Pure and Applied Mathematics Quarterly
Volume 5, Number 1
(*Special Issue: In honor of
Jean-Pierre Serre, Part 2 of 2*)
213—225, 2009

The Image of an Arboreal Galois Representation

Nigel Boston and Rafe Jones

Abstract: Much is known regarding images of p-adic Galois representations coming from subquotients of étale cohomology groups of varieties over number fields. In particular, the Mumford-Tate conjecture gives them up to subgroups of finite index, and has been proved in many cases by Serre and others. In the analogous situation of arboreal Galois representations little is known. In this paper we give a conjectural description of their images in the case that they arise via iteration of a given polynomial. We also discuss in depth the case of iteration of a quadratic polynomial with integer coefficients.

Keywords: Galois representation, rooted tree, iteration.

1. Arboreal Representations

There are two main sources of totally disconnected, locally compact groups, namely matrix groups over local fields and automorphism groups of locally finite trees [23]. Continuous homomorphisms of Galois groups into the former have been well studied and exploited but those into the latter have barely been touched upon.

If K is a number field, S a finite set of primes of K, K^S a maximal algebraic extension of K unramified outside S, and $G = \mathrm{Gal}(K^S/K)$, the Fontaine-Mazur conjecture [5] characterizes those representations $G \to GL_n(\mathbf{Z}_p)$ coming from algebraic geometry by the group-theoretical condition of being potentially

Received August 10, 2006.

semistable at p. In the case that S contains no prime lying above p, the conjecture states that every such representation should have finite image. This state of affairs is unsatisfactory in that for many K and S the group G has an infinite pro-p quotient, which therefore cannot be seen by a p-adic Galois representation. A refinement, the virtual Golod-Shafarevich conjecture [2], implies that in such cases there should exist representations $G \to \mathrm{Aut}(T)$ with image having nonzero Hausdorff dimension (see below for its definition), where T is a locally finite, rooted tree. We call such representations *arboreal*.

This source of arboreal Galois representations is hard to control. In particular, there is not one infinite finitely, tamely ramified p-extension whose Galois group has been explicitly presented. A more explicit source of arboreal Galois representations is given by the Galois action on the roots of the iterates of a given polynomial. In this paper we consider the images of such representations, mostly in the case of quadratic polynomials.

Let f be a degree d polynomial in $\mathbf{Q}[x]$, all of whose iterates are separable. The roots of the nth iterate f^n of f can be identified with the d^n vertices at level n of the d-ary rooted tree T, in such a way that the Galois group of f^n embeds in $\mathrm{Aut}(T_n)$ where T_n consists of the subtree of vertices up to and including level n. Putting these embeddings together yields a continuous homomorphism $G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(T)$, whose image $G(f)$ is the Galois group over $\mathbf{Q}$ of the extension generated by all roots of all iterates of f. The Galois group of f^n will be denoted $G_n(f)$. All $G_n(f)$ will be transitive if and only if every iterate of f is irreducible, in which case (as is typical in this paper) we call $G(f)$ spherically transitive.

The main focus of this paper is the identification of and properties of $G(f)$ as a subgroup of $\mathrm{Aut}(T)$. In particular, we focus on the case $d = 2$ In this case, $\mathrm{Aut}(T_n)$ is a 2-group, in fact a Sylow 2-subgroup of $\mathrm{Sym}(2^n)$ so of order 2^{2^n-1}, whence $G_n(f)$ is a 2-group. The main measure of the size of $G(f)$ is its Hausdorff dimension, given by the liminf of $\log_2(|G_n(f)|/(2^n-1))$.

After presenting some analogies with p-adic representations in Section 2, we discuss some general properties that $G(f)$ must obey in Section 3. In Section 4 we examine the possibilities for $G(f)$ when $f \in \mathbf{Z}[x]$ is quadratic. We decompose the set of such f into natural families and compute the generic Galois group over $\mathbf{Q}(t)$ for each of these families. For each family, we then examine specializations

of t, and we conjecture the resulting group must have finite index in the generic group. In Section 5 we summarize our main conjectures.

