

Andrea Ferraguti

A SURVEY ON ABELIAN DYNAMICAL GALOIS GROUPS

Keywords. Arithmetic dynamics, arboreal Galois representations, global fields.

Abstract. Let K be a number field, $f \in K[x]$ and $\alpha \in K$. A recent conjecture of Andrews and Petsche predicts that the dynamical Galois group of the pair (f, α) is abelian if and only if the pair (f, α) is K^{ab} -conjugated to (g, β) , where g is a power or a Chebyshev map and β is ζ or $\zeta + \zeta^{-1}$, respectively, and ζ is a root of unity. We review three completely different approaches that allow to prove several cases of the conjecture.

1. Introduction

Let K be a field, $f \in K(x)$ be a rational map of degree at least 2 and $\alpha \in K$. For every $n \geq 1$ we will denote by f^n the n -th iterate of the map f , by $K_n(f, \alpha)$ the splitting field of $f^n - \alpha$, by $G_n(f, \alpha)$ its Galois group, by $K_\infty(f, \alpha)$ the direct limit of the $K_n(f, \alpha)$'s and by $G_\infty(f, \alpha)$ the inverse limit of the $G_n(f, \alpha)$ (or, equivalently, the Galois group of $K_\infty(f, \alpha)$). The group $G_\infty(f, \alpha)$ is called *dynamical Galois group* of the pair (f, α) .

The study of dynamical Galois groups is partially motivated by the fact that certain instances of them arise as central objects in the classical context of elliptic curves. Namely, if E is an elliptic curve over a field K , G_K is the absolute Galois group of K and p is a prime different from $\text{char } K$, the Galois representation $\rho_{E,p}$ attached to the p -adic Tate module of E is a continuous homomorphism $G_K \rightarrow \text{Aut}(T_p(E)) \cong \text{GL}_2(\mathbb{Z}_p)$ whose image is essentially the dynamical Galois group of the pair $([p], \mathcal{O}_E)$, where $[p]$ is the multiplication-by- p map and \mathcal{O}_E is the identity for the group structure on E . It is interesting to notice that although the construction of dynamical Galois groups arising from self-rational maps of \mathbb{P}^1 can be generalized in a straightforward way to self-morphisms of any algebraic curve, there are no non-trivial examples where the curve is smooth and has genus at least 2, by Riemann-Hurwitz formula. Hence \mathbb{P}^1 and elliptic curves are the only interesting smooth curves for studying these objects.

When the base field K is a number field, one has the following celebrated result, due to Serre [23].

THEOREM. The index $[\text{GL}_2(\mathbb{Z}_p) : \text{Im}(\rho_{E,p})]$ is infinite if and only if E has complex multiplication.

This is part of a general philosophy according to which whenever we have a continuous action of G_K on a topological vector space V (or, equivalently, a continuous representation $G_K \rightarrow \text{Aut}(V)$) the existence of "extra

symmetries" on V has the effect of constraining the image of the associated representation to be "small". The introduction of [9] contains a nice account of this idea for Galois representations associated to various arithmetic objects.

When dealing with dynamical Galois groups arising from self-rational maps of \mathbb{P}^1 one expects a similar behaviour. If $f \in K(x)$ and $\alpha \in K$ is such that for every positive integer n the set $f^{-n}(\alpha) := (f^n)^{-1}(\alpha)$ contains no ramification points for f , then $G_\infty(f, \alpha)$ can be seen as the image of the arboreal representation associated to the pair (f, α) . This is a continuous homomorphism $\rho_{f, \alpha}: G_K \rightarrow \text{Aut}(T_\infty(f, \alpha))$, where $T_\infty(f, \alpha)$ is the infinite regular tree constructed with the *backward orbit* of α , i.e. the set $f^{-\infty}(\alpha) := \bigcup_{n \geq 1} f^{-n}(\alpha)$ (see [16] for details). This framework is far poorer of structure than the elliptic curve one; here for example the map $\rho_{f, \alpha}$ does not arise from the action of G_K on a vector space but it is just a continuous homomorphism of topological groups. Nevertheless, the pair (f, α) can admit extra symmetries that force the image of $\rho_{f, \alpha}$ to be small, i.e. to have infinite index image in $\text{Aut}(T_\infty(f, \alpha))$.

When K is a global field of characteristic not 2 and f is a quadratic map, a conjecture of Jones [16, Conjecture 3.11] describes all possible extra symmetries that force the index $[\text{Aut}(T_\infty(f, \alpha)) : \text{Im}(\rho_{f, \alpha})]$ to be infinite. When restricted to quadratic polynomials, the conjecture is the following. Recall that a rational map $f \in K(x)$ is called *post-critically finite* (PCF for short) if the orbits of its ramification points, called *critical points* by dynamicists, are all finite.

CONJECTURE 1. Let K be a global field of characteristic not 2, let $f \in K[x]$ be a quadratic polynomial and $\alpha \in K$. Suppose that $f^{-\infty}(\alpha)$ contains no ramification points for f . Then the index $[\text{Aut}(T_\infty(f, \alpha)) : \text{Im}(\rho_{f, \alpha})]$ is infinite if and only if f is post-critically finite or α is periodic for f .

The "if" part of the conjecture is actually a theorem (see [16]); the difficult part is showing necessity. Some results conditional on the *abc* conjecture for number fields are proven in [17].

