GALOIS $p$-GROUPS UNRAMIFIED AT $p$ - A SURVEY

NIGEL BOSTON

Abstract. We survey the theory of Galois groups of $p$-extensions of number fields. These are well understood when $p$ is ramified, and related to the much applied theory of $p$-adic Galois representations. When $p$ is unramified, the situation is completely different with very little known about the structure of the Galois groups. We can, however, present glimpses of a rich theory, culminating in the study of Galois actions on locally finite, rooted trees. Analogies with link groups are mentioned.

1. Introduction.

Throughout $p$ is fixed to be a rational prime, $K$ a number field, i.e. a finite extension of $\mathbb{Q}$, and $S$ a finite set of primes of its ring of integers $O_K$. We shall investigate Galois extensions $L$ of $K$ that are ramified only at primes in $S$ (allowing ramification at any infinite primes - equivalently, the discriminant of $L/K$ is divisible only by primes in $S$) and whose degree is a power of $p$. Such an extension or a union of them will be called a $p$-extension. The union of all $p$-extensions of $K$ unramified outside $S$ will be denoted $K_S$ and its Galois group over $K$ by $G_S$. Alternatively this is the maximal pro-$p$ quotient of the étale fundamental group of $\text{Spec}(O_K) - S$. The big question then is to identify $G_S$, given $p$, $K$, and $S$. One case of particular interest is that where $S = \emptyset$, when $K_S$ is called the Hilbert $p$-class field of $K$.

If $S$ contains the primes $S_p$ above $p$, then much is known about $G_S$ and in many cases it can be explicitly presented [27]. On the other hand, assume for the rest of this introduction that $S \cap S_p = \emptyset$ (we say that $L/K$ is unramified at $p$). Then we know only a few things about $G_S$. Class field theory tells us that all its subgroups of finite index have finite abelianization (a property we denote FIFA). It is a finitely presented pro-$p$ group [37]. For certain $K$ and $S$, we can actually compute what $G_S$ is or at least a short list of candidates for $G_S$ [9, 11, 17], although in all these cases $G_S$ is finite. For many years [22], it has been known that there exist number fields $K$ for which $G_\emptyset$ is infinite and the theorem of Golod-Shafarevich can be used to show that many other $G_S$ are infinite. Not one example, however, is known of an explicit presentation for an infinite $G_S$. We obtain conjectural presentations in some simple cases.

On the other hand, there are fundamental conjectures that concern infinite $G_S$. In particular, the Fontaine-Mazur conjecture [19] says that $G_S$ should have no

1991 Mathematics Subject Classification. 11R32, 11Y40, 12F10, 20D15.

Key words and phrases. Explicit Galois group, class tower, just-infinite, branch, Fontaine-Mazur.

The author was supported by NSF DMS.
infinite $p$-adic analytic quotients, meaning quotients that embed in $GL_n(\mathbb{Z}_p)$ for some $n$. This is equivalent [7] to claiming that the just-infinite quotients of $G_S$ are not $p$-adic analytic. Classification of all just-infinite pro-$p$ groups is a major activity of group theorists today [16] and has yielded various families and in particular Grigorchuk’s dichotomy [23]. My extension [7] of the Fontaine-Mazur conjecture proposes that the just-infinite quotients of $G_S$ always lie on one side of this dichotomy, namely are branch. Branch pro-$p$ groups are certain groups of automorphisms of locally finite, rooted trees, and so this extension yields interesting actions of $\text{Gal}(\overline{K}/K)$ on these trees.

We know much about actions of $\text{Gal}(\overline{K}/K)$ on $p$-adic vector spaces such as étale cohomology groups of varieties over $K$, and the theory has found many applications, in particular in the proof of Fermat’s Last Theorem [39, 41] and similar results. The Fontaine-Mazur conjecture however predicts that such actions are always ramified in particular of $\text{Gal}(\overline{K}/K)$ on $p$-adic analytic quotients reveals little about $p$-extensions of $K$ unramified at $p$. My extension of the Fontaine-Mazur conjecture implies that Galois actions on trees fill this gap. This theory, which may also be of use in 3-manifold theory, is introduced in the last section.