2. Analogies with p-adic Galois Representations

If V is a smooth projective variety over $\mathbf{Q}$, then its étale cohomology groups [12] are p-adic vector spaces on which $G_{\mathbf{Q}}$ acts. These and their subquotients yield representations $G_{\mathbf{Q}} \to GL_n(\mathbf{Q}_p)$, which we say come from algebraic geometry. Since there is always a stable lattice, this in turn produces representations $G_{\mathbf{Q}} \to GL_n(\mathbf{Z}_p)$. The most important examples are the 1-dimensional (cyclotomic) representations given by Galois action on the p^nth roots of 1, the 2-dimensional representations given by Galois action on the p^n-division points of an elliptic curve, and the 2-dimensional representations associated to modular forms arising as subquotients of the Galois action on the p^n-division points of Jacobians of modular curves.

In analyzing these representations the main questions concern the size of the image and the nature of the images of Frobenius elements. In general, for representations coming from algebraic geometry, the image is conjecturally determined up to finite index subgroups by the p-adic points of a Hodge (or Mumford-Tate) group. The first such results concerned CM elliptic curves, whose Galois representations have image the normalizer of a Cartan subgroup of $GL_2(\mathbf{Z}_p)$. Serre [18] showed that elliptic curves without CM have Galois representations whose image is of finite index in $GL_2(\mathbf{Z}_p)$. Other cases of the Mumford-Tate conjecture have been established by Deligne [4], Serre [19], [20], [21], and Chi [3].

Analogues for Galois representations associated to Drinfeld modules have been discovered by Pink [16]. Our goal is to shed light on these same questions in the case of arboreal Galois representations associated to the iterates of a given polynomial and to observe analogous phenomena.

3. Densely settled subgroups

Let the notation be as on p. 214. We focus on the case where f is a polynomial with integer coefficients. Let ρ_f denote the continuous homomorphism $\mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(T)$ whose image is $G(f)$. In this section we discuss some

properties of $G(f)$, particularly in the case where f is quadratic, and give conjectures on other properties.

In [10] we conjecture that the image of ρ_f must possess a property known as *settledness* that depends on the cycle decomposition of the action of $G(f)$ on each level of T. Denote by V_n the vertices of T that are distance n from the root, or in other words the roots of f^n. Let $\sigma \in G(f)$, and denote by σ_n the restriction of σ to V_n. Call a cycle C of σ_n *stable* if for each $m \geq n$, the vertices of V_m above C all lie in a single cycle of σ_m of length $2^{m-n} \cdot |C|$, where $|C|$ denotes the length of C. In other words, if g is the irreducible factor whose roots comprise C, then $g(f^{m-n})$ is irreducible for all $m \geq n$. We say that σ is *settled* if the proportion of elements of V_n contained in stable cycles of σ_n goes to one as n grows. We say that $G(f)$ is *densely settled* if settled elements are dense in the profinite topology.

Let Frob_p be a Frobenius element at the prime p. Then the cycle decomposition of the action of Frob_p on the roots of f^n is given by the degrees of the irreducible factorization of $f^n \bmod p$. Since Frobenius elements are dense in $G(f)$ by the Tchebotarev Density Theorem, we can show that $G(f)$ is densely settled by showing that the irreducible factors of $f^n \bmod p$ are settled in a sense precisely analogous to the definition given in the previous paragraph. In [10] we conjecture that any irreducible quadratic over $\mathbf{F}_p$ is settled, and we give a heuristic argument and extensive computations in support of this conjecture. Indeed it seems likely that all separable polynomials over $\mathbf{F}_p$ are settled. From this it would follow that $G(f)$ is densely settled for all quadratic $f \in \mathbf{Z}[x]$.

However, while conjecturally $G(f)$ must be settled at least for quadratic f, this alone appears insufficient to characterize the possible images of ρ_f. Indeed, there are many abelian subgroups of $\mathrm{Aut}(T)$ that are settled, but very few can occur as $G(f)$ for quadratic $f \in \mathbf{Z}[x]$:

Call f *critically infinite* if the set $\{f^n(\gamma) : n = 1, 2, \ldots\}$, where γ is the critical point of f, is infinite.

Theorem 3.1. *Let $f \in \mathbf{Z}[x]$ be a critically infinite quadratic polynomial with all iterates irreducible. If $G(f)$ is abelian, then it is cyclic.*

Proof: Suppose that $G(f)$ is abelian, and denote by $G_n(f)$ the action of $G(f)$ on V_n. We claim that the center of $G_n(f)$ contains a unique element of order 2

for all but finitely many n. This claim immediately implies that $G_n(f)$ is cyclic for infinitely many n, and thus for all n. Hence $G(f)$ is cyclic.

