Arboreal Galois Representations

Nigel Boston (boston@math.wisc.edu) and Rafe Jones
(jones@math.wisc.edu)
University of Wisconsin-Madison

Abstract.
Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$, and let T be the complete rooted d-ary tree, where $d \geq 2$. In this article we study "arboreal" representations of $G_{\mathbb{Q}}$ into the automorphism group of T, particularly in the case $d = 2$. In doing so, we propose a parallel to the well-developed and powerful theory of linear p-adic representations of $G_{\mathbb{Q}}$. We first give some methods of constructing arboreal representations and discuss a few results of other authors concerning their size in certain special cases. We then discuss the analogy between arboreal and linear representations of $G_{\mathbb{Q}}$. Finally, we present some new examples and conjectures, particularly relating to the question of which subgroups of $\mathrm{Aut}(T)$ can occur as the image of an arboreal representation of $G_{\mathbb{Q}}$.

Keywords: Galois representation, rooted tree, tree automorphisms, pro-p group, iterates, monodromy group

MR classification: 11F80, 11R32, 20E08, 20E18

1. Arboreal Representations

To define an arboreal representation, we need two preliminary notions. For an integer $d \geq 2$, the *complete rooted d-ary tree* is the rooted tree with d^n vertices at level n (i.e. distance n from the root), each connected to d vertices at level $n+1$. An automorphism of a tree T with vertex set V, is a bijection $\sigma : V \to V$ such that $v \in V$ is connected to $v' \in V$ if and only if $\sigma(v)$ is connected to $\sigma(v')$.

DEFINITION 1.1. *An* arboreal representation *of a profinite group G is a continuous homomorphism $G \to \mathrm{Aut}(T)$, where T is the complete rooted d-ary tree for some d.*

Denote by T_n the set of vertices of the complete rooted d-ary tree T of distance at most n from the root. This is also the truncation of T to the first n levels. It is well-known (Nekrashevych, 2005, Proposition 1.4.2) that $\mathrm{Aut}(T_n)$ is isomorphic to the n-fold iterated wreath product of the symmetric group S_d, which we denote by W_n (the value of d will always be clear from context; usually it will be 2). Moreover, we have that $\mathrm{Aut}(T) \cong \varprojlim \mathrm{Aut}(T_n) \cong \varprojlim W_n$, via the natural restriction maps $\mathrm{Aut}(T_n) \to \mathrm{Aut}(T_{n-1})$.

In this article our main interest is in arboreal representations coming from iterated polynomials defined over $\mathbb{Z}$. Let $f \in \mathbb{Z}[x]$ be a polynomial of degree d, and let $f^1 = f$ and $f^n = f \circ f^{n-1}$, so that f^n is the nth iterate of f. Suppose that all the iterates f^n are separable. The successive f-preimages of 0 (contained in $\overline{\mathbb{Q}}$) now form a complete rooted d-ary tree. Indeed, for each root α of f^n there is a unique root β of f^{n-1} related to α in the sense that $f(\alpha) = \beta$. Assigning edges according to this relation, the disjoint union $\bigcup_{n=0}^{\infty}\{\text{roots of } f^n\}$ becomes a complete d-ary tree with root 0.

Let $K_n(f)$ be the splitting field of f_n over $\mathbb{Q}$, and let $G_n(f)$ be the corresponding Galois group. Consider $G(f) := \varprojlim G_n(f)$, which is the Galois group over $\mathbb{Q}$ of the union of the splitting fields of all iterates of f. Elements of $G(f)$ are determined completely by their action on the roots of the f^n, and it follows that $G(f)$ acts faithfully on the tree formed by these roots. Thus $G(f)$ gives an arboreal representation of $G_{\mathbb{Q}}$.

One can generalize this construction to the setting of iterated polynomial covers of $\mathbb{P}^1_K$, as first done in (Aitken et al., 2005). Let K be a field and t a parameter for $\mathbb{P}^1_K$. As above, the f-preimages of t form a complete d-ary rooted tree, and the Galois group corresponding to the infinite tower of iterations of f acts on this tree. In terms of function fields, the polynomials $F_n(x,t) = f^n(x) - t \in K(t)[x]$ generate extensions $K_n(f,t)$ over $K(t)$, and the Galois group $G(f,t)$ of the compositum of these extensions has a faithful action on the tree of roots of the F_n (equivalently the tree of f-preimages of t). Moreover, for any specialization $t_0 \in K$ of t, the corresponding Galois group $G(f,t_0)$ gives an arboreal representation of the absolute Galois group G_K. For details, see (Aitken et al., 2005, p.856). The case discussed in the previous paragraph corresponds to $t_0 = 0$.

