JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Nigel BOSTON

Galois groups of tamely ramified p-extensions

Tome 19, n° 1 (2007), p. 59-70.

<http://jtnb.cedram.org/item?id=JTNB_2007__19_1_59_0>

Journal de Théorie des Nombres
de Bordeaux **19** (2007), 59-70

Galois groups of tamely ramified p-extensions

par Nigel BOSTON

Résumé. On connait très peu à propos du groupe de Galois de la p-extension maximale non-ramifiée en dehors d'un ensemble fini S de nombres premiers d'un corps de nombres lorsque les nombres premiers au-dessus de p ne sont pas dans S. Nous décrivons des méthodes pour calculer ce groupe quand il est fini et ses propriétées conjecturales quand il est infini.

Abstract. Very little is known regarding the Galois group of the maximal p-extension unramified outside a finite set of primes S of a number field in the case that the primes above p are not in S. We describe methods to compute this group when it is finite and conjectural properties of it when it is infinite.

1. Introduction

Let K be a number field, S a finite set of primes of K, and p a rational prime. The Galois group over K of the maximal extension unramified outside S will be denoted $G_{K,S}$. Algebraic geometry produces p-adic representations of $G_{K,S}$ by its action on subquotients of étale cohomology groups of varieties defined over K. The Fontaine-Mazur Conjecture [18] says that these representations are precisely the potentially semistable representations of $G_{K,S}$, a group-theoretical characterization.

For the whole of this paper we make the assumption (T) that no prime above p lies in S. In this case Fontaine and Mazur conjecture that:

Conjecture. Under (T), every representation $\rho : G_{K,S} \to GL_n(\mathbf{Q}_p)$ has finite image.

There are a couple of equivalent forms of this conjecture [8]. Let $G_{K,S}(p)$ denote the Galois group over K of the maximal p-extension unramified outside S. A (finitely generated) pro-p group is called analytic if it embeds in $GL_n(\mathbf{Q}_p)$ for some n.

Conjecture. Under (T), $G_{K,S}(p)$ has no infinite analytic quotient, i.e. if L/K is an infinite pro-p extension ramified at finitely many primes (none above p), then $\mathrm{Gal}(L/K)$ is not analytic.

Manuscrit reçu le 10 janvier 2006.

Call a pro-p group just-infinite if its only infinite quotient is itself. Every infinite, finitely generated pro-p group has a just-infinite quotient and the tame Fontaine-Mazur conjecture reduces to a statement about these quotients.

Conjecture. Under (T), no just-infinite quotient of $G_{K,S}(p)$ is analytic.

This begs the question of what these just-infinite quotients actually are then.

In this paper, a natural conjecture is made regarding the pro-p groups $G_{K,S}(p)$ under assumption (T). This is analogous to the virtual positive Betti number conjecture on fundamental groups of certain 3-manifolds. This conjecture leads to interesting refinements of the above Fontaine-Mazur Conjecture and suggests that there should exist a theory of 'arboreal' Galois representations in parallel to the established theory of p-adic Galois representations. This latter theory is probably of no help in investigating $G_{K,S}(p)$ under assumption (T), as indeed the Fontaine-Mazur conjecture predicts. The new theory of arboreal Galois representations gives glimpses into a rich new field at an early stage of development.

2. VGS Conjecture

For many years it was not known whether under (T) infinite $G_{K,S}(p)$ even existed. Finally, this was resolved by Golod and Shafarevich [20]. The generator rank and relation rank of a pro-p group G will be denoted by $d(G)$ and $r(G)$ respectively.

Definition. A pro-p group G is called Golod-Shafarevich if $d(G)$ and $r(G)$ are finite and satisfy $r(G) \leq d(G)^2/4$.

The following two theorems imply for instance that under (T), $G_{\mathbf{Q},S}(p)$ is infinite if S is a finite set of rational primes with at least 4 elements.

Theorem 2.1. (1) *Every Golod-Shafarevich pro-p group is infinite* [20].
(2) $d(G_{\mathbf{Q},S}(p)) = r(G_{\mathbf{Q},S}(p)) = |S|$ [33].