To prove the claim, first note that in [8, Corollary 4.11 and remarks before] it is shown that if f^n is irreducible and Disc f^n is not a square in $\mathbf{Q}$, then the center of $G_n(f)$ contains a unique element of order 2. From [9, p. 10] we have that the squarefree part of Disc f^n is equal to the squarefree part of $f^n(\gamma)$. If there are infinitely many n with $y^2 = f^n(\gamma)$ for some $y \in \mathbf{Q}$, then since f is critically infinite, it follows that for all $k > 0$ there are infinitely many distinct $(x, y) \in \mathbf{Q}^2$ with $y^2 = f^k(x)$. Since f is assumed separable, k can be selected so the curve $Y^2 = f^k(X)$ has genus at least two. However, this violates Faltings' theorem [7, Part E].

As for quadratic f such that $\{f^n(\gamma) : n = 1, 2, \ldots\}$ is finite (such f are called *critically finite*), one can reproduce the proof of Theorem 3.1 provided that Disc f^n is not a square for infinitely many n. A straightforward calculation shows that all critically finite quadratic $f \in \mathbf{Z}[x]$ are of the form $(x-k)^2+k$, $(x-k)^2+k-1$, or $(x-k)^2+k-2$ for some $k \in \mathbf{Z}$. In each of these cases, Disc f^n is a square for all sufficiently large n only if k is a square, $k = 1$, or $k-2$ is a square respectively. For these values of f and k, the group $G_n(f)$ appears to be either cyclic, isomorphic to $(\mathbf{Z}/2^n\mathbf{Z})^*$, or nonabelian. This follows from the first part of Section 4.2 as well an examination of the cases $f = (x-k)^2+k$, $k = \pm 1$ and $(x-k)^2+k-2$, $|k| \leq 2$ and the fact that any finite index subgroup of $\mathbf{Z}_2 \rtimes \mathbf{Z}_2^*$, the group of invertible affine linear transformations of $\mathbf{Z}_2$, is nonabelian. Thus even when f is critically finite, only a very restricted set of abelian groups can occur as $G(f)$. This leads us to ask what additional properties besides settledness $G(f)$ should possess.

4. Quadratic Polynomials

4.1. **Generic quadratic families.** We now turn to a more detailed analysis of $G(f)$ in the case of quadratic $f \in \mathbf{Z}[x]$. Any such f may be written

$$f = (x-\gamma)^2 + \gamma + m, \tag{1}$$

where 2γ and $4m$ are integers. One easily checks that f is critically finite if and only if $m \in \{-2, -1, 0\}$. We now fix a value of m and consider all f whose

decomposition in (1) has the prescribed value of m. Let us describe the Galois groups for iterates of a generic such f.

Theorem 4.1. *Suppose $f = (x-t)^2 + t + m \in \mathbf{Q}(t)[x]$, where $m \notin \{0, -1, -2\}$. Let $G_n(f)$ be the Galois group over $\mathbf{Q}(t)$ of the splitting field of the nth iterate f^n, and let $G(f) = \varprojlim G_n(f)$. Then $G(f) \cong \mathrm{Aut}(T)$, where T is the infinite binary rooted tree of preimages of 0*

Proof: We first show that f^n is irreducible, and therefore separable, for all n. From [9, Proposition 3.3] we need only show that $f^n(t)$ is never a square in $\mathbf{Q}(t)$. This clearly holds, as $f^n(t)$ has degree one for each n.

We now wish to show that for all n, $G_n(f)$ is isomorphic to $\mathrm{Aut}(T_n)$, the group of automorphisms of the binary rooted tree of height n. It is well-known that $\mathrm{Aut}(T_n)$ is isomorphic to the n-fold iterated wreath product of $\mathbf{Z}/2\mathbf{Z}$, and in particular $|\mathrm{Aut}(T_n)| = 2^{2^n-1}$. Let K_n denote the splitting field of f^n over $\mathbf{Q}(t)$, and put $H_n = \mathrm{Gal}\,(K_n/K_{n-1})$. If we show that $|H_n| = 2^{2^{n-1}}$ for all n, then it follows by induction and comparison of degrees that $G_n \cong \mathrm{Aut}(T_n)$.

