is an abelian extension if and only if the pair (ϕ, α) is K^{ab}-conjugate to the pair (ψ, β) occurring in one of the following two families of examples*:

(i) *$\psi(x) = x^d$ and $\beta = \zeta$, a root of unity in $\overline{K}$.*

(ii) *$\psi(x) = T_d(x)$ is the d-th Chebyshev polynomial and $\beta = \zeta + \zeta^{-1}$, where ζ is a root of unity in $\overline{K}$.*

As a special case, when $K = \mathbb{Q}$ and $d = 2$, we recall the well-known fact that every quadratic polynomial over $\mathbb{Q}$ is $\overline{\mathbb{Q}}$-conjugate to $x^2 + c$ for a unique $c \in \mathbb{Q}$, and moreover any such $\overline{\mathbb{Q}}$-conjugacy is actually defined over $\mathbb{Q}$. Thus the Conjecture asserts in this case that for a pair (ϕ, α) defined over $\mathbb{Q}$ with $\deg(\phi) = 2$, the extension $K_\infty(\phi, \alpha)/\mathbb{Q}$ is abelian if and only if (ϕ, α) is $\mathbb{Q}$-conjugate to $(x^2, \pm 1)$ or $(x^2 - 2, \beta)$ for $\beta = 0, \pm 1, \pm 2$.

We prove partial results toward the Conjecture which can be divided into three main categories. First, we prove the Conjecture in the quadratic, stable, postcritically infinite case (Theorem 8). (Recall that a quadratic polynomial $\phi(x)$ is said to be *postcritically finite* if its critical point is ϕ-preperiodic; otherwise it is postcritically infinite.) The main ideas in this proof are algebraic, and culminate in showing under the above hypotheses that if K_∞/K were abelian, then no primes of K with odd residue characteristic would ramify in K_∞, in contradiction with a result of Bridy et al. [2017] on arbitrary postcritically infinite maps.

Next, we prove the Conjecture for polynomials ϕ which are $\overline{K}$-conjugate to either a powering map or a Chebyshev map (Theorems 12 and 13). These proofs use the theory of heights together with a result of Amoroso and Zannier [2000] (generalizing a result of Amoroso and Dvornicich [2000]), giving a lower bound on the heights of elements in abelian extensions of number fields. Notably, the results on powering and Chebyshev maps do not require a stability hypothesis.

Finally, we treat the particular postcritically finite map $\phi(x) = x^2 - 1$. Using a combination of the ramification techniques of Theorem 8 with the height techniques of Theorems 12 and 13 (and in particular a lower bound on the height in certain cyclotomic extensions due to Amoroso and Dvornicich [2000]), we prove the Conjecture for stable pairs $(x^2 - 1, \alpha)$ over $\mathbb{Q}$. We point out that the proof of this result is computer-assisted, in the sense that the key step in the proof is to numerically calculate the Arakelov–Zhang pairing $\langle x^2 - 1, x^2 \rangle$ with enough precision to show that it is less than the Bogomolov constant of the maximal abelian extension of $\mathbb{Q}$ unramified at all odd primes. In particular, we use SageMath to calculate a sum of elementary approximations to local height functions evaluated at roots of unity.

Combining these results, and using the well known fact that every quadratic polynomial over $\mathbb{Q}$ is either postcritically infinite or else $\mathbb{Q}$-conjugate to either the squaring map x^2, the Chebyshev map $x^2 - 2$, or $x^2 - 1$, we obtain the following.

Theorem 1. *The Conjecture is true for all quadratic stable pairs (ϕ, α) over $\mathbb{Q}$.*

It is well-known that any iterate of an Eisenstein polynomial in $\mathbb{Z}[x]$ is again Eisenstein, so the pair $(\phi(x), 0)$ is stable whenever $\phi(x) \in \mathbb{Z}[x]$ is Eisenstein. Using this observation, we can give the following simple examples to show that in each of the cases described above, stable pairs $(x^2 + c, \alpha)$ exist over $\mathbb{Q}$ and hence Theorem 1 is nonvacuous in each case:

(i) For any prime p, the (postcritically infinite) pair $(x^2 + p, 0)$ is stable.

(ii) If $\alpha \in \mathbb{Z}$ and $\alpha \equiv 2$ or $3 \pmod 4$, then the squaring pair (x^2, α) is stable, since it is conjugate to $(x^2 + 2\alpha x + \alpha^2 - \alpha, 0)$, which is 2-Eisenstein. Note that this family includes both abelian examples, such as $(x^2, -1)$, and nonabelian examples, such as $(x^2, 3)$.

(iii) If $\alpha \in \mathbb{Z}$ and $\alpha \equiv 0$ or $1 \pmod 4$, then the Chebyshev pair (x^2-2, α) is stable, since it is conjugate to $(x^2+2\alpha x+\alpha^2-\alpha-2, 0)$, which is 2-Eisenstein. Note that this family includes both abelian examples, such as $(x^2-2, 0)$, and nonabelian examples, such as $(x^2-2, 4)$.

(iv) This example was shown to us by Chifan Leung. If $\alpha \in \mathbb{Z}$ and $\alpha \equiv 1$ or $2 \pmod 4$, then the pair (x^2-1, α) is stable. It suffices to show that (ϕ^2, α) is stable, where $\phi(x) = x^2-1$ and $\phi^2(x) = x^4-2x^2$, since the irreducibility of $\phi^{2n}(x)-\alpha$ implies the irreducibility of $\phi^{2n-1}(x)-\alpha$. The stability of (ϕ^2, α) follows from the fact that it is conjugate to $(\phi^2(x+\alpha)-\alpha, 0)$, which is easily checked to be 2-Eisenstein. (See also [Ahmad et al. 2019] for a study of large-image results for arboreal Galois representations associated to $\phi(x) = x^2-1$.)

While this paper was under review, A. Ferraguti and C. Pagano [2020] informed us that they have used an entirely different approach to give a complete proof of the $K = \mathbb{Q}$, $d = 2$ case of the Conjecture (not requiring any stability assumption).

The plan of this paper is as follows. In Section 2 we prove some preliminary algebraic lemmas, and in Section 3 we prove the Conjecture in the quadratic, stable, postcritically infinite case. In Section 4 we review the absolute Weil height function defined on algebraic extensions of $\mathbb{Q}$, we recall the concept of the Bogomolov constant associated to such fields, and we describe related results of Amoroso and Zannier [2000] and Amoroso and Dvornicich [2000]. In Section 5 we prove the Conjecture for powering maps and Chebyshev maps. In Section 6 we review the definition and basic facts about the Arakelov–Zhang pairing, and in Sections 7 and 8 we treat the particular polynomial $\phi(x) = x^2-1$, calculate the Arakelov–Zhang pairing $\langle x^2-1, x^2\rangle$, and prove the Conjecture for stable pairs (x^2-1, α) over $\mathbb{Q}$.

2. Some algebraic lemmas

Lemma 2. *Let G be a finite abelian group acting faithfully and transitively on a finite set X. Then $|G| = |X|$.*

Proof. For each $x \in X$, let G_x be the stabilizer of x. Then $G_x = G_y$ for all $x, y \in X$. Indeed, writing $y = gx$ for $g \in G$, if $h \in G_x$ then $hy = hgx = ghx = gx = y$, showing that $h \in G_y$ as well. Thus $G_x \subseteq G_y$, and $G_x = G_y$ follows from symmetry. Since the action is faithful, we have $\bigcap_{x\in X} G_x = \{1\}$, and since the stabilizers are all equal to each other we conclude that $G_x = \{1\}$ for all $x \in X$. Therefore $|X| = (G : G_x) = (G : 1) = |G|$ by the orbit stabilizer theorem. □

Lemma 3. *If G is an abelian, transitive subgroup of S_N and if $\sigma \in G$ is an element of order ℓ, then $\sigma = c_1 c_2 \cdots c_r$ for some r disjoint ℓ-cycles $c_1, c_2, \ldots, c_r$, where $r = N/\ell$.*

Proof. Recall the standard calculation that if $(i_1 \cdots i_\ell) \in S_N$ is a cycle and if $\tau \in S_N$, then $\tau(i_1 \cdots i_\ell)\tau^{-1} = (\tau(i_1) \cdots \tau(i_\ell))$.

We may write $\sigma = c_1 c_2 \cdots c_r$ for some r disjoint cycles $c_1, c_2, \ldots, c_r$ of lengths $\ell_1, \ell_2, \ldots, \ell_r$, respectively, and this decomposition is unique up to ordering. If necessary, interpreting some of the cycles c_j to be 1-cycles, we may assume that every element of $\{1, 2, \ldots, N\}$ occurs in precisely one of the cycles c_j.