If $|S| = 1$, then $G_{\mathbf{Q},S}(p)$ has 1 generator and 1 relator, so is finite, cyclic. If $|S|$ is 2 or 3, then there are examples known both of finite and infinite $G_{\mathbf{Q},S}(p)$. An illustrative example is the following:

Example. [11] Suppose $p = 2$ and $S = \{q, r, s\}$ where $q, r, s \equiv 3 \pmod 4$ and cannot be ordered so that $\left(\frac{q}{r}\right) = \left(\frac{r}{s}\right) = \left(\frac{s}{q}\right)$, e.g. $S = \{3, 19, 43\}$. Then $G_{\mathbf{Q},S}(p)$ has a subgroup H of index 2 whose fixed field is imaginary. An extension of Theorem 2.1(2) implies that $r(H) = d(H)$. By class field theory, H^{ab} is isomorphic to the 2-Sylow subgroup of a ray class group, calculated to be $(\mathbf{Z}/2)^4$, denoted $[2, 2, 2, 2]$ for simplicity. Thus, $d(H) =$

$r(H) = 4$ and since H is Golod-Shafarevich, it is infinite, as must $G_{\mathbf{Q},S}(p)$ be.

My main claim is that this approach to showing infiniteness should be generally applicable. More precisely, in analogy with Lubotzky's conjecture on 3-manifold groups [29], I conjecture:

Virtually Golod-Shafarevich (VGS) Conjecture. If L/K is an infinite pro-p extension ramified at finitely many primes (none above p), then $\mathrm{Gal}(L/K)$ has an open (i.e. finite-index) subgroup that is Golod-Shafarevich.

We begin by obtaining some refinements of the Fontaine-Mazur Conjecture as consequences. These depend on a famous conjecture of Zelmanov's that is close to being proven (and therefore denoted ϵ). Many cases have been established by Zubkov [37], Barnea-Larsen [3], and Zelmanov himself.

Conjecture ϵ. Nonabelian free pro-p groups are not linear.

Here, linear means over any p-adic ring, including e.g. $\mathbf{F}_p((t))$. Conjecture ϵ is related to our work via a theorem of Wilson and Zelmanov [36].

Theorem 2.2. *Every Golod-Shafarevich pro-p group contains a nonabelian free pro-p group.*

This now gives an explanation for the Fontaine-Mazur Conjecture under (T).

Theorem 2.3. *The VGS Conjecture together with ϵ implies the Fontaine-Mazur Conjecture under (T).*

This follows since $\mathrm{Gal}(L/K)$ cannot be both virtually-Golod-Shafarevich and analytic. Indeed, it implies my extension of the Fontaine-Mazur conjecture that suggests that under (T) every representation $\rho : G_{K,S} \to GL_n(R)$, where R is any p-adic ring, should have finite image. In fact, we get much more by using part of the (incomplete) classification of just-infinite pro-p groups.

Theorem 2.4. *(Grigorchuk* [22]*) A just-infinite pro-p group either*

(a) has a subgroup of finite index isomorphic to $H \times ... \times H$ with H hereditarily just-infinite

or

(b) is branch.

Hereditarily just-infinite pro-p groups are ones where every finite-index subgroup is also just-infinite. Since Golod-Shafarevich groups are never just-infinite (except for $\mathbf{Z}_p$, which cannot arise here), we deduce the following, which answers the question posed towards the end of the Introduction.

Theorem 2.5. *The VGS Conjecture together with ϵ implies that under (T) the just-infinite quotients of $G_{K,S}(p)$ are branch groups.*

A branch pro-p group is a certain kind of subgroup of the automorphism group of a locally finite, rooted tree, and so this implies that there exist actions with infinite image of $G_{K,S}(p)$ on such trees. In fact these actions should be large in another sense.

Definition. [4] Let T be a locally finite, rooted tree, and T_n denote the (finite) subtree of all vertices of distance at most n from the root. Let G be a (closed) subgroup of $\mathrm{Aut}(T)$ and G_n its image in $\mathrm{Aut}(T_n)$. The Hausdorff dimension of G in $\mathrm{Aut}(T)$ is defined to be lim inf, as $n \to \infty$, of $\log(|G_n|)/\log(|\mathrm{Aut}(T_n)|)$.