Notice that the two types of symmetries appearing in Conjecture 1 are quite different in nature: being post-critically finite is a property of the polynomial f : no matter how we choose the basepoint α the group $G_\infty(f, \alpha)$ is going to be small. This means that the so-called *iterated monodromy group* of the map f , namely the dynamical Galois group of the pair (f, t) where t is transcendental over K , is small as well. On the other hand, α being periodic for f is a symmetry of the pair (f, α) . The iterated monodromy group of f might even be large, for example if $f = x^2 - 3$ and $K = \mathbb{Q}$ we have that $G_\infty(f, t) \cong \text{Aut}(T_\infty(f, \alpha))$ (see [22] for the general theory of iterated monodromy groups of quadratic functions), but specializing at $t = 1$ makes the dynamical Galois group of the specialized pair far smaller. One would expect that most specializations do not have such a

drastic impact on the size of the dynamical Galois group. Certainly f has only a finite number of K -rational periodic points, for example. In [1], the authors propose a conjecture along these lines for the iterated monodromy group of $x^2 - 1$.

For all the reasons above, it seems natural to expect that dynamical Galois groups can rarely be abelian. In the elliptic curves framework, abelian images of Galois representations are fully described by complex multiplication theory. Let K be a number field, E/K be an elliptic curve, p a prime and $\rho_{E,p}$ the Galois representation of G_K on the p -adic Tate module of E . Then the following theorem holds (see for example [19]).

THEOREM. The image of $\rho_{E,p}$ is virtually abelian if and only if E has complex multiplication, and it is abelian if and only if E has complex multiplication defined over K .

That is, in the elliptic curve case the existence of extra symmetries not only has the effect of forcing the image of the associated representation to be small, it even forces it to be (virtually) abelian.

Once again, the dynamical side of the story is far more mysterious, and only recently a conjecture has been formulated in [4]. Recall that if $f, g \in K(x)$, $\alpha, \beta \in K$ and L is an extension of K , we say that (f, α) and (g, β) are *conjugated* over L if there exist a Möbius transformation $m \in \text{PGL}_2(L)$ such that $g = m^{-1} \circ f \circ m$ and $m(\beta) = \alpha$. If the two pairs (f, α) and (g, β) are K -conjugated, the two groups $G_\infty(f, \alpha)$ and $G_\infty(g, \beta)$ are isomorphic. Moreover, a point $\alpha \in \bar{K}$ is *exceptional* for f if its backward orbit is finite.

CONJECTURE 2 ([4, Conjecture]). Let K be a number field, $f \in K[x]$ a polynomial of degree $d \geq 2$ and $\alpha \in K$ be a non-exceptional point for f . Then $G_\infty(f, \alpha)$ is abelian if and only if there exists a root of unity ζ such that the pair (f, α) is K^{ab} -conjugated to either (x^d, ζ) or $(\pm T_d(x), \zeta + \zeta^{-1})$, where T_d is the Chebyshev polynomial of degree d .*

Hence in the dynamical framework the current prediction is that abelian dynamical Galois groups can only occur in a very special case: not only the polynomial needs to be PCF, but it also needs to come from an endomorphism of an algebraic group.

The sufficiency part of Conjecture 2 has been proven by the same authors, as below.

THEOREM 1 ([4, Theorems 12 and 13]). *Let K be a number field, $f \in K[x]$ be a polynomial of degree $d \geq 2$ and $\alpha \in K$ be a non-exceptional point for f . Suppose that f is \bar{K} -conjugate to x^d or $\pm T_d(x)$. Then $G_\infty(f, \alpha)$*

*The formulation of [4] overlooked the case of $-T_d(x)$. Notice that d and T_d have the same parity, and hence it is immediate to see that $G_\infty(-T_d(x), \zeta + \zeta^{-1})$ is abelian. However, $-T_d(x)$ and $T_d(x)$ are never conjugated over \bar{K} when d is odd.

is abelian if and only if (f, α) is K^{ab} -conjugated to (x^d, ζ) or $(\pm T_d(x), \zeta + \zeta^{-1})$, for some root of unity ζ .

This survey is devoted to illustrate three approaches, based on very different strategies, that have been used to prove several cases of Conjecture 2. Notice that since power and Chebyshev maps are both PCF, a natural idea in order to prove Conjecture 2 is to start by proving that if $G_\infty(f, \alpha)$ is abelian then f is PCF. If the base field K is fixed there are only finitely many \bar{K} -conjugacy classes of PCF rational maps of degree d , outside the flexible Lattès locus (see [6]), that contains no polynomials. Hence showing the above implication already reduces considerably the complexity of the problem: for example when $K = \mathbb{Q}$ and $d = 2$ the only PCF polynomials are (up to conjugacy over \mathbb{Q}) $x^2, x^2 - 1$ and $x^2 - 2$. The approaches described in sections 2 and 3 both follow this route, while the third one uses a completely different strategy.

2. Height pairing approach

In this section we illustrate the route taken by the authors of [4], which proved the following theorem. Recall that if K is a field, $f \in K[x]$ and $\alpha \in K$ the pair (f, α) is said to be *stable* if for every $n \geq 1$ the polynomial $f^n - \alpha$ is irreducible over K .