Fix $2 \le j \le r$. By transitivity, select $\tau \in G$ taking some element of $\{1, 2, \dots, N\}$ occurring in the cycle c_j to some element occurring in the cycle c_1. Since G is abelian,

$$\sigma = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \cdots (\tau c_r \tau^{-1}),$$

and so by uniqueness of the disjoint cycle decomposition of σ, we conclude that $c_1 = \tau c_j \tau^{-1}$. In particular, all of the cycles c_j have the same length ℓ_1, which must then be equal to the order ℓ of σ. Finally, $r\ell = N$, as every element of $\{1, 2, \dots, N\}$ occurs in precisely one of the cycles c_j. □

Lemma 4. *Let G be an abelian, transitive subgroup of S_{2^n} which is not a subgroup of A_{2^n}. Then G is cyclic.*

Proof. By Lemma 2, we have $|G| = 2^n$. Let $\sigma \in G$ be an odd permutation of order ℓ; thus $\ell \ge 2$ is a power of 2. By Lemma 3, we have a decomposition $\sigma = c_1 c_2 \cdots c_r$ into disjoint ℓ-cycles c_j, and $r\ell = 2^n$. Since ℓ is even, $\operatorname{sgn}(c_j) = -1$ for all j, and therefore

$$-1 = \operatorname{sgn}(\sigma) = \prod_{1 \le j \le r} \operatorname{sgn}(c_j) = (-1)^r.$$

Thus r is odd, and as $r\ell = 2^n$, we must have $r = 1$. We conclude that $\sigma = c_1$ is a 2^n-cycle and hence that $G = \langle\sigma\rangle$ is cyclic. □

The assumption that $G \not\subseteq A_{2^n}$ cannot be omitted. For example, the order 8 subgroup $G = \langle\sigma, \tau\rangle$ of A_8 generated by the (commuting) permutations $\sigma = (1537)(2648)$ and $\tau = (12)(34)(56)(78)$ is abelian and transitive, but not cyclic. We also point out that this counterexample cannot be removed using properties of tree automorphisms, as we may view G as a subgroup of the automorphism group of a binary rooted tree of level 3, by embedding the tree in the usual way in the plane and labeling the level-3 vertices by the numbers $1, \dots, 8$ from left to right.

Lemma 5. *Let $f(x) = Ax^2 + Bx + C \in K[x]$ be a quadratic polynomial, and let $c = -B/2A$ be its critical point. Then for all $n \ge 1$,*

$$\operatorname{disc}(f^n) = (-1)^{2^{n-1}} 2^{2^n} A^{2^{2n-1}-1} \operatorname{disc}(f^{n-1})^2 f^n(c). \tag{3}$$

This identity is worked out (in greater generality) up to sign by Jones [2008, Lemma 2.6]; it is straightforward to go through Jones' calculation and keep track of the factor $(-1)^{2^{n-1}}$, which of course is -1 when $n = 1$ and $+1$ when $n \ge 2$. To check (3) when $n = 1$, take $f^0(x) = x$ and hence $\operatorname{disc}(f^0) = 1$, which is reasonable as one typically interprets the empty product to be 1. In this case, the right-hand side of (3) simplifies to $-4Af(c) = B^2 - 4AC$, as expected.

3. Ramification and postcritically infinite quadratic maps

We recall standard facts and notation surrounding a finite Galois extension L/K of number fields; see Lang [1970, Chapter 1]. Given a prime $\mathfrak{p}$ of K, by the Galois assumption we have a factorization of the form $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^e \cdots \mathfrak{q}_r^e$ for primes $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ of L, and $ref = [L : K]$, where $e = e(\mathfrak{q}_i/\mathfrak{p})$ and $f = f(\mathfrak{q}_i/\mathfrak{p})$

are the (common) ramification indices and inertial degrees of the $\mathfrak{q}_i$, respectively. Moreover, each $\mathcal{O}_L/\mathfrak{q}_i$ is a degree f extension of $\mathcal{O}_K/\mathfrak{p}$. For each $1 \le i \le r$, let

$$D_{\mathfrak{q}_i/\mathfrak{p}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{q}_i) = \mathfrak{q}_i\}$$
$$I_{\mathfrak{q}_i/\mathfrak{p}} = \{\sigma \in D_{\mathfrak{q}_i/\mathfrak{p}} \mid \sigma(x) \equiv x \pmod{\mathfrak{q}_i} \text{ for all } x \in \mathcal{O}_L\}$$

be the associated decomposition and inertia groups. Thus $I_{\mathfrak{q}_i/\mathfrak{p}}$ has order $e(\mathfrak{q}_i/\mathfrak{p})$, $\mathfrak{p}$ is unramified in $L^{I_{\mathfrak{q}_i/\mathfrak{p}}}$, and if $\mathfrak{p}'$ denotes any prime of $L^{I_{\mathfrak{q}_i/\mathfrak{p}}}$ lying over $\mathfrak{p}$, then $\mathfrak{p}'$ is totally ramified in L.

Lemma 6. *Let L/K be a Galois extension of number fields and let $\mathfrak{p}$ be a prime of K which is tamely ramified in L. Let $\mathfrak{q}$ be a prime of L lying over $\mathfrak{p}$. Then*

$$e(\mathfrak{q}/\mathfrak{p}) \le |\mathcal{O}_K/\mathfrak{p}|^{f(\mathfrak{q}/\mathfrak{p})} - 1.$$

Proof. Let $\pi \in \mathcal{O}_L$ be a uniformizer for $\mathfrak{q}$, and consider the group homomorphism

$$I_{\mathfrak{q}/\mathfrak{p}} \to (\mathcal{O}_L/\mathfrak{q})^\times$$
$$\sigma \mapsto \sigma(\pi)/\pi \pmod{\mathfrak{q}}$$

Standard arguments from the theory of local fields show that this map does not depend on the choice of uniformizer, and the tame ramification hypothesis implies that it is injective; see [Cassels and Fröhlich 1967, Section I.8]. Together with the fact that $|\mathcal{O}_L/\mathfrak{q}| = |\mathcal{O}_K/\mathfrak{p}|^{f(\mathfrak{q}/\mathfrak{p})}$, we obtain the desired inequality. □

Lemma 7. *Let K be a number field, let $K = K_0 \subset K_1 \subset K_2 \subset \cdots$ be a tower of distinct cyclic p-extensions of K, and let $K_\infty = \bigcup K_n$. If $\mathfrak{p}$ is a prime of K with residue characteristic not equal to p, then $\mathfrak{p}$ is unramified in K_∞.*

Proof. Since a quotient of a cyclic p-group is another cyclic p-group, without loss of generality we may insert intermediate fields and reindex to ensure that $[K_n : K_{n-1}] = p$ for all $n \ge 1$. Since $\mathrm{Gal}(K_n/K)$ is a cyclic p-group, its subgroups are totally ordered by inclusion, and thus the same is true of intermediate fields $K \subseteq F \subseteq K_n$. In particular, the fields $K = K_0 \subset K_1 \subset \cdots \subset K_n$ are the only subfields of K_n containing K.

Contrary to what has been claimed, assume that $\mathfrak{p}$ has residue characteristic not equal to p and that $\mathfrak{p}$ ramifies (hence tamely ramifies) in K_∞. Let $\mathfrak{p}_0 = \mathfrak{p}$, and for each $n \ge 1$, let $\mathfrak{p}_n$ be a prime of K_n lying over $\mathfrak{p}_{n-1}$. Let n_0 be maximal with the property that $\mathfrak{p}$ is unramified in K_{n_0}; thus $\mathfrak{p}_{n_0}$ is ramified in K_{n_0+1}. Let $n > n_0$ be arbitrary, and define $F_\mathfrak{p} = K_n^{I_{\mathfrak{p}_n/\mathfrak{p}}}$, the fixed field of the inertia subgroup $I_{\mathfrak{p}_n/\mathfrak{p}}$ of $\mathrm{Gal}(K_n/K)$. In particular, $\mathfrak{p}$ is unramified in $F_\mathfrak{p}$, and if $\mathfrak{p}'$ denotes any prime of $F_\mathfrak{p}$ lying over $\mathfrak{p}$, then $\mathfrak{p}'$ is totally ramified in K_n. Since we must have $F_\mathfrak{p} = K_m$ for some $0 \le m \le n$, the only possibility is $F_\mathfrak{p} = K_{n_0}$.