The argument in [9, Lemma 4.1] applies verbatim over $\mathbf{Q}(t)$, and putting $g = id$ in that Lemma shows that $|H_n| = 2^{2^{n-1}}$ if and only if $f^n(t)$ is not a square in K_{n-1}. Now the only primes of $\mathbf{Q}(t)$ (by which we mean a discrete valuation ring O_P with maximal ideal P) that ramify in K_n are those such that $\mathrm{Disc}\, K_n$ is zero in O_P/P [17, Proposition 7.9] and moreover if $\mathrm{Disc}\, f^n$ is not zero in O_P/P then $\mathrm{Disc}\, K_n$ is not zero in O_P/P (for the last assertion one can adapt the argument in [13, Corollary 2, p. 157]). It follows that the only primes ramifying in K_{n-1} are those with $\mathrm{Disc}\, f^{n-1} = 0$ in O_P/P, and by [9, p. 10] these are precisely the primes dividing $f^m(t)$ for some $m \leq n-1$.

To show that $\mathrm{Disc}\, f^n$ is not a square in K_{n-1}, we show that its squarefree part is divisible by a prime that does not ramify in K_{n-1}. By [9, p. 10] the squarefree part of $\mathrm{Disc}\, f^n$ is precisely the squarefree part of $f^n(t)$. In the case currently under consideration, $f^n(t)$ has degree 1 as a polynomial in t, and thus is squarefree. Moreover, since f is critically infinite by our assumption that $m \notin \{0, -1, -2\}$, the set $\{f^m(t) : m = 1, 2, \ldots\}$ consists of infinitely many distinct degree 1 polynomials, and thus all its elements are relatively prime to one another. It follows that $f^n(t)$ cannot divide $\mathrm{Disc}\, f^{n-1}$, and thus does not ramify in K_{n-1}. ■

We remark that if K is a number field and $\mathcal{O}_K$ is its ring of integers, then as in (1) every quadratic polynomial in $\mathcal{O}_K[x]$ can be written as $(x-\gamma)^2+\gamma+m$, where $2\gamma, 4m \in \mathcal{O}_K$. Moreover, if m is such that $f=(x-t)^2+t+m \in K(t)[x]$ is critically infinite, a straightforward adaptation of the proof of Theorem 4.1 shows that $G(f) \cong \mathrm{Aut}(T)$.

Theorem 4.2. *Using the notation of Theorem 4.1, suppose* $f=(x-t)^2+t+m \in \mathbf{Q}(t)[x]$, *where* $m \in \{0,-2\}$. *Then* $G(f) \cong \mathbf{Z}_2 \rtimes \mathbf{Z}_2^*$, *the group of invertible affine linear transformations of* $\mathbf{Z}_2$.

Proof: In the case $m=0$, we have $f^n = x^{2^n}-t$, whence the splitting field K_n of f^n over $\mathbf{Q}(t)$ is just $\mathbf{Q}(\sqrt[2^n]{t}, \zeta_{2^n})$. One now checks easily that f^n remains irreducible over $\mathbf{Q}(t, \zeta_{2^n})$, and thus $[K_n : \mathbf{Q}(t)] = 2^{2n-1}$. Therefore the map $\zeta_{2^n} \mapsto \zeta_{2^n}^a$, $\sqrt[2^n]{t} \mapsto \sqrt[2^n]{t}^b$ is an automorphism of $K_n/\mathbf{Q}(t)$ for all $a \in \mathbf{Z}/2^n\mathbf{Z}^*$ and all $b \in \mathbf{Z}/2^n\mathbf{Z}$. It follows that $\mathrm{Gal}\,(K_n/\mathbf{Q}(t))$ is isomorphic to the group of invertible affine linear transformations of $\mathbf{Z}/2^n\mathbf{Z}$ and thus $G(f)$ is isomorphic to the same group over $\mathbf{Z}_2$.