I conjectured that the branch groups are precisely those which embed with nonzero Hausdorff dimension. Abért and Virág [1] produced several interesting results concerning this conjecture. In fact:

Definition. Let T be a locally finite, rooted tree. A subgroup G of $\mathrm{Aut}(T)$ is called *spherically transitive* if it acts transitively on the vertices at distance n from the root, for every n. The rigid stabilizer of vertex v is the subgroup of G of elements acting trivially on the complement of the subtree with root v. Then G is called *branch* if for every n the subgroup generated by the rigid stabilizers of vertices of level n has finite index in G.

Finally, note that VGS Conjecture is analogous to the Virtual Positive Betti Number Conjecture, which states that the fundamental group of certain 3-manifolds should have a subgroup of finite index with infinite abelianization. This leads to the following definition.

Definition. A pro-p group satisfies FAb if every open subgroup of it has finite abelianization.

Unlike the 3-manifold groups, our pro-p Galois groups satisfy FAb, since class field theory identifies abelianizations with Sylow p-subgroups of ray class groups and under (T) those are finite. The VGS Conjecture and Virtual Positive Betti Number Conjecture do however both indicate that fundamental groups (pro-p or otherwise) are in some sense large.

3. Explicit finite Galois groups

We are curious about the structure of $G_{K,S}(p)$. There are various ways to compute explicit presentations. One method, due to Leedham-Green and me [11], is to find $G_{K,S}(p)$ in O'Brien trees [31]. We define the *p-central series* of a finite p-group G by setting $P_0(G) = G$ and $P_c(G) = [P_{c-1}(G), G]P_{c-1}(G)^p$ $(c = 1, 2, ...)$. The smallest c such that $P_c(G) = 1$ is the *p-class* of G. We say that G is a *descendant* of H if $G/P_c(G) \cong H$

for some c. Thus the d-generated finite p-groups are the descendants of C_p^d. Organizing these descendants into a tree, the ends of the tree are the d-generated pro-p groups.

O'Brien [31] makes it computationally efficient to search in these trees for $G_{K,S}(p)$. Number-theoretical information such as the abelianizations of low index subgroups (computed as ray class groups by class field theory), the form of the relations (in the simplest cases all relations come from local tame relations which say that a generator is conjugate to a certain power of itself), and constraints on the number of relations coming from Galois cohomology [26] is used to prune the tree. In [11] and [17], this was used to show in some cases that $G_{K,S}(p)$ is one of a short list of groups. For example, $G_{\mathbf{Q},\{5,19\}}(2)$ is isomorphic to either $< x, y | x^2, yxyxy^3xy^{-2}xy^{-2}xy^{-5}x >$ or to $< x, y | x^2, yxy^2xy^2xyxy^3xy^{-5}x >$, both of order 2^{19} and 2-class 11.

4. Explicit infinite Galois groups

For infinite $G_{K,S}(p)$, this search fails, but we can impose a new condition using the fact that $G_{K,S}(p)$ satisfies FAb. For $K = \mathbf{Q}$ all the relations are tame and we define NT-groups as follows [9].

An $[r_1, ..., r_n]$ *NT-group* is a pro-p group with presentation of the form

$$(*) \quad G =< x_1, ..., x_n | x_i^{a_i} = x_i^{r_i+1} \text{ for } i = 1, ..., n >$$

where the a_i are elements of the free pro-p group F on generators $x_1, ..., x_n$, such that G satisfies FAb. The following theorem (of Shafarevich) captures the fact that all the relations of $G_{\mathbf{Q},S}(p)$ come from local Galois groups.