To summarize, we have shown that $\mathfrak{p}$ is unramified in K_{n_0}, and that $\mathfrak{p}_{n_0}$ is totally ramified in K_n for all $n > n_0$. In particular, we have

$$\begin{aligned} f(\mathfrak{p}_n/\mathfrak{p}) = f(\mathfrak{p}_{n_0}/\mathfrak{p}) &\le [K_{n_0} : K] = p^{n_0}, \\ e(\mathfrak{p}_n/\mathfrak{p}) = e(\mathfrak{p}_n/\mathfrak{p}_{n_0}) &= [K_n : K_{n_0}] = p^{n-n_0}. \end{aligned} \tag{4}$$

But for large enough n, (4) contradicts the bound

$$e(\mathfrak{p}_n/\mathfrak{p}) \le |\mathcal{O}_K/\mathfrak{p}|^{f(\mathfrak{p}_n/\mathfrak{p})} - 1.$$

which follows from Lemma 6. □

Theorem 8. *Let $\phi(x) \in K[x]$ be a quadratic polynomial which is not postcritically finite, let $\alpha \in K$, and assume that the pair (ϕ, α) is stable. Then* $\mathrm{Gal}(K_\infty/K)$ *is nonabelian.*

Proof. Let $\phi(x) \in K[x]$ be a quadratic polynomial which is not postcritically finite, let $\alpha \in K$, assume that the pair (ϕ, α) is stable, and assume that $\mathrm{Gal}(K_\infty/K)$ is abelian; we will obtain a contradiction.

We first prove that $\mathrm{Gal}(K_n/K)$ is cyclic for all $n \ge 1$. To see this, note first that the stability and abelian hypotheses imply via Lemma 2 that $[K_n : K] = 2^n$ for all $n \ge 1$. It suffices to show that $\mathrm{Gal}(K_n/K)$ is cyclic for arbitrarily large n, because if $\mathrm{Gal}(K_n/K)$ is cyclic then so are its quotients $\mathrm{Gal}(K_m/K)$ for $1 \le m < n$. By the stability hypothesis and Lemma 4, it suffices to show, for arbitrarily large n, that $\mathrm{Gal}(K_n/K)$ is not contained in A_{2^n} when viewed as a subgroup of S_{2^n} via its action on the roots of $\phi^n(x) - \alpha$. Suppose on the contrary that $\mathrm{Gal}(K_n/K) \subseteq A_{2^n}$ for all sufficiently large n. By a well-known exercise in elementary Galois theory, this means that $\mathrm{disc}(\phi^n(x) - \alpha)$ is a square in K for all sufficiently large n. Letting $\psi(x) = \phi(x + \alpha) - \alpha$, using Lemma 5 we have

$$\mathrm{disc}(\phi^n(x) - \alpha) = \mathrm{disc}(\phi^n(x + \alpha) - \alpha) = \mathrm{disc}(\psi^n(x)) = R_n^2 A\psi^n(c)$$

for all $n \ge 2$, where $A, R_n \in K$ are nonzero and where c is the critical point of $\psi(x)$. In particular, $A\psi^n(c)$ is a square in K for all sufficiently large n.

The pair $(\psi, 0)$ is stable by the stability assumption on the pair (ϕ, α). In particular, the degree 8 polynomial $\psi^3(x)$ has eight distinct roots in $\overline{K}$, and thus $C = \{y^2 = A\psi^3(x)\}$ is a smooth hyperelliptic curve of genus 3. There are infinitely many $n \ge 3$ for which $A\psi^n(c)$ is a square in K and hence for which $\psi^{n-3}(c)$ is the x-coordinate of a K-rational point on C. Moreover, these points are distinct by the postcritically infinite hypothesis on ϕ (and hence on ψ as well). This violation of Faltings theorem provides a contradiction, and thus the assumption $\mathrm{Gal}(K_n/K) \subseteq A_{2^n}$ for all large enough n is false. As explained above, by Lemma 4 this completes the proof that $\mathrm{Gal}(K_n/K)$ is cyclic for all $n \ge 1$.

We now apply the $p = 2$ case of Lemma 7, which implies that no primes $\mathfrak{p}$ of K with odd residue characteristic can ramify in K_∞. However, this violates a theorem of Bridy et al. [2017], which states that if K_∞ is generated over K by the preimage tree associated to a postcritically infinite rational map, then infinitely many primes of K ramify in K_∞. The contradiction completes the proof of the theorem. □

The use of Falting's theorem to limit the number of squares in the critical orbit of a polynomial is borrowed from Boston and Jones [2009]. In fact, Theorem 8 may be viewed as a generalization of Theorem 3.1 of [loc. cit.], in the sense that our result implies that the hypotheses of that theorem can never be satisfied.

4. Heights and Bogomolov constants

We recall the definition of the absolute Weil height function $h : \overline{K} \to \mathbb{R}$ for a number field K. For each finite extension L/K, denote by M_L the set of places of L, and for each place v let $|\cdot|_v$ be a corresponding absolute value normalized so that it coincides with either the standard real or p-adic absolute value when restricted to $\mathbb{Q}$. Given $\alpha \in \overline{K}$, Let L/K be a finite extension containing α, and define

$$h(\alpha) = \sum_{v \in M_L} r_v \log^+ |\alpha|_v \tag{5}$$

where $r_v = [L_v : \mathbb{Q}_v]/[L : \mathbb{Q}]$ and $\log^+ t = \log \max(1, t)$. Standard arguments show that this definition is independent of the choice of L, and that $h(\alpha) \geq 0$ for all $\alpha \in \overline{K}$, with $h(\alpha) > 0$ unless α is zero or a root of unity. It is immediate from the definition that $h(\zeta\alpha) = h(\alpha)$ for all roots of unity ζ, and that $h(\alpha^n) = |n| h(\alpha)$ for all $n \in \mathbb{Z}$.

Given a field $K \subseteq L \subseteq \overline{K}$ (with L/K not necessarily a finite extension), define the Bogomolov constant of L by

$$B_0(L) = \liminf\{h(\alpha) \mid \alpha \in L \text{ and } h(\alpha) > 0\}.$$

In other words, $B_0(L)$ is the unique extended real number $[0, +\infty]$ with the property that the set $\{\alpha \in L \mid 0 < h(\alpha) \leq B\}$ is finite for all $B < B_0(L)$ and infinite for all $B > B_0(L)$.

Theorem 9 [Amoroso and Zannier 2000]. *If L/K^{ab} is a finite extension of degree $D = [L : K^{\mathrm{ab}}]$, then $h(\alpha) \geq C_{K,D} > 0$ for all nonzero, nonroot of unity $\alpha \in L$, where $C_{K,D}$ is a constant depending only on K and D. In particular, $B_0(L) \geq C_{K,D} > 0$.*

This result generalizes a result of Amoroso and Dvornicich [2000], which states that $h(\alpha) \geq (\log 5)/12$ for all nonzero, nonroot of unity $\alpha \in \mathbb{Q}^{\mathrm{ab}}$. In particular, $B_0(\mathbb{Q}^{\mathrm{ab}}) \geq (\log 5)/12$. For our purposes, another useful result from the paper [Amoroso and Dvornicich 2000] is the following. For each $k \geq 1$, let ζ_k be a primitive k-th root of unity in $\mathbb{C}$, and let μ_k be the group of all k-th roots of unity in $\mathbb{C}$. Let $\mu_{2^\infty} = \bigcup_{m \geq 1} \mu_{2^m}$; thus $\mathbb{Q}(\mu_{2^\infty}) = \bigcup_{m \geq 1} \mathbb{Q}(\zeta_{2^m})$.

Theorem 10 [Amoroso and Dvornicich 2000]. *If $\alpha \in \mathbb{Q}(\mu_{2^\infty})$ is nonzero and not a root of unity, then $h(\alpha) \geq (\log 2)/4$. In particular, $B_0(\mathbb{Q}(\mu_{2^\infty})) \geq (\log 2)/4$.*

Basically all of the ideas needed to prove this result are present in Proposition 2 of [Amoroso and Dvornicich 2000], which treats the cyclotomic fields $\mathbb{Q}(\zeta_k)$ for $4 \mid k$. The statement of the height bound in that result excludes certain elements of $\mathbb{Q}(\zeta_k)$, but we can easily recover the bound for these excluded elements in the special case that $k = 2^m$. As it may be of some interest, we include the complete proof in this case.

Proof of Theorem 10. If $\zeta\alpha \in \mathbb{Q}$ for some root of unity $\zeta \in \mathbb{Q}(\mu_{2^\infty})$, then $\zeta\alpha \notin \{0, \pm 1\}$ and so $h(\alpha) = h(\zeta\alpha) \geq \log 2 > (\log 2)/4$. Thus we may assume that $\zeta\alpha \notin \mathbb{Q}$ for all roots of unity $\zeta \in \mathbb{Q}(\mu_{2^\infty})$. Let m be the smallest positive integer with the property that $\zeta\alpha \in \mathbb{Q}(\zeta_{2^m})$ for some root of unity $\zeta \in \mathbb{Q}(\mu_{2^\infty})$;

thus $m \geq 2$ by assumption. Since $h(\zeta\alpha) = h(\alpha)$, without loss of generality we may just assume that $\alpha \in \mathbb{Q}(\zeta_{2^m})$ and that $\zeta\alpha \notin \mathbb{Q}(\zeta_{2^{m-1}})$ for all roots of unity $\zeta \in \mathbb{Q}(\mu_{2^\infty})$.