An important attribute of a polynomial is the orbits of its critical points.

DEFINITION 1.2. *Let K be a field, let $f \in K[x]$ have degree d, and let $\gamma_1, \ldots, \gamma_{d-1}$ be the critical points of f. The* post-critical set *of f is $\{f^i(\gamma_j) : i \geq 1, 1 \leq j \leq d-1\}$. If this set is finite, we call f* critically finite*, while otherwise we call f* critically infinite.

Only primes of $K(t)$ that divide an element of the post-critical set of f can ramify in the compositum L of the fields $K_n(f,t)$. A similar statement holds for specializations of t, although one must add primes dividing the degree of f. Therefore $L/K(t)$ is finitely ramified if f is critically finite, and the same statement holds for specializations of t (Aitken et al., 2005, Theorem 1.1). It follows that $G(f,t)$ is finitely generated. In section 5 we discuss several instances where $f \in \mathbb{Z}[x]$ has degree 2 and is critically finite. The resulting finitely generated arboreal representations furnish an interesting class of examples.

2. Previous Work

Arboreal representations obtained by the method given in section 1 have been studied by a few authors. Let T denote the tree of f-preimages of t or some specialization t_0, depending on the context. When f is critically infinite, most of the investigations have considered the case $t_0 = 0$ and have shown that the associated arboreal representations are large. Odoni (Odoni, 1985, Theorem 1) considered the following situation: let k have characteristic 0, f be the generic monic polynomial of degree d defined over $K = k(x_1, \ldots, x_d)$, and $t_0 = 0$. He showed that $G(f) \cong \mathrm{Aut}(T)$. Odoni also considered the case $K = \mathbb{Q}$, $t_0 = 0$, and $f = x^2 + a$, where $a \in \mathbb{Z}$, and further work by Stoll (Stoll, 1992) showed that $G(f) \cong \mathrm{Aut}(T)$ for $a > 0$, $a \equiv 1, 2 \pmod 4$ and for $a < 0, a \equiv 0 \pmod 4$. For $K = \mathbb{Q}$, $t_0 = 0$ and f of the form $x^2 - ax + a$, the second author (Jones, 2006, p. 21) has shown that $G(f)$ has finite index in $\mathrm{Aut}(T)$ for all $a \notin \{-2, 2, 4\}$. It is reasonable to speculate that whenever a quadratic $f \in \mathbb{Z}[x]$ is critically infinite, $G(f)$ will not be finitely generated, and indeed will have finite index in $\mathrm{Aut}(T)$. Presently neither of these assertions is known (c.f. (Jones, 2006, Conjecture 4.7)).

Another line of inquiry has looked at the case where there is no specialization and has tended to focus on critically finite f. When $K = \mathbb{C}$ the group $G(f, t)$ is the *iterated monodromy group* of f (see (Nekrashevych, 2005, Chapter 5)). In the case where f is critically finite, the iterated monodromy group is a finitely generated, self-similar subgroup of $\mathrm{Aut}(T)$ that is the closure of a group generated by a finite automaton.

Another interesting example along these lines is due to R. Pink (personal communication). Let K be a finite field of odd order, and f a quadratic polynomial. Since the critical orbit of f belongs to a finite extension of K, f must be critically finite, and it follows that $G(f, t)$ is a finitely generated subgroup of $\mathrm{Aut}(T)$. Little appears to be known about the subgroups obtained in this manner. For $K = \mathbb{F}_5$ and $f = x^2 - 1$, Pink explicitly computed the geometric part Δ of $G(f, t)$ (meaning we take $\overline{\mathbb{F}_5}$ to be our ground field) and found it has Hausdorff dimension $2/3$. In this case, $G(f, t)/\Delta$ is an infinite, procyclic group.