Theorem 4.1. *If $S = \{q_1, ..., q_n\}$, then setting r_i to be the highest power of p dividing $q_i - 1$, $G_{\mathbf{Q},S}(p)$ is an $[r_1, ..., r_n]$ NT-group.*

In [9], using Magma [7] it appeared that all [4,4] NT-groups have presentation $< x, y | x^a = x^5, y^4 = 1 >$ with $a \in F$, a particular subset of the free pro-2 group on x, y. The shortest element of F is y^2xyxy. Moreover, the sequence $\log_2(|G/P_n(G)|)$ is always the same, namely

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

Putting sequence $\Delta_n := \log_2|P_n(G)/P_{n+1}(G)|$ into Sloane's On-Line Encyclopedia of Integer Sequences `http://www.research.att.com/~ njas/sequences/Seis.html` yields A001461, arising in knot theory and quantum field theory [13]. 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 μ is the usual Möbius function and F_n the nth Fibonacci number (so in fact $F_{d-1} + F_{d+1}$ is the dth Lucas number).

Letting $L(G) = \oplus P_n(G)/P_{n+1}(G)$, the $\mathbf{F}_p$-Lie algebra of G, it appears further that all the [4, 4] NT-groups possess the same $\mathbf{F}_p$- 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 [13]) and (ii) Cameron's permutation group algebra [19] of $C_2 \wr A$, where A is the group of all order-preserving permutations of the rationals.

The VGS Conjecture now presents a method (map) for finding number-theoretical cases to which the above applies. The abstract NT-groups above each have a normal subgroup H of index 4 with $d(H) = r(H) = 4$ (and so H is Golod-Shafarevich). To show that a particular $G_{\mathbf{Q},\emptyset}(2)$ is infinite, we simply use this as a map to locate the corresponding number field (in this case the quartic subfield of $\mathbf{Q}(\zeta_q)$) to which to apply the Golod-Shafarevich criterion using Galois cohomology. It turns out then that if $S = \{q, r\}$ where $q, r \equiv 5 \pmod 8$ are primes such that one is a 4th power modulo the other but not vice versa, then $G_{\mathbf{Q},S}(2)$ is an infinite NT-group and so should have the above form of presentation. This suggests the following amazing possibility, which has been checked as far as computationally feasible.

Conjecture. Let $S = \{q, r\}$ where $q, r \equiv 5 \pmod 8$ are primes such that one is a 4th power modulo the other but not vice versa. Then the pro-2 group $G_{\mathbf{Q},S}(2)$ is isomorphic to $< x, y | x^a = x^5, y^4 = 1 >$ where $a \in F$ and $\log_2(|G/P_n(G)|)$ is given by the sequence (†).

By group theory, every $[2, 2]$ NT-group is finite. Long calculations with Magma (sometimes requiring us to check thousands of subgroups of index 64 before finding one with infinite abelianization) suggest that every $[2, 4]$ NT-group is finite. It appears that every $[3, 3]$ NT-group is finite except for the Sylow 3-subgroup of $PSL_2(\mathbf{Z}_3)$.

Labute [28] showed that for certain p and S, for instance $p = 3$ and $S = \{7, 19, 61, 163\}$, $G_{\mathbf{Q},S}(p)$ is a mild pro-p group, meaning that its relations have a particularly simple form. A striking consequence of this is that their cohomological dimension is 2 and so they are torsion-free. This contrasts strongly with the NT-group presentations found, which exhibit torsion. It appears, however (but does not quite follow from Labute's methods), that the Golod-Shafarevich subgroups of index 4 of the NT-groups above are mild. We wonder if (when no prime in S lies above p) all $G_{K,S}(p)$ are virtually mild and therefore virtually torsion-free with potential cohomological dimension 2.

5. Applications to root-discriminant bounds

Definition. The root-discriminant rd_K of a number field K is the $[K : \mathbf{Q}]$th root of $|Disc(K)|$.

Bounds on it, such as Odlyzko bounds, are applied in many areas such as existence of group schemes over $\mathbf{Z}$, of certain special Galois representations,

etc. Let $c = \liminf rd_K$ as K runs over all totally complex fields. By GRH, $c > 44$. The upper bound on c has been creeping slowly downwards and most recently $c < 82.2$ has been established by using an infinite tame tower [23]. If K is a totally complex field with infinitely many unramified extensions, then $c \geq rd_K$. It is therefore important to establish whether the p-class tower or equivalently $G_{K,\emptyset}(p)$ is infinite (for some p).