Write $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^m})/\mathbb{Q}(\zeta_{2^{m-1}})) = \{1, \sigma\}$; thus $\sigma(\zeta_{2^m}) = -\zeta_{2^m}$. Set

$$\gamma = \sigma(\alpha)^2 - \alpha^2.$$

Note that $\gamma \neq 0$ as otherwise either $\sigma(\alpha) = \alpha$ or $\sigma(\alpha) = -\alpha$; the former case implies $\alpha \in \mathbb{Q}(\zeta_{2^{m-1}})$, and the latter case implies $\zeta_{2^m}\alpha \in \mathbb{Q}(\zeta_{2^{m-1}})$, both of which are forbidden by assumption.

If v is a place of $\mathbb{Q}(\zeta_{2^m})$, then

$$|\gamma|_v \leq \max(1, |\alpha|_v)^2 \max(1, |\sigma(\alpha)|_v)^2 \qquad \text{if } v \nmid 2, \infty \tag{6}$$

$$|\gamma|_v \leq \tfrac{1}{4} \max(1, |\alpha|_v)^2 \max(1, |\sigma(\alpha)|_v)^2 \qquad \text{if } v \mid 2 \tag{7}$$

$$|\gamma|_v \leq 2 \max(1, |\alpha|_v)^2 \max(1, |\sigma(\alpha)|_v)^2 \qquad \text{if } v \mid \infty \tag{8}$$

These inequalities and the product formula, together with the fact that $h(\sigma(\alpha)) = h(\alpha)$, imply that $0 = \sum_v r_v \log|\gamma|_v \leq 4h(\alpha) - \log 4 + \log 2$, and the desired bound $h(\alpha) \geq (\log 2)/4$ follows. The bounds (6) and (8) are trivial applications of the triangle inequality.

It remains only to prove (7); thus fix a place $v \mid 2$ of $\mathbb{Q}(\zeta_{2^m})$. Using Proposition Lemma 4.4.12 of [Bombieri and Gubler 2006], there exists $\beta \in \mathbb{Z}[\zeta_{2^m}]$ such that $\alpha\beta \in \mathbb{Z}[\zeta_{2^m}]$ and $|\beta|_v = \max(1, |\alpha|_v)^{-1}$. Note that for arbitrary $x \in \mathbb{Z}[\zeta_{2^m}]$, writing $x = \Sigma_j a_j \zeta_{2^m}^j$, since $\sigma(\zeta_{2^m}) = -\zeta_{2^m}$ we have

$$\sigma(x)^2 - x^2 = (\sigma(x) - x)(\sigma(x) + x) = -4\left(\sum_{2\nmid j} a_j \zeta_{2^m}^j\right)\left(\sum_{2 \mid j} a_j \zeta_{2^m}^j\right)$$

and thus $|\sigma(x)^2 - x^2|_v \leq \frac{1}{4}$. We conclude

$$\begin{aligned}
|\beta|_v^2 |\gamma|_v &= |\beta^2\sigma(\alpha)^2 - \alpha^2\beta^2|_v \\
&= |(\beta^2 - \sigma(\beta)^2)\sigma(\alpha)^2 + \sigma(\alpha\beta)^2 - (\alpha\beta)^2|_v \\
&\leq \max(|\beta^2 - \sigma(\beta)^2|_v |\sigma(\alpha)|_v^2, |\sigma(\alpha\beta)^2 - (\alpha\beta)^2|_v) \\
&\leq \max\left(\tfrac{1}{4}|\sigma(\alpha)|_v^2, \tfrac{1}{4}\right) \\
&= \tfrac{1}{4}\max(1, |\sigma(\alpha)|_v)^2,
\end{aligned}$$

which is equivalent to (7) as $|\beta|_v = \max(1, |\alpha|_v)^{-1}$. □

5. Powering maps and Chebyshev maps

In a slightly more general framework than what has been described above, in this section we consider pairs (ϕ, α), where $\phi(x) \in \overline{K}[x]$ is a polynomial and where $\alpha \in \overline{K}$. We define recursively $K_0 = K_0(\phi, \alpha) = K(\alpha)$ and $K_n = K_n(\phi, \alpha) = K_{n-1}(\phi^{-n}(\alpha))$ for $n \geq 1$, and set $K_\infty(\phi, \alpha) = \bigcup K_n(\phi, \alpha)$. Since the requirement that ϕ and α are defined over K have been relaxed, K_0/K may be a proper extension and the K_n/K may no longer be Galois extensions.

Proposition 11. *Let K be a number field, let $\phi(x), \psi(x) \in \overline{K}[x]$ be two polynomials of degree $d \geq 2$, and let $\alpha, \beta \in \overline{K}$.*

(a) *If (ϕ, α) is $\overline{K}$-conjugate to (ψ, β), then $K_\infty(\phi, \alpha)$ is contained in a finite extension of K^{ab} if and only if $K_\infty(\psi, \beta)$ is contained in a finite extension of K^{ab}.*

(b) *If $\phi(x), \psi(x), \alpha, \beta$ are defined over K^{ab} and (ϕ, α) is K^{ab}-conjugate to (ψ, β), then $K_\infty(\phi, \alpha)/K$ is an abelian extension if and only if $K_\infty(\psi, \beta)/K$ is an abelian extension.*

Proof. (a) There exists a finite extension F/K such that $\phi(x)$, $\psi(x)$, α, β are all defined over F, and extending F if necessary there exists an automorphism $\gamma(x) = ax + b$ defined over F for which $\psi = \gamma \circ \phi \circ \gamma^{-1}$ and $\beta = \gamma(\alpha)$. Note that for each $n \geq 0$, γ restricts to a bijection from $\phi^{-n}(\alpha)$ onto $\psi^{-n}(\beta)$. In particular, it follows that $K_\infty(\psi, \beta) \subseteq F K_\infty(\phi, \alpha)$, and thus if $K_\infty(\phi, \alpha)$ is contained in a finite extension L of K^{ab}, then $K_\infty(\psi, \beta)$ is contained in the finite extension LF of K^{ab}. The reverse implication follows from symmetry.

(b) In the preceding argument, we may take $F \subseteq K^{\mathrm{ab}}$. Thus if $K_\infty(\phi, \alpha) \subseteq K^{\mathrm{ab}}$, then $K_\infty(\psi, \beta) \subseteq K^{\mathrm{ab}}$ as well, and conversely by symmetry. □

The following two results verify the Conjecture in the special case that $\phi(x)$ is $\overline{K}$-conjugate to a powering map x^d or to a Chebyshev map $T_d(x)$.

Theorem 12. *Let $\phi(x) \in \overline{K}[x]$ be a polynomial of degree $d \geq 2$, let $\alpha \in \overline{K}$ be a nonexceptional point for ϕ, and assume that the pair (ϕ, α) is $\overline{K}$-conjugate to the pair (x^d, β) for $\beta \in \overline{K}$. Then $K_\infty(\phi, \alpha)/K$ is an abelian extension if and only if β is a root of unity and (ϕ, α) is K^{ab}-conjugate to (x^d, β).*

Proof. Assume that β is a root of unity and that (ϕ, α) is K^{ab}-conjugate to (x^d, β). Then $K_\infty(x^d, \beta)$ is a cyclotomic, and hence abelian, extension of K, and it follows from Proposition 11(b) that $K_\infty(\phi, \alpha)/K$ is an abelian extension.

Conversely, assume that $K_\infty(\phi, \alpha)/K$ is an abelian extension. Using Proposition 11(a), it follows that $K_\infty(x^d, \beta)$ is contained in a finite extension L of K^{ab}. If β is not a root of unity, then $h(\beta) > 0$. (Note that $\beta \neq 0$ by the assumption that α is not an exceptional point of ϕ, and hence β is not an exceptional point of x^d.) But $\beta^{1/d^n} \in K_\infty(x^d, \beta) \subseteq L$ for all $n \geq 0$, and $h(\beta^{1/d^n}) = \frac{1}{d^n} h(\beta) \to 0^+$ as $n \to +\infty$, a contradiction of Theorem 9. We conclude that β must be a root of unity.