3. Analogy with p-adic Galois Representations

If O is the valuation ring of some finite extension of $\mathbb{Q}_p$ and K is any field, then there are many natural sources of p-adic Galois representations $\rho : G_K \to GL_n(O)$, most notably from algebraic geometry, namely the Galois action on subquotients of étale cohomology groups of varieties defined over K. This is, for instance, how the representations associated to cuspidal eigenforms are produced. This theory has been very fruitful since its inception by Shimura (Shimura, 1966) and others about 40 years ago, and in particular there are three topics that have dominated the development of the subject.

First, the size of the image has been of interest ever since Serre (Serre, 1972) proved that elliptic curves over $\mathbb{Q}$ with no complex multiplication lead to representations with image of finite index (typically 1) in $GL_2(\mathbb{Z}_p)$. Equivalently, their Lie algebra is gl_2. For more general abelian varieties, this Lie algebra is conjecturally characterized by the Mumford-Tate group of the variety.

Second, the images of Frobenius elements under ρ, or at least their characteristic polynomials, can be described in geometric terms, yielding some sort of nonabelian reciprocity law. For instance, for a cuspidal eigenform f of weight k and Nebentypus ϵ, the characteristic polynomial of the image of a Frobenius element at q under the p-adic representation is $T^2 - a_q T + \epsilon(q) q^{k-1}$, where a_q is the qth coefficient of f. Taking the product of the reciprocals of these characteristic polynomials for varying q with $T = q^{-s}$ and a modified version for primes q dividing the level of f produces the L-series $L(s, \rho)$, which turns out to be independent of both ρ and p and so is denoted $L(s, f)$.

Finally and most recently, the problem of characterizing representations arising from standard constructions has come to the fore. For instance, elliptic curves and cuspidal eigenforms produce odd representations $G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}_p})$, where *odd* means that the determinant of complex conjugation is -1. Serre's conjecture (Serre, 1987) proposes that all such odd representations, if absolutely irreducible, should arise from some cuspidal eigenform. Most cases of this conjecture have recently been established. Moreover, the Fontaine-Mazur conjecture (Fontaine and Mazur, 1995), which suggests that the representations from algebraic geometry should be exactly those that are finitely ramified and potentially semistable at p, has been successively chipped away, most notably by Wiles (Wiles, 1995) (completed by Breuil-Conrad-Diamond-Taylor (Breuil et al., 2001)), who established enough of it to prove the famous Taniyama-Shimura conjecture that all elliptic curves over $\mathbb{Q}$ are modular.

In order to carry these three topics over to arboreal Galois representations, we introduce the notion of *settledness*

DEFINITION 3.1. *Given a quadratic polynomial $f \in \mathbb{F}_q[x]$, a polynomial $h \in \mathbb{F}_q[x]$ is called* f-stable *if for every $n \geq 0$ $h \circ f^n$ is irreducible. For a given n let $g_1, ..., g_r$ denote the f-stable factors of f^n and s_n the sum of their degrees. The polynomial $f \in \mathbb{F}_q[x]$ is called* settled *if the limit of $s_n/2^n$ as $n \to \infty$ is 1.*

In (Boston and Jones, 2006) it is shown that if $h(a)$ is not a square for every a in the critical orbit of f, then h is f-stable. We conjecture there that every irreducible quadratic $f \in \mathbb{F}_q[x]$ is settled and give computational evidence in support.

The notion of settledness is related to arboreal Galois representations because of a result of van der Waerden, stating that if $g \in \mathbb{Z}[x]$, then (for all but finitely many primes q) the degrees appearing in its factorization mod q coincide with the cycle structure of the Frobenius element at q in the Galois group of g over $\mathbb{Q}$.

DEFINITION 3.2. *Suppose an element $\sigma \in \mathrm{Aut}(T)$ has image $\sigma_n \in \mathrm{Aut}(T_n)$. A cycle of σ_n of length 2^k is called* stable *if it is mapped to by a cycle of σ_r of length 2^{k+r-n} for all $r > n$. Let the sum of the lengths of the stable cycles of σ_n be s_n. Then σ is called* settled *if the limit of $s_n/2^n$ as $n \to \infty$ is 1.*

For example, an element of $\mathrm{Aut}(T)$ that acts as a single cycle on every level is settled. Such an element is called an *adding machine*. Settled elements consist of a proliferation of adding machines on subtrees of T.