2. Some Group-Theoretical Preliminaries.

Whenever we talk about profinite groups, homomorphisms will always be continuous maps, subgroups closed, and generators will generate topologically. If $G$ is a pro-$p$ group, then it can be written as a quotient $F/R$ of a free pro-$p$ group $F$, i.e. given by a presentation. The minimal number of generators of $G$, denoted $d(G)$, is the smallest rank of such an $F$, and by Burnside’s lemma equals $d(G/\Phi(G))$, where $\Phi(G)$ is the Frattini subgroup of $G$, i.e. the intersection of all open maximal subgroups of $G$. Since $G/\Phi(G)$ is the largest elementary abelian quotient of $G$, $G/\Phi(G) \cong C_p^{d(G)}$. Dualizing, $d(G) = \dim H^1(G, \mathbb{Z}/p)$.

Likewise, if $F$ has rank $d(G)$, then the minimal number of generators of $R$ as a normal subgroup of $F$ will be denoted $r(G)$ and in fact $r(G) = \dim H^2(G, \mathbb{Z}/p)$. The most important result here is the inequality of Golod and Shafarevich [GS] that states that if $r(G) \leq d(G)^2/4$, then $G$ is infinite, not $p$-adic analytic [30] (except for the cases of $G = \mathbb{Z}_p$ and $\mathbb{Z}_p \times \mathbb{Z}_p$), and not just-infinite [42] (see below).

We shall need certain filtrations of $G$. The derived series of subgroups of $G$ is defined by $G^{(0)} = G, G^{(n)} = [G, G^{(n-1)}]$. The smallest $n$ for which $G^{(n)} = \{1\}$, if it exists, is called the derived length of $G$. Groups of derived length 1 are abelian, length 2 metabelian. The $p$-central series of $G$ is defined by $P_0(G) = G, P_n(G) = P_{n-1}(G)^p[G, P_{n-1}(G)]$. The smallest $n$ for which $P_n(G) = \{1\}$, if it exists, is called the $p$-class of $G$. Note that $P_1(G) = \Phi(G)$ and that if $G$ is finite, then the $p$-class and derived length both exist, the former being at least the latter.

If $G$ is any infinite, finitely generated pro-$p$ group, then it has minimally infinite quotients called just-infinite pro-$p$ groups [26]. The attempted classification [16] of just-infinite pro-$p$ groups has so far yielded four classes of just-infinite pro-$p$ groups, namely

I. Solvable (and so linear over $\mathbb{Z}_p$).
II. Nonsolvable and linear over $\mathbb{Z}_p$.
III. Nonsolvable and linear over $\mathbb{F}_p[[T]]$. 
IV. The rest!

At present, the rest consists of certain subgroups of the Nottingham groups $R_k$ ($k$ a finite field) (in particular open subgroups, the Fesenko groups [18], and the Barnea-Klopsch groups [3]), where $R_k$ consists of the automorphisms $T \mapsto T + a_2 T^2 + a_3 T^3 + \ldots$ of $k[[T]]$, and Grigorchuk-type (or ‘branch’) groups [23], which are certain pro-$p$ automorphism groups of the regular $p$-ary rooted tree. This tree has $p^n$ vertices at distance $n$ from its root with each vertex above the root having valency $p + 1$. In fact, Grigorchuk [23] has proved that every just-infinite pro-$p$ group either is branch or contains an open subgroup of the form $H \times \ldots \times H$ (finitely many factors), where $H$ is hereditarily just-infinite (i.e. every open subgroup of $H$ is just-infinite).

Note also that each of the types of just-infinite pro-$p$ groups is attached to a kind of Galois representation. Linear representations over $\mathbb{Z}_p$ and $\mathbb{F}_p[[T]]$ are well-known and important. The field of norms construction yields representations of local Galois groups into $R_k$, something that Fesenko has attempted to globalize. In section 7, we explore possible Galois representations into branch groups.

3. The Ramified Case.

A good reference for this section is Koch’s book [27]. We assume $p > 2$ in this section. Let $K$ be a finite Galois extension of $\mathbb{Q}$ with Galois group $H$. Let $r_2$ be the number of complex places of $K$ ($[K : \mathbb{Q}]/2$ if $K$ is complex, else 0). If $v$ is a place of $K$, then $K_v$ will denote the completion of $K$ at $v$, a local field. If $F$ is a field, set $\delta(F) = 1$ if $F$ contains a nontrivial $p$th root $\zeta_p$ of 1, $\delta(F) = 0$ otherwise.

Let $Z_S$ be the set of nonzero elements $x$ of $K$ such that the fractional ideal $(x)$ is a $p$th power and such that $x$ is a $p$th power in each completion $K_v$ for $v \in S$. Then $K^{*p} \subseteq Z_S$. Let $B_S$ denote the quotient $\mathbb{F}_p[H]$-module $Z_S/K^{*p}$.