Finally, we must show that the $\overline{K}$-conjugacy between (ϕ, α) and (x^d, β) is actually defined over K^{ab}. By hypothesis there exists $\gamma(x) = ax + b$ defined over $\overline{K}$ for which $x^d = \gamma \circ \phi \circ \gamma^{-1}(x)$ and $\beta = \gamma(\alpha)$. Moreover, γ restricts to a bijection from the backward ϕ-orbit of α onto the backward x^d-orbit of β. These are infinite sets contained in K^{ab}, since both $K_\infty(\phi, \alpha)/K$ and $K_\infty(x^d, \beta)/K$ are abelian extensions. Selecting distinct corresponding pairs $\gamma(s_1) = t_1$ and $\gamma(s_2) = t_2$ with $s_j, t_j \in K^{\mathrm{ab}}$, we have that both $a = (t_1 - t_2)/(s_1 - s_2)$ and $b = (s_1 t_2 - t_1 s_2)/(s_1 - s_2)$ are in K^{ab}. □

Let $d \geq 2$ be an integer, and let $T_d(x) \in \mathbb{Z}[x]$ be the d-th Chebyshev polynomial; that is, $T_d(x)$ is the unique polynomial of degree d satisfying $T_d(x + 1/x) = x^d + 1/x^d$. In other words, considering the

2-to-1 rational map $\pi : \mathbb{G}_m \to \mathbb{A}^1$ defined by $\pi(x) = x + 1/x$, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{G}_m & \xrightarrow{x^d} & \mathbb{G}_m \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{A}^1 & \xrightarrow{T_d} & \mathbb{A}^1. \end{array} \tag{9}$$

See [Silverman 2007, Section 6.2].

Theorem 13. *Let $\phi(x) \in \bar{K}[x]$ be a polynomial of degree $d \geq 2$, let $\alpha \in \bar{K}$ be a nonexceptional point for ϕ, and assume that the pair (ϕ, α) is $\bar{K}$-conjugate to the pair (T_d, β) for $\beta \in \bar{K}$. Then $K_\infty(\phi, \alpha)/K$ is an abelian extension if and only if $\beta = \zeta + 1/\zeta$ for some root of unity $\zeta \in \bar{K}$ and (ϕ, α) is K^{ab}-conjugate to (T_d, β).*

Proof. Assume that $\beta = \zeta + 1/\zeta$ for some root of unity $\zeta \in \bar{K}$ and that (ϕ, α) is K^{ab}-conjugate to (T_d, β). By the commutative diagram (9), the points $\epsilon \in \bar{K}$ satisfying $T_d^n(\epsilon) = \beta$ are precisely the points of the form $\epsilon = \xi + 1/\xi$, as ξ ranges over the d^n-th roots of ζ. In particular, $K_\infty(T_d, \beta)$ is contained in a cyclotomic, and hence abelian, extension of K, and it follows from Proposition 11(b) that $K_\infty(\phi, \alpha)/K$ is an abelian extension.

Conversely, assume that $K_\infty(\phi, \alpha)/K$ is an abelian extension. Using Proposition 11(a), it follows that $K_\infty(T_d, \beta)$ is contained in a finite extension L of K^{ab}; let $D = [L : K^{\mathrm{ab}}]$. Select $\zeta \in \pi^{-1}(\beta)$, thus $\beta = \zeta + 1/\zeta$, and assume that ζ is not a root of unity. In particular $h(\zeta) > 0$. Let $n \geq 0$ and select $\epsilon_n \in \bar{K}$ satisfying $T_d^n(\epsilon_n) = \beta$; thus $\epsilon_n = \xi_n + 1/\xi_n$ for some d^n-th root $\xi_n = \zeta^{1/d^n}$ of ζ. Since $\epsilon_n \in K_\infty(T_d, \beta) \subseteq L$, it follows that ξ_n is contained in a quadratic extension of L and hence contained in an extension of K^{ab} of degree $\leq 2D$. It follows from Theorem 9 that $h(\xi_n) \geq C_{K,2D}$. But as $n \geq 0$ is arbitrary, we may let $n \to +\infty$ and obtain $h(\xi_n) = \frac{1}{d^n} h(\zeta) \to 0^+$, a contradiction. We conclude that ζ must be a root of unity. That the $\bar{K}$-conjugacy between (ϕ, α) and (T_d, β) is actually defined over K^{ab} follows from the same argument used in Theorem 12. □

6. Maps with small Arakelov–Zhang pairing

We now describe how to extend the ideas used in the proof of Theorem 12 to treat polynomials which are not necessarily $\bar{K}$-conjugate to powering maps, but which are K^{ab}-conjugate to some polynomial $\phi(x) \in K[x]$ that is arithmetically close to a powering map.

We first recall the definitions of several arithmetic-dynamical objects associated to a polynomial $\phi(x) \in K[x]$ of degree $d \geq 2$ defined over a number field K; see [Silverman 2007, Sections 3.4–3.5] for further details. The *Call–Silverman canonical height function* $\hat{h}_\phi : \bar{K} \to \mathbb{R}$ may be defined by the limit

$$\hat{h}_\phi(x) = \lim_{n \to +\infty} \frac{h(\phi^n(x))}{d^n}$$

and can be characterized by the identity $\hat{h}_\phi(\phi(x)) = d\hat{h}_\phi(x)$ together with the fact that $h - \hat{h}_\phi$ is bounded on $\bar{K}$. Locally, given a finite extension L/K, for each place $v \in M_L$ define the *canonical local height*

function by

$$\lambda_{\phi,v} : \mathbb{C}_v \to \mathbb{R}, \quad \lambda_{\phi,v}(x) = \lim_{n\to+\infty} \frac{1}{d^n} \log^+ |\phi^n(x)|_v. \tag{10}$$

Then an alternative expression for the canonical height is given by

$$\hat{h}_\phi(\alpha) = \sum_{v\in M_L} r_v \lambda_{\phi,v}(\alpha), \tag{11}$$

for all $\alpha \in L$, a formula which may be viewed as analogous to (5).

For each place $v \in M_K$, standard arguments show that $\lambda_{\phi,v}(x) \geq 0$ for all $x \in \mathbb{C}_v$, with equality if and only if x is in the filled Julia set

$$F_{\phi,v} = \{x \in \mathbb{C}_v \mid |\phi^n(x)|_v \text{ is bounded as } n \to +\infty\}$$

associated to ϕ. The *canonical measure* $\mu_{\phi,v}$ associated to ϕ is a ϕ-invariant unit Borel measure supported on $F_{\phi,v}$ which describes the limiting distribution of preperiodic points and iterated inverse images with respect to ϕ. There are several equivalent constructions of this measure in the literature; see [Freire et al. 1983; Ljubich 1983] in the Archimedean case and [Baker and Rumely 2006; Chambert-Loir 2006; Favre and Rivera-Letelier 2006] in the non-Archimedean case. (Technically, when v is a non-Archimedean place, the objects $\lambda_{\phi,v}$, $F_{\phi,v}$, and $\mu_{\phi,v}$ need to be interpreted on the Berkovich affine line $\boldsymbol{A}^1_v$. We will not need to go into these details in the present paper.)

Given two polynomials $\phi(x), \psi(x) \in K[x]$ of degree at least two, the *Arakelov–Zhang pairing* can be defined by either of the two expressions

$$\langle \phi, \psi \rangle = \sum_{v\in M_K} r_v \int \lambda_{\phi,v}\, d\mu_{\psi,v} = \sum_{v\in M_K} r_v \int \lambda_{\psi,v}\, d\mu_{\phi,v}. \tag{12}$$

Thus $\langle \phi, \psi \rangle$ is a nonnegative real number, and in some sense it measures the global arithmetic-dynamical distance between the two maps. This pairing was originally defined as a limit of arithmetic intersection products by Zhang [1995], and described analytically using Berkovich spaces by Petsche, Szpiro and Tucker [Petsche et al. 2012]. For our purposes the most important fact about the Arakelov–Zhang pairing is that it is closely related to points which have small canonical height with respect to one of the two maps. In particular, it was shown in [Petsche et al. 2012] that if $\{\alpha_n\}$ is a sequence of distinct points in $\overline{K}$ with $\hat{h}_\phi(\alpha_n) \to 0$, then $\hat{h}_\psi(\alpha_n) \to \langle \phi, \psi \rangle$.

In the special case $\psi(x) = x^d$ for $d \geq 2$, the canonical height $\hat{h}_\psi$ is the same as the usual Weil height h, $\lambda_{\psi,v}(\cdot) = \log^+|\cdot|_v$, $F_{\psi,v}$ is the closed unit disc, and $\mu_{\psi,v}$ is equal to the normalized Haar measure supported on the unit circle of $\mathbb{C}_v = \mathbb{C}$ when v is Archimedean, and equal to the Dirac measure supported at the Gauss point of $\boldsymbol{A}^1_v$ when v is non-Archimedean. In particular, the value of the pairing $\langle \phi, x^d \rangle$ does not depend on d.