The main conjecture of (Boston and Jones, 2006) above implies that if f is an irreducible quadratic polynomial in $\mathbb{Z}[x]$, then the Frobenius elements in $G(f)$ are settled. Since by Tchebotarev's density theorem the Frobenius elements are dense, it follows that the settled elements in $G(f)$ are dense in $G(f)$. Such a subgroup of $\mathrm{Aut}(T)$ will be called *densely settled*. The above notions now allow us to address the three important issues regarding p-adic Galois representations but in the case of arboreal Galois representations.

First, it is easy to see that settled elements are rare (of density zero) in $\mathrm{Aut}(T)$. There certainly exist subgroups of $\mathrm{Aut}(T)$ that fail to be densely settled, for example because they have too much torsion (torsion elements are never settled). A group is densely settled if and only if it has a densely settled subgroup of finite index, and so we need consider densely settled groups only up to commensurability. The next section considers some examples. In general, we ask for a classification of them up to commensurability (in analogy to how p-adic Lie groups are classified up to commensurability by their Lie algebra). For example, which groups defined by automata are densely settled?

Second, assuming the settledness conjecture, we can associate to a Frobenius element at q a certain (possibly infinite) partition of 1. Namely, if $\sigma \in \mathrm{Aut}(T)$ is its image and the stable parts of σ_n have degrees $d_1, ..., d_r$, then $d_1/2^n + d_2/2^n + ... + d_r/2^n$ is the initial segment of what as $n \to \infty$ becomes a partition of 1. This might be thought of as analogous to a local zeta function. The question arises as to whether this partition has a finitely expressible generating function. In (Boston and Jones, 2006), it is conjectured that a Markov process approximates the factorization of the iterates $f^n \pmod q$ and the rate at which this process converges might alternatively be associated to q. The question then arises as to how to convert these numbers into useful analogues of L-series.

Finally, the question of which arboreal Galois representations arise from our construction is one for the future. Some consequences of the Fontaine-Mazur conjecture are given in the next section.

4. Another Source of Arboreal Representations

The unramified Fontaine-Mazur conjecture (Fontaine and Mazur, 1995) says that for a number field K any finitely ramified representation $\rho : G_K \to GL_n(\mathbb{Z}_p)$ that is unramified at p should have finite image. There do, however, exist infinite, finitely and tamely ramified p-extensions of number fields. The above conjecture implies that their Galois groups G can have no infinite p-adic analytic quotients.

In fact little is known about these Galois groups. In particular, not one such G has been explicitly presented. The recent breakthrough of Labute (Labute, 2006) shows that some are mild pro-p groups and hence have cohomological dimension 2. In (Boston, 2006) an analogy of the virtual positive Betti number conjecture for 3-manifolds is given, stating that all such G should be virtually Golod-Shafarevich, meaning that G has a subgroup H of finite index such that $r(H) \leq d(H)^2/4$ (and $H \ncong \mathbb{Z}_p$). This conjecture implies the unramified Fontaine-Mazur conjecture.

Every finitely generated infinite pro-p group has just-infinite quotients and the above conjecture has strong implications for those of G. In particular, the Grigorchuk-Wilson dichotomy says that just-infinite pro-p groups are either branch or have an open subgroup that is a direct product of finitely many copies of the same hereditarily just-infinite pro-p group. Since Golod-Shafarevich groups are never just-infinite, the conjecture of (Boston, 2006) implies that the just-infinite quotients of G cannot be of the second kind. They must therefore be branch. These branch just-infinite quotients of G naturally embed in the automorphism group of a locally finite, rooted tree, so producing arboreal representations of G.

So far no critically finite polynomial whose iterates produce a tamely ramified representation is known and so the class of arboreal representations of this section is as yet disjoint from the class considered in the rest of the paper. Further discussion of this can be found in (Aitken et al., 2005).

5. Examples

I. The examples of arboreal representations coming from iterated polynomials defined over $\mathbb{Z}$ that were considered in section 2 have densely settled images. Indeed, their images are of finite index in $\mathrm{Aut}(T)$ and it follows that they are densely settled. However, the question of whether Frobenius elements are settled is harder. Consider, for example, $f = x^2+1$, whose critical orbit over $\mathbb{Z}$ is infinite. Modulo 3 all its iterates are irreducible, so f is f-stable, meaning that the corresponding partition is just $1/1$.