THEOREM 2. *Conjecture 2 holds true when $K = \mathbb{Q}$, $f \in \mathbb{Q}[x]$ is a quadratic polynomial and $\alpha \in \mathbb{Q}$ is such that (f, α) is stable.*

As explained in the Introduction, the first step is to be able to reduce to the PCF case. This is done in [4, Theorem 8], where the authors prove that if $f \in K[x]$ is quadratic, K is a number field, (f, α) is stable and $G_\infty(f, \alpha)$ is abelian, then f is PCF. However, as we will see in Section 3, it is possible to remove the stability hypothesis by following a different approach. Theorem 2 is superseded by Theorems 5 and 7, but it is nevertheless interesting to understand the proof strategy, as it is completely different from that of the aforementioned theorems.

The PCF reduction argument implies that in order to prove Theorem 2 it is enough to show that if $f \in \{x^2, x^2 - 1, x^2 - 2\}$ and $\alpha \in \mathbb{Q}$ is such that (f, α) is stable and $G_\infty(f, \alpha)$ is abelian, then Conjecture 2 holds true. Notice that $x^2 - 2$ is the Chebyshev polynomial of degree 2. The hard part of the proof is to show that $G_\infty(x^2 - 1, \alpha)$ cannot be abelian.

In order to explain the proof strategy, let us start with the toy case $f = x^d \in K[x]$, with $d \geq 2$, K a number field and $\alpha \in K^\times$ (notice that 0 is an exceptional point for x^d). Theorem 1 says that $G_\infty(x^d, \alpha)$ is abelian if and only if α is a root of unity. Sufficiency is obvious, so now assume that $G_\infty(x^d, \alpha)$ is abelian. This is equivalent to saying that the whole backward orbit of α is contained in K^{ab} . Now observe that if $\gamma_n \in \bar{K}$ is such that

$f^n(\gamma_n) = \alpha$ for some $n \geq 1$, then

$$h(\gamma_n) = \frac{1}{d^n} h(\alpha),$$

where $h(\cdot)$ is the absolute logarithmic Weil height. Hence if $\{\gamma_n\}_{n \geq 0} \subseteq \overline{K}$ is a sequence of algebraic numbers with $\gamma_0 = \alpha$ and $f^n(\gamma_n) = \alpha$ for every $n \geq 1$, then $h(\gamma_n) \rightarrow 0$ as $n \rightarrow +\infty$. Now the key tool is the following theorem of Amoroso and Zannier [2].

THEOREM 3. *Let K be a number field. There exists a positive constant c_K such that if $\gamma \in K^{ab}$ is not zero nor a root of unity, then $h(\gamma) \geq c_K$.*

Hence the fact that all the γ_n 's belong to K^{ab} and their heights tend to zero implies that they must all be roots of unity, and in turn α must be a root of unity.

Of course the argument for $\pm T_d(x)$ is also very similar, using the fact that $T_d(x+x^{-1}) = x^d + x^{-d}$.

Now the idea for proving that if $\alpha \in \mathbb{Q}$ and $(x^2 - 1, \alpha)$ is stable then $G_\infty(x^2 - 1, \alpha)$ cannot be abelian is similar in spirit, but it uses more sophisticated tools. The first one is the so-called *Call-Silverman canonical height* (see [24, Chapter 3]), which is a function $\widehat{h}_\phi : \overline{K} \rightarrow \mathbb{R}_{\geq 0}$ associated to a polynomial $\phi \in K[x]$ where K is a number field. This is defined as follows: let $\phi \in K[x]$ be a degree d polynomial and let $\gamma \in \overline{K}$. Then

$$\widehat{h}_\phi(\gamma) := \lim_{n \rightarrow \infty} \frac{h(\phi^n(\gamma))}{d^n}.$$

This can be viewed as a dynamical generalization of the absolute logarithmic Weil height, and in fact it differs from it by a bounded amount. Notice that on the one hand we have that $\widehat{h}_{x^d} = h$, and on the other one $\widehat{h}_\phi(\phi(\gamma)) = d \cdot \widehat{h}_\phi(\gamma)$. An algebraic number γ satisfies $\widehat{h}_\phi(\gamma) = 0$ if and only if it is preperiodic for ϕ ; this is consistent with the fact that preperiodic points of x^d are exactly 0 and roots of unity. A crucial property of the Call-Silverman height is that it decomposes as a (weighted) sum of local components $\lambda_{\phi,v}$ for each place v of K .

The next crucial ingredient in the proof is the *Arakelov-Zhang pairing*. This is defined, for two polynomials $\phi, \psi \in K[x]$ as

$$\langle \phi, \psi \rangle := \sum_v \int_{\mathbb{C}_v} \lambda_{\psi,v} d\mu_{\phi,v}.$$

Here the sum is over all places v of K , while $\mu_{\phi,v}$ is the canonical measure associated to ϕ , and is a ϕ -invariant Borel unit measure supported on the filled Julia set of ϕ . It is not important for the purpose of this paper to go into detail about it, the interested reader can refer to [5, 8, 21]. The Arakelov-Zhang pairing has three key properties: it is non-negative, it is

symmetric and if $\{\gamma_n\}_{n \in \mathbb{N}} \subseteq \bar{K}$ is a sequence of points such that $\widehat{h}_\phi(\gamma_n) \rightarrow 0$, then $\widehat{h}_\psi(\gamma_n) \rightarrow \langle \phi, \psi \rangle$ (see [21]).