Theorem 14. *Let $\phi(x) \in K[x]$ be a polynomial of degree $d \geq 2$ defined over K such that $\langle \phi, x^d \rangle > 0$, and let α be a nonexceptional point for ϕ. If $K_\infty(\phi, \alpha) \subseteq L \subseteq \overline{K}$, then*

$$B_0(L) \leq \langle \phi, x^d \rangle. \tag{13}$$

Proof. For each $n \geq 1$, let $\alpha_n \in K_\infty \subseteq L$ satisfy $\phi^n(\alpha_n) = \alpha$; since α is not an exceptional point we may assume that the α_n are distinct. It follows from properties of the canonical height that $\hat{h}_\phi(\alpha_n) = \hat{h}_\phi(\alpha)/d^n \to 0$ as $n \to +\infty$. By Theorem 1 of [Petsche et al. 2012], it follows that $h(\alpha_n) \to \langle \phi, x^d \rangle > 0$, and (13) follows from the definition of $B_0(L)$. □

As a sample application of Theorem 14, we can show that for any number field K, a certain infinite family of polynomials satisfies the Conjecture.

Corollary 15. *For each number field K, there exists a constant C_K such that $\mathrm{Gal}(K_\infty((x^p - x)/p, \alpha)/K)$ is nonabelian over K for all $\alpha \in K$ and all primes $p \geq C_K$. In particular, $\mathrm{Gal}(K_\infty((x^p - x)/p, \alpha)/\mathbb{Q})$ is nonabelian for all $\alpha \in \mathbb{Q}$ and all $p \geq 29$.*

Proof. It has been shown by Petsche and Stacy [2019] that $\langle (x^p - x)/p, x^d \rangle = \log p/(p-1)$. Thus if $K_\infty((x^p - x)/p, \alpha) \subseteq K^{\mathrm{ab}}$, Theorem 14 implies that $B_0(K^{\mathrm{ab}}) \leq \log p/(p-1)$. But since $B_0(K^{\mathrm{ab}}) > 0$ [Amoroso and Zannier 2000], we have a contradiction for large enough p. In particular, it was shown by Amoroso and Dvornicich [2000] that $B_0(\mathbb{Q}^{\mathrm{ab}}) \geq (\log 5)/12$, which exceeds $\log p/(p-1)$ once $p \geq 29$. □

We remark that, according to the Conjecture, we expect that $\mathrm{Gal}(K_\infty((x^p - x)/p, \alpha)/K)$ is nonabelian for all number fields K, all $\alpha \in K$, and all primes p.

7. The map $x^2 - 1$

It is well known that there are exactly three $\mathbb{Q}$-conjugacy classes of postcritically finite quadratic polynomials over $\mathbb{Q}$, represented by x^2, $x^2 - 1$, and $x^2 - 2$. By $\mathbb{Q}$-conjugacy it suffices to check the family $\phi_c(x) = x^2 + c$ for $c \in \mathbb{Q}$, and the assumption that the critical point 0 is preperiodic (i.e., $\phi_c^m(0) = \phi_c^n(0)$ for $m < n$) forces c to be an algebraic integer (hence a rational integer) and also an element of the complex Mandelbrot set $\mathcal{M} = \{c \in \mathbb{C} \mid \phi_c^n(0) \not\to \infty\}$. It is elementary to check that $\mathcal{M} \cap \mathbb{Z} = \{-2, -1, 0\}$.

Since x^2 and $x^2 - 2$ are a powering map and a Chebyshev map, respectively, they are treated by Theorems 12 and 13, and the stable postcritically infinite quadratic case is treated in Theorem 8. Thus in order to complete the proof of Theorem 1, it suffices to consider the polynomial $\phi(x) = x^2 - 1$ over $\mathbb{Q}$ in the stable case.

In order to show that $K_\infty(x^2 - 1, \alpha)/\mathbb{Q}$ is never an abelian extension, one might hope to combine the bound $B_0(\mathbb{Q}^{\mathrm{ab}}) \geq (\log 5)/12 = 0.134\ldots$ of Amoroso and Dvornicich with Theorem 14, but it turns out that the Arakelov–Zhang pairing $\langle x^2 - 1, x^2 \rangle = 0.167\ldots$ is too large for this argument to apply directly. However, we can recover this strategy (in the stable case) by showing that if $K_\infty(x^2 - 1, \alpha)$ is an abelian extension of $\mathbb{Q}$ then it is contained in the subfield $\mathbb{Q}(\mu_{2^\infty})$ of $\mathbb{Q}^{\mathrm{ab}}$, which has Bogomolov constant $B_0(\mathbb{Q}(\mu_{2^\infty})) \geq (\log 2)/4 = 0.173\ldots$, large enough to obtain a contradiction.

Lemma 16. *Let $\phi(x) = x^2 - 1$, let $\alpha \in K$, and assume that the pair (ϕ, α) is stable over K and that $K_\infty = K_\infty(x^2 - 1, \alpha)$ is an abelian extension of K. If $\mathfrak{p}$ is a prime of K with residue characteristic not equal to 2, then $\mathfrak{p}$ is unramified in K_∞.*

Proof. The stability and abelian hypotheses imply via Lemma 2 that $[K_n : K] = 2^n$ for all $n \geq 1$. Let $\psi(x) = \phi(x+\alpha) - \alpha = x^2 + 2\alpha x + \alpha^2 - \alpha - 1$. The critical point of $\psi(x)$ is $c = -\alpha$, which is part of a 2-cycle; that is, $\psi^n(c) = -\alpha$ for all even n, and $\psi^n(c) = -1 - \alpha$ for all odd n. Clearly

$$\operatorname{disc}(\phi(x) - \alpha) = 4(1 + \alpha)$$

and using Lemma 5 for $n \geq 2$ we have

$$\operatorname{disc}(\phi^n(x) - \alpha) = \operatorname{disc}(\phi^n(x+\alpha) - \alpha) = \operatorname{disc}(\psi^n(x)) = \begin{cases} R_n^2(-\alpha) & \text{if } n \geq 2 \text{ is even,} \\ R_n^2(-1-\alpha) & \text{if } n \geq 3 \text{ is odd,} \end{cases}$$

for some nonzero $R_n \in K$.

Case 1: $-1 - \alpha$ is not a square in K. Then $\operatorname{disc}(\phi^n(x) - \alpha)$ is not a square for all odd $n \geq 3$, and thus viewing $\operatorname{Gal}(K_n/K)$ as a subgroup of S_{2^n} via its action on the roots of $\phi^n(x) - \alpha$, $\operatorname{Gal}(K_n/K)$ is not a subgroup of A_{2^n} for all odd $n \geq 3$. By Lemma 4, it follows that $\operatorname{Gal}(K_n/K)$ is cyclic for all odd $n \geq 3$. Then $\operatorname{Gal}(K_n/K)$ must be cyclic for all n, since $\operatorname{Gal}(K_m/K)$ is a quotient of $\operatorname{Gal}(K_n/K)$ when $1 \leq m < n$. We conclude from Lemma 7 that no primes of K of odd residue characteristic ramify in K_∞.

Case 2: $-1 - \alpha = t^2$ for $t \in K$. By the stability hypothesis we know that $\operatorname{disc}(\phi(x) - \alpha) = 4(1+\alpha) = -4t^2$ is not a square in K, and thus we conclude that -1 is not a square in K and $K_1 = K(\phi^{-1}(\alpha)) = K(\sqrt{4(1+\alpha)}) = K(\sqrt{-1})$. In particular, no primes of K with odd residue characteristic ramify in K_1, so it now suffices to show that no primes of K_1 with odd residue characteristic ramify in K_∞.