Considering f modulo 7, extensive computations in (Boston and Jones, 2006) give evidence for the settledness of Frobenius elements and indeed the conjecture of an underlying Markov process (here with convergence rate 0.901). Here we just give the associated partition, which turns out to be $1/4+1/8+3/16+2/32+8/64+10/128+8/256+12/512+22/1024+45/2048+45/4096+85/8192+179/16384+...$

II. At the other extreme is the example $f = x^2 - 2$. Here the critical orbit is $\{-2, 2\}$ and the splitting field of f^n is $\mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive 2^nth root of 1, which has Galois group cyclic of order 2^n acting regularly on the 2^n vertices of T at level n. In the limit, as $n \to \infty$, we obtain $\mathbb{Z}_2$, the "adding machine", which is easily seen to be densely settled. In fact, all nontrivial elements are settled, implying that all Frobenius elements are also settled.

III. A somewhat more complicated example is afforded by $f = (x-p)^2+p$ for any odd prime p. Here the critical orbit is just $\{p\}$ and the Galois group $G(f)$ is isomorphic to the group of affine linear transformations of $\mathbb{Z}_2$, namely $A(\mathbb{Z}_2) = \{ax + b, a \in \mathbb{Z}_2^*, b \in \mathbb{Z}_2\}$. This group is metabelian and also the normalizer in $\mathrm{Aut}(T)$ of the group in example II.

The group $A(\mathbb{Z}_2)$ is densely settled and also all Frobenius elements are settled. As this group is richer than the adding machine in example II, we give some details on cycle structures of general elements and Frobenius elements. Given $g = ax + b \in A(\mathbb{Z}_2)$, denote by g_n the action of g on $\mathrm{Aut}(T_n)$. There are two fundamental kinds of behavior:

1. If $v_2(a-1) > v_2(b)$, then for each n all cycles of g_n are of equal length. If g is not the identity and $a \neq -1$, then for all sufficiently large n the order of g_{n+1} is twice that of g_n. It follows that g is settled.

2. If $v_2(a-1) \leq v_2(b)$, then g_n has at least two fixed points for all n. If g is not the identity and $a \neq -1$, then for all sufficiently large n there are nonzero constants c_1, c_2, c_3, and m such that g_n consists of c_1 fixed points, c_2 2-cycles, c_3 4-cycles, c_3 8-cycles, $\ldots, c_3$ 2^{n-m}-cycles. Moreover, g_{n+1} has the same cycle structure, but with an additional c_3 2^{n-m+1}-cycles. It follows that g is settled.

One sees from this that nearly all elements of $A(\mathbb{Z}_2)$ are settled. Indeed, the only unsettled elements are the torsion elements, namely the identity and those g of the form $-x+b$. It follows immediately that the affine group is densely settled.

Now let q be an odd prime not equal to p, and consider a Frobenius element Frob_q at q. Note that for $g = ax + b \in A(\mathbb{Z}_2)$, the image of g in the abelianization of $A(\mathbb{Z}_2)$ is simply a. Each $h \in G(f)$ acts on the primitive 2^nth roots of unity by raising to the r_n power, and the image of h in the abelianization of $G(f)$ is given by $\varprojlim r_n$. Since Frob_q raises elements to the q power, we have that the cycle structure of Frob_q is the same as that of $g = qx + b \in A(\mathbb{Z}_2)$ for some $b \in \mathbb{Z}_2$. It follows immediately that Frob_q is not torsion, and thus is settled.