The properties of the Call-Silverman height and the Arakelov-Zhang pairing suggest a strategy to prove Theorem 2. In fact, suppose that $\alpha \in \mathbb{Q}$ is such that $G_\infty(x^2 - 1, \alpha)$ is abelian, and let $\{\gamma_n\}_{n \geq 0} \subseteq \bar{\mathbb{Q}}$ be a sequence of points such that $\gamma_0 = \alpha$ and $\gamma_n^2 - 1 = \gamma_{n-1}$ for every $n \geq 1$. Then $\widehat{h}_{x^2-1}(\gamma_n) \rightarrow 0$, and therefore $h(\gamma_n) = \widehat{h}_{x^2}(\gamma_n) \rightarrow \langle x^2 - 1, x^2 \rangle$, that is a positive constant (see [21]) and it can be numerically approximated, as explained in [4]. On the other hand, since all γ_n 's belong to \mathbb{Q}^{ab} , their logarithmic Weil height must be either zero or at least the constant $c_{\mathbb{Q}}$ arising from Theorem 3. If now we are lucky enough that $\langle x^2, x^2 - 1 \rangle < c_{\mathbb{Q}}$, the theorem is proven. Unfortunately, this is not the case. However, the hypothesis under which Andrews-Petsche work, namely the fact that $(x^2 - 1, \alpha)$ is stable, allows to show, using ramification theory, that if $G_\infty(x^2 - 1, \alpha)$ is abelian then $\mathbb{Q}_\infty(x^2 - 1, \alpha) \subseteq \mathbb{Q}(\zeta_{2^\infty})$. Clearly since Theorem 3 holds for \mathbb{Q}^{ab} then it holds for $\mathbb{Q}(\zeta_{2^\infty})$ with a larger constant. It turns out that such constant is computable, and is indeed larger than $\langle x^2, x^2 - 1 \rangle$, completing the proof of Theorem 2.

3. Group theoretic approach

The approach taken by the author and Pagano in [12] is of a completely different nature than the one described in Section 2. In fact, it is based on the group-theoretical properties of $\text{Aut}(T_\infty(f, \alpha))$ when f is quadratic. Let Ω_∞ denote, from now on, the group of automorphisms of the infinite, regular, rooted binary tree (see [11] for details about the structure of the group). The reason why the quadratic case differs heavily from the general one is that Ω_∞ is a pro-2-group, and therefore its structure is far more accessible than in the general case.

Elements of Ω_∞ can be uniquely identified by their *portrait*. If $\sigma \in \Omega_\infty$, its portrait is an infinite sequence of the following form:

$$(\varepsilon_1^1, \varepsilon_1^2 \varepsilon_2^2, \varepsilon_1^3 \varepsilon_2^3 \varepsilon_3^3 \varepsilon_4^3, \dots, \varepsilon_1 \dots n, \dots),$$

where $\varepsilon_i^j \in \mathbb{F}_2$ for every i, j . This has a very clear combinatorial interpretation: at each level n of the tree, if the 2^{n-1} pairs of brother nodes are labeled from 1 to 2^{n-1} , the symbol ε_i^n determines whether the nodes of the i -th pair are swapped by σ or not. If $\sigma = 1$ they are swapped, otherwise they are not. See Figure 1 for how to picture the portrait of an element $\sigma = (1, 01, 1010, \dots)$.

The portrait is a very useful tool for thinking about elements of Ω_∞ . In [12] we showed that for every $n \geq 1$ there is a continuous surjective homomorphism

$$\phi_n: \Omega_\infty \rightarrow \mathbb{F}_2$$

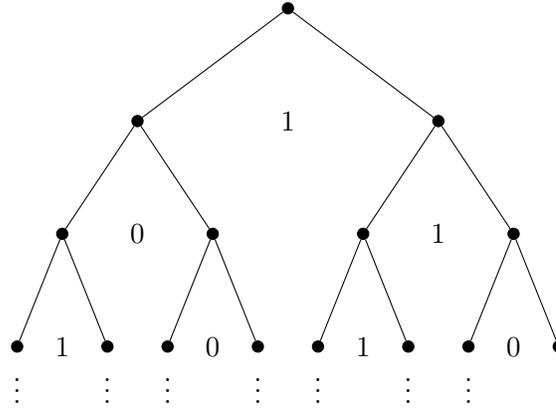


Figure 1: The portrait of an element $\sigma = (1, 01, 1010, \dots)$. If we label from 1 to 8, from left to right, the nodes at distance 3 from the root, σ corresponds to the permutation $(1736)(2845)$ on those nodes.

$$\sigma = (\varepsilon_1^1, \varepsilon_1^2 \varepsilon_2^2, \dots) \mapsto \sum_{i=1}^{2^{n-1}} \varepsilon_i^n,$$

and the \mathbb{F}_2 -vector space $\text{hom}_{\text{cont}}(\Omega_\infty, \mathbb{F}_2)$ is generated by the ϕ_n 's. This allows for a compact description of maximal subgroups of Ω_∞ : they are precisely those of the form $\ker \sum_{i \in I} \phi_i$, where $I \subseteq \mathbb{N}$ is a finite subset. Moreover, the commutator subgroup $[\Omega_\infty, \Omega_\infty]$ coincides with $\bigcap_{n \geq 1} \ker \phi_n$, and there is an isomorphism $\Omega_\infty^{\text{ab}} \xrightarrow{\cong} \prod_{n \geq 1} \mathbb{F}_2$. The composite map $\psi: \Omega_\infty \twoheadrightarrow \Omega_\infty^{\text{ab}} \rightarrow \prod_{n \geq 1} \mathbb{F}_2$ is given by $\sigma \mapsto (\phi_1(\sigma), \phi_2(\sigma), \dots, \phi_n(\sigma), \dots)$. This fact can be used to prove the following very useful lemma.