If $m=-2$, the proof is identical to that of part 1) of Theorem 1.1 in [6]. ■

Any extension L of $\mathbf{Q}(t)$ has a sub-extension $A=\overline{\mathbf{Q}} \cap L$ of $\mathbf{Q}$, which we call the *arithmetic part* of L (it is also the maximal constant field extension contained in L). We refer to the extension $L/A(t)$ as the *geometric part* of L. If L is the splitting field of a polynomial g, there is a natural isomorphism of $L/A(t)$ and $E/\mathbb{C}(t)$, where E is the splitting field over $\mathbb{C}(t)$ of g considered as a polynomial in $\mathbb{C}(t)[x]$. It now follows that if K_n is the splitting field over $\mathbf{Q}(t)$ of f^n for some $f \in \mathbf{Q}(t)[x]$, $L=\cup_n K_n$, and $E/\mathbb{C}(t)$ corresponds to $L/A(t)$, then the group $\mathrm{Gal}\,(E/\mathbb{C}(t))$ is isomorphic to the closure in $\mathrm{Aut}(T)$ of the iterated monodromy group of f over $\mathbb{C}$ (see [14, Chapter 5]). This last group may be computed using geometric methods. In the case of $f=(x-t)^2+t+m \in \mathbf{Q}(t)[x]$, $m \notin \{0,-1,-2\}$, the geometric part of L has Galois group $\mathrm{Aut}(T)$, while if $m \in \{0,-2\}$ then the geometric part of L has Galois group $\mathbf{Z}_2$. In the former case, this observation can be used to provide an alternate proof of Theorem 4.1

We now arrive at the lone m not treated in Theorems 4.1 and 4.2, namely $m=-1$. If $f=(x-t)^2+t-1$, K_n is the splitting field over $\mathbf{Q}(t)$ of f^n, and $L=\cup_n K_n$, then $\mathrm{Gal}\,(L/A(t))$ is isomorphic to the closure B of the Basilica

group in $\mathrm{Aut}(T)$. The Basilica group is a certain group generated by a finite automaton, and about which much is known [1] and which has a natural action on T. Unfortunately, much less seems to be known about B. Thus $G(f)$ has B as a normal subgroup, with quotient $\mathrm{Gal}\,(A/\mathbf{Q})$. It remains an open problem to determine $\mathrm{Gal}\,(A/\mathbf{Q})$ and to find the structure of $G(f)$ beyond the previous observation.

4.2. **Quadratic Specializations.** In the previous section, we examined generic behavior of ρ_f within certain families of quadratic f. In this section we focus on the behavior of ρ_f for specific f. The general theme is that specializations of t in Theorems 4.1 and 4.2 should yield Galois groups of finite index in the generic groups described in Theorems 4.1 and 4.2. This is reminiscent of work of Serre (e.g. [18]), where the Lie algebra of the Tate module of an elliptic curve determines the Tate module up to finite index.

Lemma 4.3. *Let F be a field containing a primitive kth root of unity ζ_k, and let $\alpha \in F$. Then $[F(\alpha^{1/k}) : F] = k/d$, where $1 \le d \le k$ is maximal such that $\alpha^{1/d} \in F$.*

Proof: Let $e := [F(\alpha^{1/k}) : F]$ and note that we have $\alpha^{e'/k} \notin F$ for all $e' < e$. Indeed, if $\alpha^{e'/k} \in F$ then $\alpha^{1/k}$ is a root of $x^{e'} - \alpha^{e'/k}$, whence $[F(\alpha^{1/k}) : F] \le e'$, a contradiction.

Now let $f(x) \in F[x]$ be an irreducible factor of $x^k - \alpha$, and let β be a root of f. Write $\beta = \zeta_k^i \alpha^{1/k}$ for some $1 \le i \le k$, and note that $F(\beta) = F(\alpha^{1/k})$ since F contains ζ_k. Thus $\mathrm{Gal}\,(F(\beta)/F)$ is cyclic of order e. It follows that

$$f(x) = \prod_{j=1}^{e} \left(x - \zeta_k^{i+(jk/e)} \alpha^{1/k}\right) = x^e - \zeta_k^{ei} \alpha^{e/k},$$

where the second equality is obtained by comparing roots. Thus $\alpha^{e/k} \in F$, proving that $1/d = e/k$. ■

Theorem 4.4. *Let $t_0 \in \mathbf{Z}$, let $f = (x - t_0)^2 + t_0 + m \in \mathbf{Q}[x]$, where $m = 0$. Let $G_n(f)$ be the Galois group over $\mathbf{Q}$ of the splitting field of the nth iterate f^n, and let $G(f) = \varprojlim G_n(f)$. Then $G(f)$ is a finite-index subgroup of $\mathbf{Z}_2 \rtimes \mathbf{Z}_2^*$ unless $t_0 \in \{-1, 0, 1\}$*