Bush [13] used O'Brien trees to answer affirmatively Stark's question as to whether the 2-class tower of $\mathbf{Q}(\sqrt{-2379})$ is finite. The next promising unresolved case, that of the 2-class tower of $\mathbf{Q}(\sqrt{-3135})$, was recently shown to be finite too by a more powerful implementation of the same method by my Ph.D. student, Nover. Nover has, however, found other imaginary quadratic fields with root-discriminant much less than 82.2 where O'Brien trees lead to combinatorial explosion, suggesting that these 2-class towers are infinite.

The VGS Conjecture gives a systematic method (map) for proving this. It says that for such an imaginary quadratic field K, $G_{K,\emptyset}(2)$ should be virtually Golod-Shafarevich. Applying the methods of Section 3 indicates that every FAb group with 3 generators and 4 relations and abelianizations of low index subgroups that match those of $G_{K,\emptyset}(2)$ has presentation of the form $< x, y, z | r_1, r_2, r_3, r_4 >$, where r_1, r_2, r_3, r_4 depend on some a in a subset F of the free pro-2 group on x, y, z (just as happened for the one-parameter family of [4, 4] NT-groups $< x, y | x^a = x^5, y^4 = 1 >$). These abstract groups can be analyzed with Magma and any Golod-Shafarevich subgroups of small index located. The corresponding number fields can then be located and shown to satisfy the Golod-Shafarevich criterion by Galois cohomology.

6. Arboreal representations

The two main sources of totally disconnected groups [35] are matrix groups over local fields and automorphism groups of locally finite, rooted trees, but whereas Galois representations into the first are well-studied, those into the latter have been barely touched. Odoni and Stoll [32],[34] produced the first examples, showing that the Galois group over $\mathbf{Q}$ of the nth iterate of $x^2 + 1$ is W_n, defined by $W_1 = C_2, W_n = W_{n-1} \wr C_2$, the full automorphism group of the level n subtree of the regular binary tree. Grigorchuk-Zuk [22], Pink, and Bartholdi-Virág [5] studied the Basilica group, obtained as the Galois group over $\overline{\mathbf{F}_5}(t)$ of $x^2 - 1$.

Note that whereas the function field case has finitely many primes ramified, the number field case typically has infinitely many primes ramified. Even if we pick a special a (such as the post-critically finite case [2]) for which the iterates of $x^2 + a$ are ramified at finitely many primes, then 2 is one of these primes. Despite discussions with many experts, we have yet

to find a way to produce the arboreal representations on p-regular rooted trees with large image, unramified at p. Iterates are, however, a good way to study arboreal representations.

The iterates of $x^2 + a$ are ramified only at 2 for only 4 values of a. The Galois groups of the iterates of $x^2 + a$ are cyclic or metabelian except in the case $x^2 - 1$ (conjugated to $(x + 1)^2 - 2$ to avoid irreducibles). The Galois group of its nth iterate is the largest possible quotient of $G_{\mathbf{Q}}(\{2\})$ (which is known to be isomorphic to $< x, y|x^2 >$) that embeds in W_n for $n = 1, 2, 3, 4$. This suggests:

Question. (NB, Jones) Do the roots of the iterates of $(x+1)^2-2$ generate the maximal pro-2 extension of $\mathbf{Q}$ unramified outside 2?

In fact the answer appears to be no since after extensive computation we now conjecture that the Galois group over $\mathbf{Q}(i)$ of the extension these roots generate is a specific subgroup of the completion of the Basilica group and this subgroup is not free.

The study of p-adic Galois representations makes great use of the images of Frobenius elements. These are conjugacy classes in matrix groups, for which traces or more generally characteristic polynomials are well-defined. Applying these to Frobenius elements yields modular forms, L-series, etc. The main question then is to find analogous invariants of conjugacy classes of automorphism groups of trees.