**Proposition ([27, 34])**

(a) $d(G_S) = r_2 + 1 + r(G_S)$

(b) $r(G_S) = \left( \sum_{v \in S} \delta(K_v) \right) - \delta(K) + \dim_{\mathbb{F}_p} B_S$

Note that $d(G_S) - r(G_S) = r_2 + 1 > 0$ confirming that $G_S$ has an infinite abelian quotient (in fact coming from the cyclotomic extension $\text{Gal}(\cup K(\zeta_{p^n})/K)$).

Let $E$ and $E_v$ denote the units modulo $p$th powers of the rings of integers of $K$ and $K_v$ respectively. If the class number $h(K)$ is prime to $p$, then global class field theory gives an exact sequence of $\mathbb{F}_p[H]$-modules:

$$(*): 0 \rightarrow B_S \rightarrow \oplus_{v \in S} E_v \rightarrow G_S / \Phi(G_S) \rightarrow 0.$$  

For each rational prime $\ell$, let $H_\ell$ be a decomposition subgroup of $H$ for $\ell$ and let $H_\infty$ be the subgroup generated by a chosen complex conjugation. Let $\mu_p$ be the group of $p$th roots of 1 in $K$ with the Galois $H$ (and so $H_\ell$) actions (note: $\mu_p$ can be trivial).
Proposition ([10]) As $F_p[H]$-modules, if $H$ has order prime to $p$,
\[
\oplus_{v \in S} E_v \cong F_p[H] \oplus (\oplus_{\ell \in S_0} \text{Ind}^H_{H\ell} \mu_p),
\]
\[
\cong E \oplus F_p \oplus \text{Ind}^H_{H\infty} F_p.
\]

The relations coming from $B_S$ are called the unknown relations, since they do not come from the relations of the local Galois groups, which are well-known to be tame or Demushkin. This situation is remedied either by noting that increasing $S$ decreases $B_S$ (and so auxiliary primes are routinely added to reduce $B_S$ to 0) or by employing the following fact.

Proposition ([27]). If $\delta(K) = 1$, then $B_S$ is a quotient $F_p[H]$-module of the ideal class group modulo $p$th powers.

The maximal metabelian quotient of $G_S$ is studied by means of Iwasawa theory [40]. In certain cases, $G_S$ can be presented exactly - for example, if $K = \mathbb{Q}, p = 2$, and $S = \{2\}$, then Markscheits [31] showed that $G_S = \langle x, y \mid x^2 \rangle$.

4. The Analogy With 3-manifold Theory.

As noted elsewhere [33], there are analogues between these Galois groups and link groups. Assume that $S$ contains the primes above $p$. Then $G_S$ has an infinite abelian quotient isomorphic to $\mathbb{Z}_p$, corresponding to the union of cyclotomic fields. The action of this on $G_S'/G_S^{(2)}$ yields Iwasawa’s characteristic polynomial [31], which Mazur and Wiles [32] proved coincides with the Leopoldt-Kubota $p$-adic L-function. The fundamental group of a knot complement has similar properties, leading to the Alexander polynomial. In the unramified case, there are still similarities with link groups, mentioned below.

5. The Unramified Case.

Suppose for simplicity that $K = \mathbb{Q}$. In the unramified case, we assume $p \not\in S$. Suppose $S = \{p_1, ..., p_n\}$ and that $p^{e_i}$ exactly divides $p_i - 1$. If $e_i = 0$, then in every $p$-extension of $\mathbb{Q}$, $p_i$ is unramified and so can be omitted from $S$. We therefore assume, without loss of generality, that $e_i \geq 1$ for all $i$. Then it is known [20, 37] that $d(G_S) = \tau(G_S) = |S|$. Moreover the inertia subgroups $I_i$ at $p_i$ are procyclic subgroups $< \tau_i >$ of $G_S$, defined up to conjugacy, and the generators of $G_S$ are the generators $\tau_i (1 \leq i \leq n)$.

As for the relations of $G_S$, these are the local tame relations $\sigma_i^{-1} \tau_i \sigma_i = \tau_i^{p_i}$, where the decomposition subgroup of $G_S$ at $p_i$ is $< \sigma_i, \tau_i >$. We do not know formulae for $\sigma_i$ in terms of $\tau_1, ..., \tau_n$, although approximations to it modulo $G_S^{(2)}$ are given in [27]. These are related to linking numbers and Milnor invariants [33]. In general, we cannot give an explicit presentation for $G_S$.