PROPOSITION 1 ([13, Proposition 7.3]). *Let $\sigma, \tau \in \Omega_\infty$ and suppose that $\phi_1(\sigma) = 1$. If $\psi(\sigma)$ and $\psi(\tau)$ are linearly independent vectors in the \mathbb{F}_2 -vector space $\prod_{n \geq 1} \mathbb{F}_2$, then σ and τ do not commute.*

It is an immediate consequence that if $G \leq \Omega_\infty$ is abelian and there is at least one $\sigma \in G$ with $\phi_1(\sigma) = 1$, then $\psi(G)$ is an \mathbb{F}_2 -vector space of dimension 1.

Clearly this forces a very restrictive condition on the nature of abelian subgroups of Ω_∞ ; the problem is how to translate it on a condition on (f, α) in order for $G_\infty(f, \alpha)$ to be abelian. From now on, suppose that K is a field of characteristic not 2, let $f \in K[x]$ be a monic, quadratic polynomial and $\alpha \in K$ be an element such that $f^{-\infty}(\alpha)$ contains no ramification points for f , so that the image of the arboreal representation $\rho_{f, \alpha}: G_K \rightarrow \text{Aut}(T_\infty(f, \alpha))$ can be identified with a closed subgroup of Ω_∞ . Up to conjugation over K , we can always assume that $f = x^2 + c$ for some $c \in K$. Recall that the *adjusted post-critical orbit* of f is the se-

quence $\{c_n\}_{n \geq 1} \subseteq K$ given by $c_1 = -c$, $c_n = f(c_{n-1})$ for every $n \geq 2$. We denote by $\{c_{n,\alpha}\}$ the sequence defined by $c_{1,\alpha} = c_1 + \alpha$ and $c_{n,\alpha} = c_n - \alpha$ for every $n \geq 2$. Now the link between the group theoretical properties of Ω_∞ and the structure of $\rho_{f,\alpha}$ is provided by the following proposition.

PROPOSITION 2. [13, Proposition 4.2] *Let $I \subseteq \mathbb{N}$ be a finite subset. The image of $\rho_{f,\alpha}$ is contained in $\ker(\sum_{i \in I} \phi_i)$ if and only if $\prod_{i \in I} c_i \in K^2$.*

Propositions 1 and 2 together imply immediately the following theorem.

THEOREM 4. *If $\text{Im } \rho_{f,\alpha}$ is an abelian subgroup of Ω_∞ and $f - \alpha$ is irreducible over K , then the sub- \mathbb{F}_2 -space generated by the sequence $\{c_{n,\alpha}\}$ inside the \mathbb{F}_2 -vector space $K^\times / K^{\times 2}$ is 1-dimensional.*

When K is a number field the 1-dimensionality condition given by Theorem 4 is a heavy constraint on the arithmetic of f . In fact it is a standard expectation in arithmetic dynamics that if the orbit of 0 is infinite, i.e. if f is *post-critically infinite*, then all but finitely many elements of the sequence $\{c_{n,\alpha}\}$ admit a primitive prime divisor with odd valuation, and this is a theorem (with certain extra assumptions) under the abc conjecture (see [15]). A standard application of Faltings' theorem on rational points on curves of high genus shows easily that when K is a number field such 1-dimensionality condition implies that f must be PCF. A couple of observations show that for the sake of this implication it is possible to remove the conditions on $f^{-\infty}(\alpha)$ not to contain ramification points and on $f - \alpha$ to be irreducible; one therefore obtains the following corollary.

COROLLARY 1. *Let K be a number field, let $\alpha \in K$ and let $f \in K[x]$ be a quadratic polynomial. If $G_\infty(f, \alpha)$ is abelian, then f is PCF.*

However one should absolutely not overlook the conclusion on the 1-dimensionality of the span of $\{c_{n,\alpha}\}$ given by Theorem 4 for two reasons: in the first place, it is useful in proving that $G_\infty(f, \alpha)$ is not abelian for a given pair (f, α) , and in the second place it is extremely versatile because it holds over any number field, and not just over \mathbb{Q} .

Hence when $K = \mathbb{Q}$ and $f \in \mathbb{Q}[x]$ is quadratic we are again reduced to study the three polynomials $x^2, x^2 - 2$ and $x^2 - 1$, but as we already explained in Section 2 the only hard case is $x^2 - 1$. In [12] we took once again a completely different route than the one used in [4]. Our idea was that in order for the group $G_\infty(x^2 - 1, \alpha)$ to be abelian, it needs to be locally abelian at every prime. In particular since $G_\infty(x^2 - 1, \alpha)$ is a pro-2-group, if p is an odd prime then local class field theory implies that the extension $(\mathbb{Q}_p)_\infty(x^2 - 1, \alpha)$ must be finitely ramified. A general result of Anderson et al. [3, Lemma 7.1, Theorem 7.4] shows that if p is odd then for