We can say even more. Put $s = v_2(q-1)$. If f^{s+1} has no roots in $\mathbb{F}_q$ then the cycle structure of Frob_q is described by case (1) above, and thus the associated partition of unity is finite. If f^{s+1} has a root in $\mathbb{F}_q$ then the cycle structure of Frob_q is described by case (2), and the corresponding partition of unity is infinite. Let us do some explicit calculations in the case $p = 3$. First suppose that $q \equiv 3 \pmod 4$, which implies that $s = 1$. If $q \equiv 7 \pmod{12}$ then $\sqrt{-3} \in \mathbb{F}_q$ and since $\sqrt{-1} \in \mathbb{F}_q$ it follows that one of $\pm\sqrt{-3}$ is a square in $\mathbb{F}_q$. Hence $f^2 = (x-3)^4 + 3$ has a root in $\mathbb{F}_q$ so that Frob_q has an infinite partition. For example if $q = 19$ the associated partition is $2/4+2/8+2/16+2/32+\ldots.$ If $q \equiv 11 \pmod{12}$ then f already has no roots in $\mathbb{F}_q$, so f^2 cannot either, implying the associated partition is finite. For example if $q = 23$ then the partition associated to q is $4/4$.

Now suppose that $q \equiv 1 \pmod 4$, so that $s > 1$. If $q \equiv 5 \pmod{12}$ then $\sqrt{-3} \notin \mathbb{F}_q$ and thus already f has no roots in $\mathbb{F}_q$. It follows that we are in case (1) and the partition is finite. Indeed, in this case all iterates of f mod q must be irreducible, so the associated partition is 1/1. If $q \equiv 1 \pmod{12}$ then f^{s+1} may either have roots or not have roots. For instance, if $q = 13$ then f^3 has no roots, and the associated partition is 2/2. For $q = 61$, f^3 has a root in $\mathbb{F}_q$, and the partition associated to q is $2/4 + 2/8 + 2/16 + 2/32 + ...$

The partitions produced are finite or are geometric series and so have finite descriptors. One difference with the theory of p-adic representations is the fact that it can happen that the Frobenius elements for different primes can map to the same conjugacy class in $\mathrm{Aut}(T)$. For instance, this is the case for the examples of $q = 19$ and $q = 61$ above.

IV. An interesting intermediate example is given by $f = (x+1)^2 - 2$, which has critical orbit $\{-2, -1\}$. We calculate the absolute value of the discriminant of f^n to be $\Delta_n = \Delta_{n-1}^2 2^{k_n}$ where $k_n = 2^n$ if n is even and $2^n + 1$ if n is odd. Since Δ_n is a power of 2, the splitting field extension $K_n/\mathbb{Q}$ is unramified outside 2 and ∞. Thus $G_n := \mathrm{Gal}\,(K_n/\mathbb{Q})$ is a quotient of the Galois group M of the maximal 2-extension of $\mathbb{Q}$ unramified outside 2 and ∞. The structure of M has been known since 1963, when it was proved (Markšaĭtis, 1963) that M is the free product of C_2 and $\mathbb{Z}_2$, i.e. has pro-2 presentation $< \sigma, \tau | \sigma^2 >$, where σ can be taken to be complex conjugation. We would like to determine if the surjection $M \to G(f)$ is an isomorphism. If so, the fact that the roots of the iterates of f generate the maximal pro-2 extension of $\mathbb{Q}$ unramified outside $\{2, \infty\}$ could be viewed as a kind of Jugendtraum.

By Burnside's basis theorem, M is generated by any two elements whose images generate $M/\Phi(M)$, which is the maximal elementary abelian quotient of M. We have $M/\Phi(M) \cong C_2 \times C_2$, which corresponds to the extension $\mathbb{Q}(\sqrt{-1}, \sqrt{2})$. In particular, any Frobenius element Frob_q for $q \equiv 3$ or $5 \pmod 8$ together with σ generates $G(f)$.

The image of complex conjugation σ in G_n can be taken to be

$$(3,4)(5,7)(6,8)(9,13)(10,14)(11,15)(12,16)(17,25)(18,26)...$$

i.e. if $2^k < i \leq 2^{k+1}$, then $|i - \sigma(i)| = 2^{k-1}$.

MAGMA allows us to calculate G_n immediately for $n = 1, 2, 3, 4$. For $n = 1$ and $n = 2$, it is the whole of W_n. For $n = 3$, W_n has 3 generators and so cannot equal G_n. In fact, the Galois group G_3 has index 2 (so order 64). The 4th iterate f^4 has Galois group G_4 of order 2^{11}.