What we can do is to define an NT-group of type $[m_1, ..., m_n]$, where $m_1, ..., m_n$ are powers of $p$, to be a pro-$p$ group with presentation of the form $< \tau_1, ..., \tau_n \mid \tau_1^{m_1} = \cdots = \tau_n^{m_n} >$. 


ray class group information. This enabled us to hunt down for which the abelianizations of their low index subgroups were too large, given the \( G \) and \( \sigma \), on the family of groups so obtained have been partially proven by [17].

We pruned this tree by eliminating all groups for which the abelianizations of their low index subgroups were too large, given the ray class group information. This enabled us to hunt down \( G_S \), usually obtaining a short list of very similar possible isomorphism types for it. In each of the \([2, 4]\) cases tried, this culminated in \( G_S \) being a finite group. Some conjectures from [9] on the family of groups so obtained have been partially proven by [17].

[9] also considered some cases with \( p = 3 \). The 3-groups obtained there fit into a family previously studied by Andoszkii and Cvetkov [2]. They are all related to the 3-adic analytic group \( H = \ker(GL_2(\mathbb{Z}_3) \to GL_2(\mathbb{F}_3)) \) in that if \( G_S \) has 3-class \( n \), then \( G_S/P_{n-1}(G_S) = H/P_{n-1}(H) \). We call \( H \) the governing group of the family. This seems to be a general phenomenon - for instance, Bush [14, 15] has recently studied maximal everywhere unramified \( p \)-extensions of imaginary quadratic fields \( K \). In the case \( p = 2 \), he obtains results similar to [9] with consequences for the root-discriminant problem [24]; in the case \( p = 3 \), the Galois groups are Schur \( \sigma \)-groups [28], meaning that \( r(G_S) = d(G_S) \) and that \( G_S \) has an automorphism of order 2 (complex conjugation in fact) that inverts every element of its abelianization. Bush obtains new families of Schur \( \sigma \)-groups, one of which has governing group a Sylow 3-subgroup of \( PSL_2(\mathbb{Z}_3) \).

For general \( K \), a theorem of Shafarevich [37] says that \( r(G_S) \leq d(G_S) + [K : \mathbb{Q}] - 1 \) and so by Golod-Shafarevich, \( G_S \) is infinite if \( d(G_S) \geq 2 + 2\sqrt{[K : \mathbb{Q}]} \). Schur \( \sigma \)-groups are always infinite if \( d(G_S) \geq 3 \) by refinements of Golod-Shafarevich [28].

6. A New Approach To Fontaine-Mazur.

If \( L/K \) is an infinite \( p \)-extension unramified at the primes above \( p \), then the structure of \( \text{Gal}(L/K) \) is much more of a mystery, although the conjecture of Fontaine-Mazur [19] says that it should not be \( p \)-adic analytic. In fact, no explicit presentation of such a group is known in the case of \( L/K \) ramified at finitely many primes. If we allow infinitely many primes to ramify, the recent work of Khare, Larsen, and Ramakrishna [25] exhibits a \( p \)-extension ramified at infinitely many primes but not at \( p \), with \( p \)-adic analytic Galois group. We, however, shall focus on the finitely ramified case. In this section, we pick the simplest example
where $G_S$ is known to be infinite, list all the properties it must satisfy, and obtain a conjecture as to its structure. For more details see [8].

Let $p = 2, K = \mathbb{Q}$, and $S = \{q, r\}$ where $q$ and $r$ are distinct odd primes. Then $G_S$ is known by the last section to be the NT-group with pro-2 presentation $\langle x, y | x^a = x^q, y^b = y^r \rangle$. NT-groups of type $[2, 2]$ are known to be finite, and the evidence from section 5 suggests that NT-groups of type $[2, 4]$ are always finite. We therefore try the next simplest case of $[4, 4]$ NT-groups, i.e. $q, r \equiv 5 \pmod{8}$. For many such $q, r$, the method of section 5 leads to $G_S$ being finite. If, however, one of the primes $q, r$ is a 4th power modulo the other but not vice versa, then a refinement of Golod-Shafarevich due to Kuhnt [29] shows that $G_S$ is infinite.