Invariants of such conjugacy classes, such as labeled rooted trees (or 1-2 trees) have been known to computer scientists for many years. There are uncountably many such conjugacy classes but in analogy with the p-adic representations case, where representations from algebraic geometry have images of Frobenius falling into a specified countable set namely those whose characteristic polynomial has algebraic coefficients, we expect there to be such a set for arboreal representations.

Looking for instance at the iterates of $x^2 + 1$, the cycle structure of the Frobenius at 7 is obtained by factoring the iterates modulo 7. Often *stable* factors arise, meaning that iteratively plugging $x^2 + 1$ into these factors always yields an irreducible polynomial. Dynamics gives a simple criterion for this - a polynomial is stable if its values at $1, 2$, and 5, the forward-orbit of the critical point 1, are quadratic nonresidues modulo 7. An example is $x^2 + x + 4$, which is a factor of the 3rd iterate of $x^2 + 1$. This provides a stable factor of degree 2^{n-2} of the nth iterate, which has order 2^n, so accounts for $1/4$ of the cycle structure of Frobenius.

The proportion of the factorization of the nth iterate accounted for by stable polynomials must steadily increase as n does. Under natural heuristics, we obtain a Markov model, whose prediction on the growth of the

stable proportion matches computations well. In particular, this proportion is approaching 1 (what is left decreases by approximately 0.901, which is one quarter the largest root of $x^3 - 2x^2 - 8x + 8 = 0$, each time) and thus associated to 7 we have a partition of unity into fractions with 2-power denominator. This is $1/4 + 1/8 + 3/16 + 2/32 + 8/64 + 10/128 + 8/256 + 12/512 + 22/1024 + 45/2048 + 45/4096 + 85/8192 + 179/16384 + ...$

Conjecture. (NB, Jones) For any prime $p \equiv 3 \pmod 4$, the proportion of the factorization of the nth iterate of $x^2 + 1$ (and hence of the cycle structure of Frobenius at p) that is stable approaches 1 following a Markov model.

7. Non-Abelian Cohen-Lenstra heuristics

It appears that certain pro-p groups arise as Galois groups $G_{K,S}(p)$ repeatedly whereas others never do. For instance, analytic groups should never arise by the Fontaine-Mazur conjecture. To quantify this phenomenon, in analogy to Cohen-Lenstra heuristics [15], if H is a pro-p group and x a positive real number, set $N(H, x)$ equal to the number of imaginary quadratic fields K with discriminant at least $-x$ and with $G_{K,\emptyset}(p)$ isomorphic to H.

Conjecture. (NB, Bush) For $p = 2$,

$$N(H, x) \sim c(H)x(\log\log x)^{D(H)}/(\log x)$$

as $x \to \infty$, where $D(H)$ is at most the generator rank $d(H)$.

For H cyclic this is the Cohn-Lagarias conjecture [16]. There are also conjectures for odd p.

We can prove certain cases of this conjecture. For example, if $H^{ab} = C_2 \times C_2$, then H is a Klein 4-group, dihedral, generalized quaternion, or semidihedral. Suppose K has 2-class group $C_2 \times C_2$. Kisilevsky [25] obtained criteria for each of the different possibilities for $G_{K,\emptyset}(2)$ and we checked that the conjecture holds (with $D(H) = 1 < d(H)$ interestingly for semidihedral groups).

8. Related group-theoretical problems

One family of groups for which $c(H)$ is 0 is those found by Leedham-Green and me [12]. Since $\mathbf{Q}$ has no unramified extensions, if L/K is the 2-class tower of K, then $\mathrm{Gal}(L/\mathbf{Q})$ is generated by its inertia subgroups, which have order 2. Thus $\mathrm{Gal}(L/K)$ must embed with index 2 in a group generated by elements of order 2. Not every finite 2-group does.