Proof: Note that $\mathbf{Z}_2 \rtimes \mathbf{Z}_2^* = \varprojlim \mathbf{Z}/2^n\mathbf{Z} \rtimes (\mathbf{Z}/2^n\mathbf{Z})^*$, and the order of $\mathbf{Z}/2^n\mathbf{Z} \rtimes (\mathbf{Z}/2^n\mathbf{Z})^*$ is 2^{2n-1}. Thus it suffices to show that $[\mathbf{Z}/2^n\mathbf{Z} \rtimes (\mathbf{Z}/2^n\mathbf{Z})^* : G_n(f)]$ is bounded as n goes to infinity.

Note that $f^n(x) = (x - t_0)^{2^n} + t_0$, and the splitting field K_n of f^n over $\mathbf{Q}$ must contain a primitive 2^nth root of unity ζ_{2^n} as long as $t \neq 0$. By Lemma 4.3, the degree $[K_n : \mathbf{Q}(\zeta_{2^n})]$ is $2^n/d$, where $1 \leq d \leq 2^n$ is maximal such that $t_0^{1/d} \in \mathbf{Q}(\zeta_{2^n})$. Thus $[K_n : \mathbf{Q}] = 2^{2n-1}/d$, implying that $[\mathbf{Z}/2^n\mathbf{Z} \rtimes (\mathbf{Z}/2^n\mathbf{Z})^* : G_n(f)] = d$. Now provided that $t_0 \neq \pm 1$, there is $e > 0$ and a prime p such that $v_p(t_0^{1/e})$ is odd. If $p \neq 2$ then p does not ramify in $\mathbf{Q}(\zeta_{2^n})$, and it follows that $t_0^{1/(e+1)}$ is not in $\mathbf{Q}(\zeta_{2^n})$. If $p = 2$, then one notes that $\sqrt[4]{2} \notin \mathbf{Q}(\zeta_{2^n})$ (otherwise $\mathbf{Q}(\sqrt[4]{2})$ would be a subfield of an abelian extension, and thus Galois, which is a contradiction). Therefore $t_0^{1/(e+2)} \notin \mathbf{Q}(\zeta_{2^n})$. In either case we have $d \leq e + 2$. Thus d is independent of n for n sufficiently large, which proves the Theorem. ■

We note that if $m = -2$, then matters are similar to the case $m = 0$, although more complicated and with more exceptional values, namely $t_0 \in \{-2, -1, 0, 1, 2\}$. In this case, the roots of f^n generate a subfield of degree at most two of the splitting field over $\mathbf{Q}$ of $x^{2^n} - \beta$, where β is a root of $x^2 - t_0 x + 1$ [6, p.8]. Let α be a root of $x^{2^n} - \beta$, and note that if $[\mathbf{Z}/2^n\mathbf{Z} \rtimes (\mathbf{Z}/2^n\mathbf{Z})^* : \mathrm{Gal}\,(\mathbf{Q}(\alpha, \zeta_{2^n}))/\mathbf{Q}(\beta)]$ is bounded as n goes to infinity, then it follows that $G(f)$ has finite index in $\mathbf{Z}_2 \rtimes \mathbf{Z}_2^*$. By Lemma 4.3 it is enough to show that $\sqrt[2^n]{\beta} \notin \mathbf{Q}(\beta)(\zeta_{2^\infty})$ for some $n > 0$, unless β is a root of unity, which occurs only when $|t_0| \leq 2$. It is possible, although quite laborious, to prove this using knowledge of the Galois group and subfields of $\mathbf{Q}(\beta)(\zeta_{2^\infty})/\mathbf{Q}(\beta)$. We omit the details.

We now discuss the case where $m \notin \{0, -1, -2\}$ (we touch on $m = -1$ below). Theorem 4.1 and the strong form of the Hilbert Irreducibility Theorem imply that if $m \notin \{0, -1, -2\}$ is fixed, then for all but a 'thin' set of $\gamma \in \frac{1}{2}\mathbf{Z}$ we have $G_n(f) \cong \mathrm{Aut}(T_n)$ for $f = (x - \gamma)^2 + \gamma + m$ (see [15, Section 6]). However, we would like to know something about $G(f)$ for such specializations. In order to emulate the proof of Theorem 4.1, one needs to know arithmetic properties of the critical orbit $\{f^n(\gamma) : n = 1, 2, \ldots\}$ of f, specifically the assertion that the squarefree part of $f^n(\gamma)$ is divisible by a prime that does not divide $f^m(\gamma)$ for all $m < n$. We conjecture that this condition holds for all but finitely many n.