Let $\phi^{-1}(\alpha) = \{\alpha', \alpha''\}$. Thus for each $n \geq 1$, we have a disjoint union

$$\phi^{-n}(\alpha) = \phi^{-(n-1)}(\alpha') \sqcup \phi^{-(n-1)}(\alpha'').$$

and it follows from the transitive action of $\operatorname{Gal}(K_n/K)$ on $\phi^{-n}(\alpha)$ that $\operatorname{Gal}(K_n/K_1)$ acts transitively on $\phi^{-(n-1)}(\alpha')$. We conclude that (ϕ, α') is a stable pair over K_1. Arguing as above, it follows that $1 + \alpha'$ is not a square in K_1, and as -1 is a square in K_1, we deduce that $-1 - \alpha'$ is not a square in K_1. We are now in the setting of Case 1 for the pair (ϕ, α') over K_1, and we conclude that no primes of K_1 with odd residue characteristic ramify in K_∞. □

Theorem 17. *Let $\phi(x) = x^2 - 1$, let $\alpha \in \mathbb{Q}$, and assume that the pair (ϕ, α) is stable. Then $\operatorname{Gal}(K_\infty/\mathbb{Q})$ is nonabelian.*

Proof. Assume on the contrary that $K_\infty/\mathbb{Q}$ is an abelian extension. By Lemma 16, no odd primes ramify in K_∞, and it follows from class field theory that $K_\infty \subseteq \mathbb{Q}(\mu_{2^\infty})$. As we will calculate in Section 8, we have

$$\langle x^2 - 1, x^2 \rangle = 0.167\ldots, \tag{14}$$

and we conclude from Theorem 14 that $B_0(\mathbb{Q}(\mu_{2^\infty})) \le \langle x^2-1, x^2\rangle = 0.167\ldots$. This is a contradiction of the bound $B_0(\mathbb{Q}(\mu_{2^\infty})) \ge (\log 2)/4 = 0.173\ldots$ proved in Theorem 10. □

8. Numerical approximation of Archimedean Arakelov–Zhang integrals

In this section we prove a result which may be of use in numerically approximating the value of the Archimedean part of the Arakelov–Zhang pairing $\langle x^2+c, x^2\rangle$.

Given a polynomial $\phi(x) \in \mathbb{C}[x]$ of degree 2, we may express the corresponding canonical local height function as

$$\lambda_\phi(x) = \lim_{n\to+\infty} \frac{1}{2^n} \log(1+|\phi^n(x)|^2)^{1/2}. \tag{15}$$

Note that, compared to (10), we have replaced $\log^+|\cdot|$ with $\log(1+|\cdot|^2)^{1/2}$; this choice gives differentiable approximations to $\lambda_\phi(x)$, but in the limit it defines precisely the same Archimedean local height function as in (10).

Next define

$$B(\phi) = \sup_{x\in\mathbb{C}} |\log(1+|\phi(x)|^2)^{1/2} - 2\log(1+|x|^2)^{1/2}|. \tag{16}$$

The significance of this constant follows from a standard telescoping series argument [Silverman 2007, Theorem 3.20], which shows that for each $n \ge 1$ we have

$$\left|\lambda_\phi(x) - \frac{1}{2^n}\log(1+|\phi^n(x)|^2)^{1/2}\right| \le \frac{B(\phi)}{2^n}. \tag{17}$$

Proposition 18. *Let $\phi(x) = x^2+c$ for $c \in \mathbb{C}$, let $N \ge 1$ and $M \ge 1$ be integers, and let μ_M denote the set of M-th roots of unity in $\mathbb{C}$. Then*

$$\left|\int_0^1 \lambda_\phi(e^{2\pi i t})\,dt - \frac{1}{M}\sum_{\zeta\in\mu_M} \frac{1}{2^N}\log(1+|\phi^N(\zeta)|^2)^{1/2}\right| \le \frac{B(\phi)}{2^N} + \frac{\pi T^N}{M} \tag{18}$$

where $T = (1+\sqrt{1+4|c|})/2$.

Proof. Using (17) we obtain

$$\left|\int_0^1 \lambda_\phi(e^{2\pi i t})\,dt - \int_0^1 f_N(t)\,dt\right| \le \frac{B(\phi)}{2^N} \tag{19}$$

where

$$f_N : \mathbb{R}/\mathbb{Z} \to \mathbb{R} \quad f_N(t) = \frac{1}{2^N}\log(1+|\phi^N(e^{2\pi i t})|^2)^{1/2}.$$

If $f : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ is continuously differentiable and $M \ge 1$, then

$$\left|\frac{1}{M}\sum_{m=1}^{M} f(m/M) - \int_0^1 f(t)\,dt\right| \le \frac{\|f'\|_\infty}{2M}, \tag{20}$$

where $\|g\|_\infty = \sup\{|g(t)| \mid t \in \mathbb{R}/\mathbb{Z}\}$. This inequality can be verified using an elementary Riemann sum argument, together with the mean-value theorem estimate $|f(m/M) - f(t)| \le \|f'\|_\infty/2M$ whenever $t \in [m/M - 1/(2M), m/M + 1/(2M)]$.

We are going to show that $\|f_N'\|_\infty \le 2\pi T^N$, and so applying (20) with $f = f_N$, and combining with (19), we obtain (18).

It remains only to prove $\|f_N'\|_\infty \le 2\pi T^N$. Given any polynomial $F(x) \in \mathbb{C}[x]$, an application of the multivariable chain rule gives, for $t \in \mathbb{R}$,

$$\left|\frac{d}{dt}\log(1+|F(e^{2\pi it})|^2)^{1/2}\right| \le \frac{2\pi|F(e^{2\pi it})||F'(e^{2\pi it})|}{1+|F(e^{2\pi it})|^2}. \tag{21}$$

The choice of T in terms of c was made so that $T^2 - T - |c| = 0$, which can be used to show that

$$|x| > T \Rightarrow |\phi(x)| > |x|^2/T > T \tag{22}$$

for all $x \in \mathbb{C}$. Indeed, $|\phi(x)| \ge |x|^2 - |c|$ and therefore

$$\frac{|\phi(x)|}{|x|^2} \ge 1 - \frac{|c|}{|x|^2} > 1 - \frac{|c|}{T^2} = \frac{1}{T}.$$

Using an iteration of the inequality (22), we claim that for each $x \in \mathbb{C}$, we have

$$|x\phi(x)\phi^2(x)\cdots\phi^N(x)| \le T^N(1+|\phi^N(x)|^2). \tag{23}$$

Indeed, if $|\phi^n(x)| \le T$ for all $n = 0, 1, 2, \ldots, N-1$, the bound is trivial. Otherwise, let $0 \le n_0 \le N-1$ be the smallest n for which $|\phi^n(x)| > T$. Using (22) we have $|\phi^n(x)| < T^{1/2}|\phi^{n+1}(x)|^{1/2}$ for all $n_0 \le n \le N-1$. Thus, letting $m_0 = N - n_0$, we have

$$\begin{aligned}
|x\phi(x)\phi^2(x)\cdots\phi^N(x)| &\le T^{n_0}|\phi^{n_0}(x)||\phi^{n_0+1}(x)|\cdots|\phi^N(x)| \\
&< T^{n_0}T^{1/2}|\phi^{n_0+1}(x)|^{1/2+1}|\phi^{n_0+2}(x)|\cdots|\phi^N(x)| \\
&< T^{n_0}T^{1/2}T^{1/4+1/2}|\phi^{n_0+2}(x)|^{1/4+1/2+1}|\phi^{n_0+3}(x)|\cdots|\phi^N(x)| \\
&\vdots \\
&< T^{n_0}T^{1/2}T^{1/4+1/2}\cdots T^{1/2^{m_0}+\cdots+1/2}|\phi^N(x)|^{1/2^{m_0}+\cdots+1/2+1} \\
&< T^N(1+|\phi^N(x)|^2).
\end{aligned}$$

Using $\phi'(x) = 2x$ and the chain rule we have

$$(\phi^N)'(x) = \phi'(\phi^{N-1}(x))\phi'(\phi^{N-2}(x))\cdots\phi'(\phi(x))\phi'(x) = 2^N\phi^{N-1}(x)\phi^{N-2}(x)\cdots\phi(x)x, \tag{24}$$

and applying (23) we obtain

$$|\phi^N(x)||(\phi^N)'(x)| = 2^N|\phi^N(x)\phi^{N-1}(x)\phi^{N-2}(x)\cdots\phi(x)x| \le 2^N T^N(1+|\phi^N(x)|^2). \tag{25}$$

Finally, taking $F(x) = \phi^N(x)$ in (21) and using the bound (25) we conclude $\|f_N'\|_\infty \le 2\pi T^N$, completing the proof. □

We conclude with an explanation of how to use Proposition 18 to obtain the numerical calculation (14) of $\langle x^2-1, x^2\rangle$ to the specified precision. Since both $\phi(x)=x^2-1$ and $\psi(x)=x^2$ are monic with integer coefficients, the non-Archimedean contributions in (12) vanish, and since the Archimedean canonical measure $\mu_{\phi,\infty}$ is the normalized Haar measure supported on the unit circle of $\mathbb{C}$, we have

$$\langle \phi, \psi\rangle = \int_0^1 \lambda_{\phi,\infty}(e^{2\pi i t})\,dt. \tag{26}$$

We approximate this integral using Proposition 18 with $\phi(x)=x^2-1$. Clearly $T=(1+\sqrt{5})/2$, and we will show that $B(\phi)=(\log 5)/2$, which according to the definition (16) is equivalent to checking that

$$\sup_{x\in\mathbb{C}}\left|\log\frac{1+|x^2-1|^2}{(1+|x|^2)^2}\right| = \log 5. \tag{27}$$

To establish (27) is to prove both of the inequalities

$$\tfrac{1}{5}(1+|x|^2)^2 \le 1+|x^2-1|^2 \le 5(1+|x|^2)^2 \tag{28}$$

and to prove that at least one of them is sharp. The second inequality (with the stronger constant 2 in place of 5) is easily checked using only the triangle inequality. For the second inequality, we see using the triangle inequality that $1+|x^2-1|^2 \ge |x|^4-2|x|^2+2$, with equality when x is real; we complete the proof by noting that $(r^4-2r^2+2)/(1+r^2)^2$ is minimized at $r=\sqrt{\frac{3}{2}}$ with minimum value $\frac{1}{5}$.