More interestingly yet, we observe that if $d(H) \leq 2$, then there is at most one group generated by involutions into which H embeds with index

2. This was checked for all H of order ≤ 128. In other words, $\mathrm{Gal}(L/K)$ determines $\mathrm{Gal}(L/\mathbf{Q})$. It was recently proven by me [10]:

Theorem 8.1. *If H is a pro-2 group (possibly finite) with $d(H) \leq 2$, then there exists up to isomorphism at most one pro-2 group G generated by involutions, containing H as a subgroup of index 2.*

An abstract finitely presented group with the same number of generators as relations is called a deficiency zero group. There has been a long history of searching for finite deficiency zero groups, partly because they arise as fundamental groups of certain 3-manifolds. Some families found, such as Mennicke's [30], have presentations similar to those of NT-groups. All families so far have bounded derived length, and a famous question asks whether finite deficiency zero groups of arbitrary derived length exist. The record so far has derived length 7 [24].

This connects to our work as follows. If K is an imaginary quadratic field, p is odd, then $G_{K,\emptyset}(p)$ is a Schur σ-group [27]. This means that it has an automorphism of order 2 that acts fixed-point-free on its abelianization. Bartholdi and Bush [5] looked for finite Schur σ-groups and investigated whether they arise as $G_{K,\emptyset}(p)$. For $p = 3$ they found the groups $H_n =< x, y | r_n^{-1}\sigma(r_n), t^{-1}\sigma(t) >$, where $r_n = x^3 y^{-3^n}, t = yxyx^{-1}y$, and σ is the automorphism of the free pro-3 group sending $x \mapsto x^{-1}, y \mapsto y^{-1}$.

Apparently H_n is a finite 3-group of order 3^{2+3n} and of derived length $\lceil \sqrt{n} + 1 \rceil$. Moreover, if we let $n \to \infty$ and look at the group $H =< x, y | x^3, t^{-1}\sigma(t) >$, then $H_n/P_{2n}(H_n) \cong H/P_{2n}(H)$. In fact, H is the Sylow 3-subgroup of $PSL_2(\mathbf{Z}_3)$.

Conjecture. (Bartholdi and Bush) Let H_n be given by the same presentation as above, but considered in the category of abstract groups. Then again H_n is finite and of derived length $\lceil \sqrt{n} + 1 \rceil$.

References

[1] M.ABÉRT, B.VIRÁG, *Dimension and randomness in groups acting on rooted trees.* J. Amer. Math. Soc. **18** (2005), 157–192.

[2] W.AITKEN, F.HAJIR, C.MAIRE, *Finitely ramified iterated extensions.* Int. Math. Res. Not. **14** (2005), 855–880.

[3] Y.BARNEA, M.LARSEN, *A non-abelian free pro-p group is not linear over a local field.* J. Algebra **214** (1999), 338–341.

[4] Y.BARNEA, A.SHALEV, *Hausdorff dimension, pro-p groups, and Kac-Moody algebras.* Trans. Amer. Math. Soc. **349** (1997), 5073–5091.

[5] L.BARTHOLDI, M.R.BUSH, *Maximal unramified 3-extensions of imaginary quadratic fields and $SL_2(\mathbf{Z}_3)$.* To appear in J. Number Theory.

[6] L.BARTHOLDI, B.VIRÁG, *Amenability via random walks.* To appear in Duke Math. J.

[7] W.BOSMA, J.CANNON, *Handbook of MAGMA Functions.* Sydney: School of Mathematics and Statistics, University of Sydney, 1993.

[8] N.BOSTON, *Some Cases of the Fontaine-Mazur Conjecture II.* J. Number Theory **75** (1999), 161–169.