Conjecture 4.5 (Strong Dynamical Wieferich Prime Conjecture)**.** *Let $b \in \frac{1}{2}\mathbf{Z}$ and $f \in \mathbf{Z}[x]$ be separable and quadratic such that $\{f^n(b) : n = 1, 2, \ldots\}$ is infinite. Then for all but finitely many n there exists a prime p with $v_p(f^n(b))$ odd and $v_p(f^m(b)) = 0$ for all $m < n$.*

We first remark that Conjecture 4.5 implies that $G(f)$ has finite index in $\mathrm{Aut}(T)$ for all critically infinite quadratic $f \in \mathbf{Z}[x]$ all of whose iterates are irreducible. This set of polynomials is quite a large subset of quadratic f (see [9, Theorem 3.5]). As for the name of Conjecture 4.5, recall that a Wieferich prime p is one satisfying $2^{p-1} \equiv 1 \bmod p^2$. This condition is equivalent to the following: let $a_n = 2^n - 1$, and let n_p be the smallest index such that $p \mid a_{n_p}$. Then $p^2 \mid a_{n_p}$. Currently only two Wieferich primes are known, although even the statement that their complement is infinite remains a conjecture (see e.g. [22]). Thus a reasonable analogue of this conjecture in the dynamical setting would be that given an unbounded sequence $\{f^n(b) : n = 1, 2, \ldots\}$, there exist infinitely many p such that $v_p(f^n(b)) = 1$ for some n but $v_p(f^m(b)) = 0$ for all $m < n$. Conjectu re 4.5 represents a significant strengthening of this, albeit with only the stipulation that $v_p(f^n(b))$ be odd.

Conjecture 4.5 can be proven in the case where the forward orbit of 0 $\{f^n(0) : n = 1, 2, \ldots\}$ is finite but does not contain 0 [9, p. 19]. Thus for instance the conjecture is true if f is of the form $x^2 + kx - k$ or $x^2 - kx - 1$ for some $k \in \mathbf{Z}$.

As for $m = -1$, matters are more mysterious, which perhaps is unsurprising given that the behavior in the generic case $f = (x - t)^2 + t - 1 \in \mathbf{Q}(t)[x]$ is not known (see discussion on p. 219). We conjecture that for all but finitely many specializations $t_0 \in \mathbf{Z}$, $G(f)$ has finite index in the group obtained in the generic case. However, $G(f)$ has been not been explicitly computed for any specializations t_0. The case $t_0 = -1$, which gives $f = (x+1)^2 - 2$, is particularly interesting because the splitting fields of the iterates f^n are 2-extensions ramified only at 2 (and ∞). The suggestion has been made by several people that the maximal such 2-extension should be the union of these splitting fields. This is conceivable since the Galois groups of the first few were computed (by Klüners and Fieker) and were large. Their orders (for $n \leq 7$) were $2^{(2^{n+1}+1)/3}$ if n is even and $2^{(2^{n+1}+2)/3}$ if n is odd. If true for general n, this would imply that $G(f)$ has Hausdorff dimension 2/3.

Further investigation leads to the following conjecture. With the standard generators a, b of the closure B of the Basilica group [1], let H be the subgroup generated by $[a, b]$ and aba, a normal subgroup with B/H infinite, cyclic. Let H_n be the image of H in $\mathrm{Aut}(T_n)$.

Conjecture 4.6. *Let $f = (x+1)^2 - 2$. The Galois group of f^n over $\mathbf{Q}(i)$ (a subgroup of index 2 in $G_n(f)$) is H_n for all n.*

This implies that the union of the splitting fields of all the f^n has Galois group over $\mathbf{Q}(i)$ equal to the closure of H in $\mathrm{Aut}(T)$. Using the explicit presentation of B in [1], we compute that this closure is not a free pro-2 group (its class 5 quotient is smaller than that of the 2-generated free pro-2 group). On the other hand, Markšaĭtis [11] showed that the Galois group over $\mathbf{Q}(i)$ of the maximal 2-extension unramified outside the prime above 2 is a free pro-2 group. Thus one consequence of Conjecture 4.6 is that $G(f)$ is properly contained in the Galois group of the maximal 2-extension of $\mathbf{Q}$ unramified outside $\{2, \infty\}$ - in other words, this maximal 2-extension is not generated by the roots of the iterates of f.