$(\mathbb{Q}_p)_\infty(x^2 - 1, \alpha)$ to be finitely ramified one needs $v_p(\alpha) = v_p(\alpha + 1) = 0$, where v_p is the usual p -adic valuation. But clearly there are only finitely many rational α 's that satisfy this condition at every odd prime: they are $0, -1, 1, -2, -1/2$. Now one can rule these values out by ad hoc arguments, or by explicitly computing the Galois groups of the first few iterates. Let us remark that this is an example of the usefulness of Theorem 4: for example when $\alpha = -1/2$ one has $c_{1,\alpha} = 1/2 = c_{2,\alpha}$ while $c_{3,\alpha} = -1/2$. Now clearly the subspace of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ spanned by $1/2$ and $-1/2$ has dimension 2, and therefore $G_\infty(x^2 - 1, -1/2)$ cannot be abelian (in fact, Theorem 4 can also be stated at a finite level, so that in this case the group $G_3(x^2 - 1, -1/2)$ is already non-abelian).

All in all, these arguments prove the following theorem.

THEOREM 5. *Conjecture 2 holds true for every pair (f, α) with $f \in \mathbb{Q}[x]$ quadratic and $\alpha \in \mathbb{Q}$.*

In a forthcoming work of the author and Pagano, we will in fact use the same approach to show that the same result holds true for quadratic polynomials over any quadratic field.

We also remark that thanks to the great generality of Theorem 4, one can also prove the following result.

THEOREM 6 ([12, Theorem 3.13]). *Let K be a global function field of odd characteristic p , let $f \in K[x]$ be quadratic and $\alpha \in K$. Then $G_\infty(f, \alpha)$ is abelian if and only if (f, α) is K -conjugated to a pair (g, β) with $g \in \overline{\mathbb{F}}_p[x]$ and $\beta \in \overline{\mathbb{F}}_p$.*

4. Unlikely intersection approach

The idea behind this approach had been introduced by Dvornicich and Zannier in [10], where it was used to study cyclotomic preperiodic points of rational functions. Later in [20] Ostafe used it to study cyclotomic points in backward orbits of rational functions. This technique is quite powerful, and as we will see it implies the validity of Conjecture 2 for $K = \mathbb{Q}$. The downside however is that at the present time there is no hope of generalizing it to number fields other than \mathbb{Q} .

In order to state the result, let us introduce some notation. Let K be a number field, $\alpha \in K$ and $\phi \in K(x)$ be a rational function of degree $d \geq 2$. Let K^c be the cyclotomic closure of K inside a fixed algebraic closure \overline{K} . We say that the pair (ϕ, α) is *special* if it is K^c -conjugate to one of the following pairs: $\{(x^{\pm d}, \zeta), (\pm T_d(x), \zeta + \zeta^{-1})\}$ where ζ is a root of unity. We recall that we denote by $\phi^{-\infty}(\alpha)$ the backward orbit of α , namely the set of all $\gamma \in \overline{K}$ such that $\phi^n(\gamma) = \alpha$ for some $n \geq 0$.

THEOREM 7 ([20, pp. 1933–1935]). *Let $\phi = f/g \in K(x)$, where $f, g \in K[x]$ are coprime polynomials. Suppose that $\deg f > \deg g + 1$ and that (ϕ, α) is not a special pair. Then $\phi^{-\infty}(\alpha) \cap K^c$ is finite.*

In order to illustrate the proof of this theorem, we need three preliminary results. The first one relies crucially on the hypothesis $\deg f > \deg g + 1$ that, from a dynamical point of view, says that ∞ is a superattracting fixed point for ϕ . Recall that the *house* of an algebraic number γ is defined as $|\overline{\gamma}| := \max_{\sigma: \mathbb{Q}(\gamma) \rightarrow \mathbb{C}} |\sigma(\gamma)|$.

LEMMA 1 ([20, Corollaries 2.6 and 2.8]). *Let $\gamma \in \phi^{-\infty}(\alpha)$.*

1. *There exists a positive constant H , depending on K, ϕ, α , such that $|\overline{\gamma}| \leq H$.*
2. *There exists a positive integer D , depending on K, ϕ, α , such that $D \cdot \gamma$ is an algebraic integer.*

Let us briefly explain the idea behind the above lemma. Since ∞ is superattracting, whenever v is a place of K and we consider ϕ as a rational map $\phi_v: \mathbb{P}_{K_v}^1 \rightarrow \mathbb{P}_{K_v}^1$, then ∞ stays superattracting (this fails as soon as ∞ is not superattracting, as if its multiplier is nonzero then for all but finitely many places ∞ becomes an indifferent point). Now let v be an archimedean place of K . Since ∞ is a superattracting point for $\phi_v: \mathbb{P}_{K_v}^1 \rightarrow \mathbb{P}_{K_v}^1$, then there exists a neighborhood U_v of ∞ such that $\phi_v(U_v) \subseteq U_v$ (see [7]). Hence it is clear that if U_v is chosen to be small enough so that $\alpha \notin U_v$, no point $\gamma \in U_v$ can be mapped to α by any iterate of ϕ . Of course lying outside of U_v , since the latter is a neighborhood of ∞ , translates into a bound on the absolute value of γ . Since there is a bound for every archimedean embedding, there is also a bound on the house. For non-archimedean places the situation is essentially the same. It is easy to see that there is a finite set S of places of K such that every point in the backward orbit of α is an S -integer: it is enough for S to contain all places where α or some coefficient of f or g has negative valuation. For primes in S the same argument of the archimedean case applies (see [7, Proposition 4.3]) and leads to the existence of a D as in Lemma 1. The constants H and D can be made explicit.