We, therefore, conduct in this case a search using the computer algebra system MAGMA [6], for presentations of the given form that satisfy everything we know of $G_S$. Picking words $a, b$ in $x, y$ at random, we filter out those abstract groups $G = \langle x, y | x^a = x^q, y^b = y^r \rangle$ that have low index subgroups (with core of 2-power index) with infinite abelianization (i.e. fail FIFA) and those for which the sequence $\langle G/P_n(G) \rangle$ stabilizes (i.e. have finite pro-2 completion). Amazingly, the groups that survive these filters fit into a simply described family, leading to the following conjecture.

**Conjecture.** There exists a subset $\mathcal{F}$ of the free pro-2 group on $x, y$ such that any $[4, 4]$ NT-group (such as $G_S$ for $S = \{q, r\}, q, r \equiv 5 \pmod{8}, q$ a 4th power modulo $r$ but not vice versa) has presentation $\langle x, y | x^a = x^5, y^a = 1 \rangle$ with $a \in \mathcal{F}$.

The shortest elements in $\mathcal{F}$ have length 6 and there are 48 of them, for instance $y^2xyxy, y^2xyx^{-1}y^{-1}, \ldots$

Moreover, the sequence $\log_2(|G/P_n(G)|)$ is always the same, namely

$(\Sigma) : 2, 5, 8, 11, 14, 16, 20, 24, 30, 36, 44, 52, 64, 76, 93, 110, 135, 160, 196, 232, 286, 340, 419, 498, 617, 736, 913, 1090, 1357, 1634, \ldots$

Putting sequence $\Delta_n := \log_2(|G/P_n(G)|)$ into Sloane’s On-Line Encyclopedia of Integer Sequences http://www.research.att.com/~njas/sequences/Seis.html yields A001461, arising in the paper [12] concerning knot theory and quantum field theory. If so, $\Delta_{2n-2} = \Delta_{2n-1} = \sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)(F_{d-1} + F_{d+1})$, where $\mu$ is the usual M"obius function and $F_n$ the $n$th Fibonacci number (so in fact $F_{d-1} + F_{d+1}$ is the $d$th Lucas number).

Letting $L(G) = \oplus P_n(G)/P_{n+1}(G)$, the $\mathbb{F}_p$-Lie algebra of $G$, it appears further that all the $[4, 4]$ NT-groups possess the same $\mathbb{F}_p$-Lie algebra. There are algebras arising in other areas of mathematics whose graded pieces have the same dimensions, namely (i) the free Lie algebra generated by one generator in degree 1 and one in degree 2 (arising in work on multi-zeta values and quantum field theory [12]) and (ii) Cameron’s permutation group algebra [21] of $C_2 \wr A$, where $A$ is the group of all order-preserving permutations of the rationals. This suggests the following amazing possibility.

**Conjecture.** If $G$ is a $[4, 4]$ NT-group, then $L(G)$ is the $\mathbb{F}_p$-Lie algebra in (i) or (ii) above.

7. Tree Representations.
In the unramified case, the Fontaine-Mazur conjecture [19] says that the just-infinite quotients of $G_S$ are never $p$-adic analytic. My extension [7] gives evidence that these just-infinite quotients always lie on the other side of Grigorchuk’s dichotomy [23]:

**Conjecture.** Assume $S \cap S_p = \emptyset$. The just-infinite quotients of $G_S$ are branch.

**Corollary to Conjecture.** The unramified Fontaine-Mazur conjecture [19] (and its generalization in [7]) holds.

This suggests a study of Galois representations into automorphisms of locally finite, rooted trees, where the image is branch. At first glance there are too many of these to be useful since every finitely generated pro-$p$ group embeds in the automorphism group $W$ of the regular $p$-ary rooted tree $T$ [23]. Our conjecture, however, concerns representations with large image. This is a familiar idea from the theory of $p$-adic representations, although here ‘large’ cannot mean ‘of finite index’ since $W$ is not finitely generated, whereas our Galois groups are. To define ‘large’, we need the notion of Hausdorff dimension [4].

Let $W_n$ be the quotient of $W$ given by its action on the subtree of vertices of distance $\leq n$ from the root of $T$. If $G$ is a closed subgroup of $W$, its Hausdorff dimension is defined to be $\liminf_{n \to \infty} \log |G_n| / \log |W_n|$, where $G_n$ is the image of $G$ in $W_n$. So, for instance, the first branch group discovered (by Grigorchuk) [23] has Hausdorff dimension $5/8$. If $G$ is any pro-$p$ group, then we define its Hausdorff dimension to be the supremum of its Hausdorff dimensions over all embeddings into $W$.