Using van der Waerden's criterion, we calculate the sequence of cycle structures of Frob_q in successive W_n. For example, for $q = 3$, we obtain $[2], [4], [4, 4], [8, 4, 4], [16, 8, 4, 4], [32, 8, 8, 4, 4, 4, 4], \ldots$ The strategy to determine G_n is to obtain a list $A(n)$ of permissible cycle structure sequences. For $n = 5, 6$ this is enough to compute G_n exactly. In particular, it turns out that G_5 has order 2^{22} and G_6 apparently has order 2^{43}. This is confirmed by calculations of Jürgen Klüners, using his new system that computes Galois groups of any degree.

A closer analysis shows that G_5 is generated by the image of σ given above, together with the element

$$(1, 19, 8, 22, 3, 17, 5, 24, 2, 20, 7, 21, 4, 18, 6, 23)$$
$$(9, 32, 11, 30, 10, 31, 12, 29)(13, 28, 14, 27)(15, 26)(16, 25)$$

For $n = 6$, it is seen that G_6 is generated by the image of σ given above, together with the element

$$(1, 37, 2, 38)(3, 39)(4, 40)(5, 34, 8, 35, 6, 33, 7, 36)$$
$$(9, 45, 15, 44, 12, 48, 14, 42, 10, 46, 16, 43, 11, 47, 13, 41)$$
$$(17, 61, 25, 51, 23, 57, 31, 55, 19, 64, 27, 49, 22, 59, 29, 53, 18, 62,$$
$$26, 52, 24, 58, 32, 56, 20, 63, 28, 50, 21, 60, 30, 54)$$

There are some striking patterns regarding the sequence of G_n found so far – for instance, the nilpotency class of G_n appears to be exactly 2^{n-1}. We conjecture that the group G_n has order $2^{(2^{n+1}+1)/3}$ if n is even and $2^{(2^{n+1}+2)/3}$ if n is odd. If so, then $G(f)$ has Hausdorff dimension $2/3$. It should be possible then to guess their inverse limit in $\mathrm{Aut}(T)$ and see whether this is isomorphic to M.

This compares interestingly with the famous Basilica group, which also has Hausdorff dimension $2/3$. The Basilica group is the iterated monodromy group (see section 1) of $x^2 - 1$, which is a conjugate of $(x + 1)^2 - 2$.

Acknowledgements

The authors would like to thank Richard Pink and Jürgen Klüners for helpful discussions.

References

Aitken, W., F. Hajir, and C. Maire: 2005, 'Finitely ramified iterated extensions'. *Int. Math. Res. Not.* (14), 855–880.

Boston, N.: 2006, 'Galois groups of tamely ramified p-extensions'. *Proceedings of Journées Arithmetiques 2005, special issue of Journal de Théorie des Nombres de Bordeaux.* To appear.

Boston, N. and R. Jones: 2006, 'Densely settled groups and arboreal Galois representations'. preprint.

Breuil, C., B. Conrad, F. Diamond, and R. Taylor: 2001, 'On the modularity of elliptic curves over **Q**: wild 3-adic exercises'. *J. Amer. Math. Soc.* **14**(4), 843–939 (electronic).

Fontaine, J.-M. and B. Mazur: 1995, 'Geometric Galois representations'. In: *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I. Cambridge, MA: Internat. Press, pp. 41–78.

Jones, R.: 2006, 'On the density of prime divisors of quadratic recurrences'. preprint.

Labute, J.: 2006, 'Mild pro p-groups and Galois groups of p-extensions of Q'. *J. Reine Angew. Math.* To appear.

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

Nekrashevych, V.: 2005, *Self-similar groups*, Vol. 117 of *Mathematical Surveys and Monographs.* Providence, RI: American Mathematical Society.

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

Serre, J.-P.: 1972, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques'. *Invent. Math.* **15**(4), 259–331.

Serre, J.-P.: 1987, 'Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)'. *Duke Math. J.* **54**(1), 179–230.

Shimura, G.: 1966, 'A reciprocity law in non-solvable extensions'. *J. Reine Angew. Math.* **221**, 209–220.

Stoll, M.: 1992, 'Galois groups over **Q** of some iterated polynomials'. *Arch. Math. (Basel)* **59**(3), 239–244.

Wiles, A.: 1995, 'Modular elliptic curves and Fermat's last theorem'. *Ann. of Math. (2)* **141**(3), 443–551.