The second preliminary result is the following theorem, that is a generalization proven by Dvornicich-Zannier of a result of Loxton [18].

THEOREM 8 ([10, Theorem L]). *Let K be a number field. Then there exists a finite set $E \subseteq K$ with $|E| \leq [K: \mathbb{Q}]$ and an effective positive constant $B = B_K$ with the following property: if $\gamma \in K^c$ is an algebraic integer then there exist elements $c_1, \dots, c_b \in E$ and roots of unity $\zeta_1, \dots, \zeta_b \in K^c$ such that $\gamma = \sum_{i=1}^b c_i \zeta_i$, where $b \leq |E| \cdot L(B \cdot |\overline{\gamma}|)$ for any Loxton function $L: \mathbb{R} \rightarrow \mathbb{R}$. Moreover, both E and B can be effectively computed in terms of a basis for K/\mathbb{Q} .*

Lemma 1 and Theorem 8 easily imply the following corollary.

COROLLARY 2. *Under the hypotheses of Theorem 7, there exists a finite set $E \subseteq K$ and an effective positive constant B with the following property: if $\gamma \in \phi^{-\infty}(\alpha) \cap K^c$ then there exist elements $c_1, \dots, c_B \in E$ and roots of unity $\zeta_1, \dots, \zeta_B \in K^c$ such that $\gamma = \sum_{i=1}^B c_i \zeta_i$.*

The third preliminary result is the following theorem of Fuchs and Zannier.

THEOREM 9 ([14, Corollary]). *Let K be a number field and $h \in K(x)$ be a rational function of degree $d \geq 2$ that is not \bar{K} -conjugate to $x^{\pm d}$ or to $\pm T_d(x)$. Then for every integer $n \geq 3$ and every non-constant $q \in K(x)$, the function $h^n(q(x))$ cannot be expressed by a ratio of polynomials having altogether less than $\frac{1}{\log 5}((n-2)\log d - \log 2016)$ terms.*

Now let us explain how the proof of Theorem 7 works. From now on, suppose that ϕ is not \bar{K} -conjugate to $x^{\pm d}$ or $\pm T_d(x)$, filling in the remaining cases is rather elementary. Suppose by contradiction that $\phi^{-\infty}(\alpha) \cap K^c$ is infinite. Let M be a positive integer, and consider the equation

$$(1) \quad \phi^M(z_1) = z_2,$$

where $z_1, z_2 \in \phi^{-\infty}(\alpha) \cap K^c$. Since the latter set is infinite, there exist infinitely many pairs (z_1, z_2) , with both z_i 's in the set, that satisfy equation (1). On the other hand, by Corollary 2 all elements of these pairs can be represented as $\sum_{i=1}^B c_i \zeta_i$, where the c_i 's are chosen in a finite set E . By the pigeonhole principle, this means that there exist $\bar{c}_1, \dots, \bar{c}_B \in E$ such that there are infinitely many pairs (z_1, z_2) that satisfy equation (1) and such that both z_1 and z_2 can be expressed as $\sum_{i=1}^B \bar{c}_i \zeta_i$ for some choice of roots of unity ζ_1, \dots, ζ_B . But this shows that the hypersurface

$$S: \phi^M \left(\sum_{i=1}^B \bar{c}_i x_i \right) - \sum_{i=1}^B \bar{c}_i y_i = 0 \subseteq \mathbb{G}_m^{2B}$$

has infinitely many torsion points. By the torsion coset theorem, the Zariski closure of the subset of torsion points must therefore contain a torsion coset of dimension 1, and it is easy to see that one can choose it in such a way that it is not mapped to a constant via the map $S \rightarrow \mathbb{P}^1$ that sends $(\bar{x}_1, \dots, \bar{x}_B, \bar{y}_1, \dots, \bar{y}_B)$ to $\sum_{i=1}^B \bar{c}_i \bar{x}_i$. This means that if we parametrize such coset by writing $x_i = \zeta_i t^{e_i}$ and $y_j = \zeta_j t^{e_j}$, where ζ_i, ζ_j are roots of unity and e_i, e_j are integers, not all zero, we get the following identity of rational functions:

$$(2) \quad \phi^M \left(\sum_{i=1}^B \bar{c}_i \zeta_i t^{e_i} \right) = \sum_{j=1}^B \bar{c}_j \zeta_j t^{e_j}.$$

However, M is arbitrary. Hence if we choose it to be large enough with respect to B , we obtain a representation of the rational function $\phi^M \circ q(t)$, where $q(t) = \sum_{i=1}^B \bar{c}_i \zeta_i t^{e_i}$, as a rational function (namely the RHS of (2)) that is a ratio of polynomials with altogether at most $B + 1$ nonzero terms. Since ϕ is not \bar{K} -conjugate to $x^{\pm d}$ or $\pm T_d(x)$, this contradicts Theorem 9.

Clearly, Theorem 7 implies the following corollary.