**Conjecture.** A just-infinite pro-$p$ group is branch if and only if its Hausdorff dimension is nonzero.

This conjecture is purely group-theoretical. The evidence for it is that all hereditarily just-infinite pro-$p$ groups have Hausdorff dimension zero, whereas, so far, every branch group whose Hausdorff dimension has been calculated, is of nonzero dimension. Abért and Virág [1] has made some progress on the conjecture.

Combining the two conjectures we see that when $G_S$ has infinite quotients, it should have maps to $W$ with ‘large’ image. These arise by mapping $G_S$ onto a just-infinite quotient $J$ and then embedding $J$ in $W$ with nonzero Hausdorff dimension.

We concentrate on the $p = 2$ case here. There are straightforward generalizations to other $p$, but this is computationally most convenient. Let $W_1 = C_2$ and $W_n = W_{n-1} \wr C_2$ ($n \geq 2$). Then $W_n$ is a finite $2$-group of order $2^{2^n - 1}$, that naturally arises as the automorphism group of the binary tree $T_n$, which consists of a single root vertex with two edges above each vertex to the next level extending to level $n$ (in fact, $W_n$ is isomorphic to the Sylow 2-subgroup of the symmetric group on $2^n$ letters). Thus $W_{n-1}$ is naturally a quotient of $W_n$ and we set $W = \lim \leftarrow W_n$, an infinitely generated pro-$2$ group, which is the automorphism group of the infinite binary tree $T$. We shall be interested in representations of $G_{\overline{Q}} := \text{Gal}(\overline{Q}/Q)$ into $W = \text{Aut}(T)$.

The only place where representations of this kind have been studied so far is by Odoni [36], who in work completed by Stoll [38], showed that the Galois group
of the \( n \)th iterate of \( x^2 + 1 \) is \( W_n \), so that letting \( n \to \infty \), we obtain a surjective representation \( G_\mathbb{Q} \to W \). In showing surjectivity, their approach was to prove that new primes were ramified at each level. Since \( W \) is not finitely generated, any surjective representation must be ramified at infinitely many primes.

Pink has also studied Galois groups of iterates in the case of \( \mathbb{Q} \) replaced by the function field of a finite field \( \mathbb{F}_p \), so iterating morphisms \( f : X \to X \). Here, unlike the characteristic 0 case, there are finitely many ramification points, leading to finitely generated subgroups of \( W \), which can sometimes be computed. It is easy to see using the Riemann-Hurwitz genus formula that if \( X \) is an irreducible curve of genus \( g \), then if there exists a non-constant morphism \( f : X \to X \) of degree \( > 1 \), then \( g = 0 \) or \( 1 \). In this latter case, \( f \) is unramified and the image of the geometric fundamental group is abelian with \( \leq 2 \) generators. Thus, the case of \( X = \mathbb{P}^1 \) is forced upon us.

An example of a representation \( G_\mathbb{S} \to W_4 \) with large image and \( \mathbb{S} \) not containing 2 is given in the last section of my work with Leedham-Green [9].

Some questions that arise from this are:

(i) Is there a “natural” way to construct finitely ramified tree representations in the number field case, perhaps by using a series of quadratic covering maps (the Odoni-Stoll case corresponding to the case of \( \mathbb{P}^1 \to \mathbb{P}^1 \) given by \( x \mapsto x^2 + 1 \))? Tools from algebraic geometry could then reenter.

(ii) Given a finitely ramified tree representation, do the images of Frobenius elements carry arithmetical information? Are there objects related to the representation in a way similar to modular forms being related to \( p \)-adic representations via the traces of the images of Frobenius elements? The conjugacy classes of the automorphism groups of \( p \)-ary trees have been studied - see e.g. [13]. In particular, there are uncountably many conjugacy classes. Is there a countable collection to which images of Frobenius elements are constrained? (Compare the situation of representations into \( GL_n(\mathbb{Z}_p) \), which has uncountably many conjugacy classes. Representations of arithmetical interest map Frobenius elements into the countably many conjugacy classes that have characteristic polynomials with algebraic coefficients.) Pink has suggested that perhaps a finite automaton might describe the permissible conjugacy classes.

BIBLIOGRAPHY

[38] M. Stoll, Galois groups over $\mathbb{Q}$ of some iterated polynomials, Arch. Math. (Basel) 59 (1992), no. 3, 239–244.

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: boston@math.wisc.edu