[9] N.Boston, *Reducing the Fontaine-Mazur conjecture to group theory*. Progress in Galois theory (2005), 39–50.
[10] N.Boston, *Embedding* 2*-groups in groups generated by involutions*. J. Algebra **300** (2006), 73–76.
[11] N.Boston, C.R.Leedham-Green, *Explicit computation of Galois p-groups unramified at p*. J. Algebra **256** (2002), 402–413.
[12] N.Boston, C.R.Leedham-Green, *Counterexamples to a conjecture of Lemmermeyer*. Arch. Math. Basel **72** (1999), 177–179.
[13] D.J.Broadhurst, *On the enumeration of irreducible k-fold Euler sums and their roles in knot theory and field theory*. J. Math. Phys. (to appear).
[14] M.R.Bush, *Computation of Galois groups associated to the* 2*-class towers of some quadratic fields*. J. Number Theory **100** (2003), 313–325.
[15] H. Cohen, H. W. Lenstra, Jr., *Heuristics on class groups*. Lecture Notes in Math. **1086**, Springer-Verlag, Berlin 1984.
[16] H.Cohn, J.C.Lagarias, *On the existence of fields governing the* 2*-invariants of the class-group of* $\mathbf{Q}(\sqrt{dp})$ *as p varies*. Math. Comp. **37** (1983), 711–730.
[17] B.Eick, H.Koch, *On maximal* 2*-extensions of* $\mathbf{Q}$ *with given ramification*. Proc. St. Petersburg Math. Soc. (Russian), American Math. Soc. Translations (English) (to appear).
[18] J.-M.Fontaine, B.Mazur, *Geometric Galois representations*. Proceedings of a conference held in Hong Kong, December 18-21, 1993," International Press, Cambridge, MA and Hong Kong.
[19] J.Gilbey, *Permutation groups, a related algebra and a conjecture of Cameron*. Journal of Algebraic Combinatorics, **19** (2004) 25–45.
[20] E.S.Golod, I.R.Shafarevich, *On class field towers (Russian)*. Izv. Akad. Nauk. SSSR **28** (1964), 261–272. English translation in AMS Trans. (2) **48**, 91–102.
[21] R.Grigorchuk, *Just infinite branch groups*. New Horizons in pro-p Groups, Birkhauser, Boston 2000.
[22] R.Grigorchuk, A.Zuk, *On a torsion-free weakly branch group defined by a three state automaton*. Internat. J. Algebra Comput., **12** (2000), 223–246.
[23] F.Hajir, C.Maire, *Tamely ramified towers and discriminant bounds for number fields. II*. J. Symbolic Comput. **33** (2002), 415–423.
[24] G.Havas, M.F.Newman, E.A.O'Brien, *Groups of deficiency zero*. Geometric and Computational Perspectives on Infinite Groups, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **25** (1996) 53–67.
[25] H.Kisilevsky, *Number fields with class number congruent to* 4 (mod 8) *and Hilbert's theorem* 94. J. Number Theory **8** (1976), no. 3, 271–279
[26] H.Koch, *Galois theory of p-extensions*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.
[27] H.Koch, B.Venkov, *The p-tower of class fields for an imaginary quadratic field (Russian)*. Zap. Nau. Sem. Leningrad Otdel. Mat. Inst. Steklov (LOMI) **46** (1974), 5–13.
[28] J.Labute, *Mild pro-p-groups and Galois groups of p-extensions of* $\mathbf{Q}$. J. Reine Angew. Math. (to appear).
[29] A.Lubotzky, *Group presentations, p-adic analytic groups and lattices in* $SL_2(\mathbf{C})$. Ann. Math. **118** (1983), 115–130.
[30] J.Mennicke, *Einige endliche Gruppe mit drei Erzeugenden und drei Relationen*. Arch. Math. X (1959), 409–418.
[31] E.A.O'Brien, *The p-group generation algorithm*. J. Symbolic Comput. **9** (1990), 677–698.
[32] R.W.K.Odoni, *Realising wreath products of cyclic groups as Galois groups*. Mathematika **35** (1988), 101–113.
[33] I.R.Shafarevich, *Extensions with prescribed ramification points (Russian)*. IHES Publ. Math. **18** (1964), 71–95.
[34] M.Stoll, *Galois groups over* $\mathbf{Q}$ *of some iterated polynomials*. Arch. Math. (Basel) **59** (1992), 239–244.
[35] G.Willis, *Totally disconnected, nilpotent, locally compact groups*. Bull. Austral. Math. Soc. **55** (1997), 143–146.

[36] E.ZELMANOV, *On groups satisfying the Golod-Shafarevich condition*. New horizons in pro-p groups, Birkhaüser Boston, Boston, MA, 2000.
[37] A.ZUBKOV, *Non-abelian free pro-p-group are not represented by* 2×2*-matrices*. Siberian Math.J, **28** (1987), 64–69.

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