COROLLARY 3. *Conjecture 2 holds true for any pair (f, α) where $f \in \mathbb{Q}[x]$ and $\alpha \in \mathbb{Q}$.*

It is clear how powerful Theorem 7 is, as it implies a far stronger result than that of Conjecture 2, for rational functions over the rationals. In fact, it is not unreasonable to expect that such conjecture holds true even for pairs (ϕ, α) with $\alpha \in \mathbb{Q}$ and $\phi \in \mathbb{Q}(x)$, once one adds to the statement the obvious extra case of (ϕ, α) being \mathbb{Q}^c -conjugate to (x^{-d}, ζ) . On the other hand, one cannot expect Conjecture 2 to hold true for rational functions over any number field, as the theory of complex multiplication shows that there are infinitely many examples of Lattès maps (that are never conjugated to $x^{\pm d}$ or $\pm T_d(x)$) that give rise to abelian dynamical Galois groups.

References

- [1] Faseeh Ahmad, Robert Benedetto, Jennifer Cain, Gregory Carroll, and Lily Fang. The arithmetic basilica: a quadratic PCF arboreal galois group. *J. Number Theory (to appear)*, 2021.
- [2] Francesco Amoroso and Umberto Zannier. A uniform relative Dobrowolski’s lower bound over abelian extensions. *Bull. Lond. Math. Soc.*, 42(3):489–498, 2010.
- [3] Jacqueline Anderson, Spencer Hamblen, Bjorn Poonen, and Laura Walton. Local arboreal representations. *Int. Math. Res. Not. IMRN*, (19):5974–5994, 2018.
- [4] Jesse Andrews and Clayton Petsche. Abelian extensions in dynamical Galois theory. *Algebra Number Theory*, 14(7):1981–1999, 2020.
- [5] Matthew H. Baker and Robert Rumely. Equidistribution of small points, rational dynamics, and potential theory. *Ann. Inst. Fourier (Grenoble)*, 56(3):625–688, 2006.
- [6] Robert Benedetto, Patrick Ingram, Rafe Jones, and Alon Levy. Attracting cycles in p -adic dynamics and height bounds for postcritically finite maps. *Duke Math. J.*, 163(13):2325–2356, 2014.
- [7] Robert L. Benedetto. *Dynamics in one non-archimedean variable*, volume 198 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2019.

- [8] Antoine Chambert-Loir. Mesures et équidistribution sur les espaces de Berkovich. *J. Reine Angew. Math.*, 595:215–235, 2006.
- [9] Andrea Conti, Jaclyn Lang, and Anna Medvedovsky. Big images of two-dimensional pseudorepresentations. <https://arxiv.org/abs/1904.10519>, 2021.
- [10] R. Dvornicich and U. Zannier. Cyclotomic Diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps). *Duke Math. J.*, 139(3):527–554, 2007.
- [11] Andrea Ferraguti. The set of stable primes for polynomial sequences with large Galois group. *Proc. Amer. Math. Soc.*, 146(7):2773–2784, 2018.
- [12] Andrea Ferraguti and Carlo Pagano. Constraining images of quadratic arboreal representations. *Int. Math. Res. Not. IMRN*, (22):8486–8510, 2020.
- [13] Andrea Ferraguti, Carlo Pagano, and Daniele Casazza. The inverse problem for arboreal galois representations of index two (submitted). <https://arxiv.org/abs/1907.08608>, 2019.
- [14] Clemens Fuchs and Umberto Zannier. Composite rational functions expressible with few terms. *J. Eur. Math. Soc. (JEMS)*, 14(1):175–208, 2012.
- [15] C. Gratton, K. Nguyen, and T. J. Tucker. *ABC* implies primitive prime divisors in arithmetic dynamics. *Bull. Lond. Math. Soc.*, 45(6):1194–1208, 2013.
- [16] Rafe Jones. Galois representations from pre-image trees: an arboreal survey. In *Actes de la Conférence “Théorie des Nombres et Applications”*, volume 2013 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 107–136. Presses Univ. Franche-Comté, Besançon, 2013.
- [17] Jamie Juul, Holly Krieger, NicoleLooper, Michelle Manes, Bianca Thompson, and Laura Walton. Arboreal representations for rational maps with few critical points. In *Research directions in number theory—Women in Numbers IV*, volume 19 of *Assoc. Women Math. Ser.*, pages 133–151. Springer, Cham, [2019] ©2019.
- [18] J. H. Loxton. On the maximum modulus of cyclotomic integers. *Acta Arith.*, 22:69–85, 1972.
- [19] A. Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. <https://arxiv.org/abs/1809.02584>, 2019.
- [20] Alina Ostafe. On roots of unity in orbits of rational functions. *Proc. Amer. Math. Soc.*, 145(5):1927–1936, 2017.
- [21] Clayton Petsche, Lucien Szpiro, and Thomas J. Tucker. A dynamical pairing between two rational maps. *Trans. Amer. Math. Soc.*, 364(4):1687–1710, 2012.

- [22] Richard Pink. Profinite iterated monodromy groups arising from quadratic morphisms with infinite postcritical orbits. <https://arxiv.org/abs/1309.5804>, 2013.
- [23] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.
- [24] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

2020 Mathematics Subject Classification. Primary 37P05,37P15, 11R18; Secondary 11G50.

Andrea Ferraguti,
Scuola Normale Superiore,
Piazza dei Cavalieri 7, 56126 Pisa e-mail: and.ferraguti@gmail.com

Lavoro pervenuto in redazione il 06.06.2022.