Using Proposition 18 with $M=2^{24}$ and $N=13$, we have

$$\int_0^1 \lambda_{\phi,\infty}(e^{2\pi i t})\,dt = \frac{1}{2^{38}}\sum_{\zeta\in\mu_{2^{24}}} \log(1+|\phi^{13}(\zeta)|^2)+\theta \tag{29}$$

where $|\theta| \le (\log 5)/2^{14}+\pi((1+\sqrt{5})/2)^{13}/2^{24}=0.000195\ldots$. Finally, one may perform the calculation

$$\frac{1}{2^{38}}\sum_{\zeta\in\mu_{2^{24}}} \log(1+|\phi^{13}(\zeta)|^2) = 0.16772223\ldots \tag{30}$$

using any implementation of arbitrary precision floating-point arithmetic; specifically we used the RealField() package in Sage [2016] in a computation taking about three hours. It follows from (26), (29), (30), and the bound on θ that (14) is accurate to the indicated precision.

It was pointed out to us by an anonymous referee that, if one only wants to check that $\langle x^2-1, x^2\rangle < (\log 2)/4$ but without giving an explicit numerical approximation for $\langle x^2-1, x^2\rangle$, then one could get away with the smaller parameters $N=9$ and $M=2^{16}$, resulting in a much faster calculation.

Acknowledgements

We thank Rafe Jones for several helpful suggestions.

References

[Ahmad et al. 2019] F. Ahmad, R. L. Benedetto, J. Cain, G. Carroll, and L. Fang, "The arithmetic basilica: a quadratic PCF arboreal Galois group", preprint, 2019. arXiv

[Amoroso and Dvornicich 2000] F. Amoroso and R. Dvornicich, "A lower bound for the height in abelian extensions", *J. Number Theory* **80**:2 (2000), 260–272. MR Zbl

[Amoroso and Zannier 2000] F. Amoroso and U. Zannier, "A relative Dobrowolski lower bound over abelian extensions", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **29**:3 (2000), 711–727. MR Zbl

[Baker and Rumely 2006] M. H. Baker and R. Rumely, "Equidistribution of small points, rational dynamics, and potential theory", *Ann. Inst. Fourier* (*Grenoble*) **56**:3 (2006), 625–688. MR Zbl

[Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Math. Monogr. **4**, Cambridge Univ. Press, 2006. MR Zbl

[Boston 2000] N. Boston, "Tree representations of Galois groups", preprint, 2000. arXiv

[Boston and Jones 2007] N. Boston and R. Jones, "Arboreal Galois representations", *Geom. Dedicata* **124** (2007), 27–35. MR Zbl

[Boston and Jones 2009] N. Boston and R. Jones, "The image of an arboreal Galois representation", *Pure Appl. Math. Q.* **5**:1 (2009), 213–225. MR Zbl

[Bridy et al. 2017] A. Bridy, P. Ingram, R. Jones, J. Juul, A. Levy, M. Manes, S. Rubinstein-Salzedo, and J. H. Silverman, "Finite ramification for preimage fields of post-critically finite morphisms", *Math. Res. Lett.* **24**:6 (2017), 1633–1647. MR Zbl

[Cassels and Fröhlich 1967] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory*, Academic Press, London, 1967. MR Zbl

[Chambert-Loir 2006] A. Chambert-Loir, "Mesures et équidistribution sur les espaces de Berkovich", *J. Reine Angew. Math.* **595** (2006), 215–235. MR Zbl

[Favre and Rivera-Letelier 2006] C. Favre and J. Rivera-Letelier, "Équidistribution quantitative des points de petite hauteur sur la droite projective", *Math. Ann.* **335**:2 (2006), 311–361. MR Zbl

[Ferraguti and Pagano 2020] A. Ferraguti and C. Pagano, "Constraining images of quadratic arboreal representations", preprint, 2020. arXiv

[Freire et al. 1983] A. Freire, A. Lopes, and R. Mañé, "An invariant measure for rational maps", *Bol. Soc. Brasil. Mat.* **14**:1 (1983), 45–62. MR Zbl

[Jones 2005] R. Jones, *Galois martingales and the hyperbolic subset of the p-adic Mandelbrot set*, Ph.D. thesis, Brown University, 2005, available at https://search.proquest.com/docview/305028664.

[Jones 2007] R. Jones, "Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set", *Compos. Math.* **143**:5 (2007), 1108–1126. MR Zbl

[Jones 2008] R. Jones, "The density of prime divisors in the arithmetic dynamics of quadratic polynomials", *J. Lond. Math. Soc.* (2) **78**:2 (2008), 523–544. MR Zbl

[Jones 2013] R. Jones, "Galois representations from pre-image trees: an arboreal survey", pp. 107–136 in *Actes de la Conférence 'Théorie des Nombres et Applications'* (Luminy, France, 2012), Publ. Math. Besançon Algèbre Théorie Nr. **2013**, Presses Univ. Franche-Comté, 2013. MR Zbl

[Lang 1970] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, MA, 1970. MR Zbl

[Ljubich 1983] M. J. Ljubich, "Entropy properties of rational endomorphisms of the Riemann sphere", *Ergodic Theory Dynam. Systems* **3**:3 (1983), 351–385. MR Zbl

[Looper 2019] N. Looper, "Dynamical Galois groups of trinomials and Odoni's conjecture", *Bull. Lond. Math. Soc.* **51**:2 (2019), 278–292. MR Zbl

[Odoni 1985a] R. W. K. Odoni, "The Galois theory of iterates and composites of polynomials", *Proc. Lond. Math. Soc.* (3) **51**:3 (1985), 385–414. MR Zbl

[Odoni 1985b] R. W. K. Odoni, "On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$", *J. Lond. Math. Soc.* (2) **32**:1 (1985), 1–11. MR Zbl

[Odoni 1988] R. W. K. Odoni, "Realising wreath products of cyclic groups as Galois groups", *Mathematika* **35**:1 (1988), 101–113. MR Zbl

[Odoni 1997] R. W. K. Odoni, "On the Galois groups of iterated generic additive polynomials", *Math. Proc. Cambridge Philos. Soc.* **121**:1 (1997), 1–6. MR Zbl

[Petsche and Stacy 2019] C. Petsche and E. Stacy, "A dynamical construction of small totally p-adic algebraic numbers", *J. Number Theory* **202** (2019), 27–36. MR Zbl

[Petsche et al. 2012] C. Petsche, L. Szpiro, and T. J. Tucker, "A dynamical pairing between two rational maps", *Trans. Amer. Math. Soc.* **364**:4 (2012), 1687–1710. MR Zbl

[Sage 2016] W. A. Stein et al., Sage mathematics software, 2016, available at https://www.sagemath.org. Version 7.1.

[Silverman 2007] J. H. Silverman, *The arithmetic of dynamical systems*, Grad. Texts in Math. **241**, Springer, 2007. MR Zbl

[Specter 2018] J. Specter, "Polynomials with surjective arboreal Galois representations exist in every degree", preprint, 2018. arXiv

[Stoll 1992] M. Stoll, "Galois groups over $\mathbb{Q}$ of some iterated polynomials", *Arch. Math.* (*Basel*) **59**:3 (1992), 239–244. MR Zbl

[Zhang 1995] S. Zhang, "Small points and adelic metrics", *J. Algebraic Geom.* **4**:2 (1995), 281–300. MR Zbl

Communicated by Joseph H. Silverman
Received 2020-01-02 Revised 2020-04-15 Accepted 2020-05-23

jandrews4@washcoll.edu *Department of Mathematics and Computer Science, Washington College, Department of Mathematics and Computer Science, Chestertown, MD, United States*

petschec@math.oregonstate.edu *Department of Mathematics, Oregon State University, Department of Mathematics, Corvallis, OR, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 7 2020