5. Conjectures

We gather the main conjectures made through this paper. They all pertain to the case where $f \in \mathbf{Z}[x]$ is quadratic. First we conjecture that every irreducible quadratic f is settled. This implies that the images of Frobenius elements under the corresponding arboreal Galois representation ρ_f are settled. Since Frobenius elements are dense in the image, we further conjecture that the image $G(f)$ of ρ_f is a densely settled subgroup.

A subgroup commensurable to a densely settled subgroup is densely settled. There are many commensurability classes of densely settled subgroups but we conjecture that few of these arise as possible $G(f)$ in the case where $f \in \mathbf{Z}[x]$ is quadratic. In fact the only classes appear to be that of $\mathrm{Aut}(T)$ (in the case where f is critically infinite), that of the closure of the Basilica group acting on T and a few subgroups of this group, that of the affine group on $\mathbf{Z}_2$, that of $\mathbf{Z}_2$, and that of the spherically homogeneous procyclic subgroup. Conjectures 4.5 and 4.6 go in the direction of establishing this classification. It is worth remarking that if we allow $f \in \mathcal{O}_K[x]$, where K is an algebraic number field, then the classification

should expand due to the presence of additional conjugacy classes of critically finite quadratic polynomials.

References

[1] Laurent Bartholdi and Rostislav I. Grigorchuk. On a group associated to $z^2 - 1$. Available at http://arxiv.org/pdf/math.GR/0203244, 2002.

[2] Nigel Boston. Galois groups of tamely ramified p-extensions. *Journal de Théorie des Nombres de Bordeaux*, 19:59-70, 2007.

[3] Wên Chên Chi. l-adic and λ-adic representations associated to abelian varieties defined over number fields. *Amer. J. Math.*, 114(2):315–353, 1992.

[4] Pierre Deligne. Hodge cycles on abelian varieties. In *Hodge cycles, motives, and Shimura varieties*, volume 900 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1982.

[5] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 41–78. Internat. Press, Cambridge, MA, 1995.

[6] Richard Gottesman and Kwokfung Tang. On the Galois groups of iterates of conjugates of $x^2 - 2$. Preprint.

[7] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[8] Rafe Jones. Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set. *Compos. Math.*, 43 (5):1108-1126, 2007.

[9] Rafe Jones. On the density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc.*, to appear.

[10] Rafe Jones and Nigel Boston. Settled polynomials over finite fields. Preprint, 2008.

[11] G. N. Markšaĭtis. On p-extensions with one critical number. *Izv. Akad. Nauk SSSR Ser. Mat.*, 27:463–466, 1963.

[12] J. S. Milne *Etale cohomology* Princeton Mathematical Series 33, Princeton University Press, Princeton, NJ, 1980.

[13] Władysław Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[14] Volodymyr Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.

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

[16] Richard Pink. The Mumford-Tate conjecture for Drinfeld-modules. *Publ. Res. Inst. Math. Sci.*, 33(3):393–425, 1997.

[17] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[18] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inv. Math.*, 15:259–331, 1972.

[19] Jean-Pierre Serre. Letter to J. Tate, Jan 2, 1985.

[20] Jean-Pierre Serre. Algèbre et géométrie. *Ann. Collège France*, 85:85–90, 1984/85.

[21] Jean-Pierre Serre. Algèbre et géométrie. *Ann. Collège France*, 86:95–100, 1985/86.

[22] Joseph H. Silverman. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory*, 30(2):226–237, 1988.

[23] G. Willis. Totally disconnected, nilpotent, locally compact groups. *Bull. Austral. Math. Soc.*, 55(1):143–146, 1997.

Nigel Boston and Rafe Jones
Department of Mathematics
University of Wisconsin
Madison, WI 53706, USA.
E-mail: boston@math.wisc.edu
E-mail: jones@math.wisc.edu