TAME PRO-p GALOIS GROUPS: A SURVEY OF RECENT WORK

par

Farshid Hajir

Fix a prime p, a number field K, and a finite set S of places of K none of which has residue characteristic p. Fix an algebraic closure $\overline{K}$ of K and let K_S be the maximal p-extension of K inside $\overline{K}$ which is unramified outside S; it is the compositum of all finite p-power degree extensions of K unramified outside S. We assume that real places of K not contained in S do not complexify in the extension K_S/K. Put $G_{K,S} = \mathrm{Gal}(K_S/K)$ for its (pro-p) Galois group. Very little is known about this "tame arithmetic fundamental group." Before Shafarevich's pioneering work [**Sh**], a few examples where it was possible to determine $G_{K,S}$ explicitly (and show that it was finite), were known, and it was in fact generally believed that all such $G_{K,S}$ are finite. That this is not so was first demonstrated in [**GS**] by Golod and Shafarevich.

As was noted by Artin and Shafarevich, the mere existence of infinite $G_{K,S}$ (with S finite) has an arithmetic application to the estimation of discriminants because the discriminants of successive fields in a tamely and finitely ramified tower grow as slowly as possible. For a more detailed discussion of this topic (and the analogy with curves over finite fields with many rational points) see, for example, [**HM1**] and the references therein.

***Classification mathématique par sujets* (2000).** — 11R37.
Mots clefs. — Galois groups, p-adic representations, class field towers, tame extensions of number fields.

This work was supported by the National Science Foundation under Grant No. 0226869.

Infinite $G_{K,S}$ satisfy a number of interesting group-theoretic properties (stemming from class field theory) which we will discuss below, but little attention was focussed on the group-theoretical structure of these infinite groups in the decades following their discovery. In the 1990s, through an important and influential work of Fontaine and Mazur [**FM**] on p-adic Galois representations, to this list of properties was added a conjectural one. This development is concurrent with a revitalization of the study of tame arithmetic fundamental groups.

In this brief survey, I sketch two recent contributions to this subject, the first, due to Khare, Larsen, and Ramakrishna concerning the case where S is infinite, and the second, due to Boston, suggesting a purely group-theoretical approach to the Fontaine-Mazur conjecture. I would like to thank all of these researchers for making preprints of their work available; it should be clear that the present article is merely a summary of some of their beautiful ideas. I am grateful to R. Ramkrishna and N. Boston for helpful remarks on earlier drafts of this article. Finally, I would like to thank Y. Aubry, G. Lachaud and M. Tsfasman (the organizers of AGCT-9), as well as the staff of CIRM at Luminy, for making possible a wonderful conference and inviting me to it.

1. The Tame Fontaine-Mazur Conjecture

The main thrust of attempts over the last forty years to understand the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has rested on its action on p-adic vector spaces arising from étale cohomology groups attached to geometric/analytic objects (varieties/modular forms) defined over number fields, and especially on the identification of cases where the geometric and modular ones coincide. Tremendous progress in this direction has been achieved recently, the developments leading to and resulting from the proof of Fermat's Problem comprising the most striking examples. The p-adic Galois representations arising via étale cohomology have long been suspected (and are now known [**Ts**]) to share two unique features, one local, the other global. The local one is that at primes dividing p, the restriction to the decomposition group satisfies a technical condition called *potential semi-stability* [**F**]. The global condition, namely that representations arising from geometry are unramified outside a *finite* set of primes S, is more easily grasped and has been known practically from the beginning of the subject. More precisely, outside the primes dividing

pN where N is the conductor (level) of the variety (modular form), the geometric p-adic representations are always unramified.

A fairly recent conjecture of Fontaine and Mazur [**FM**, Conj. 1] asserts that this local/global pair of properties in fact characterize representations arising from étale cohomology.

***Conjecture 1.1* (Fontaine-Mazur).** — *Suppose* $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_n(\mathbb{Q}_p)$ *is a continuous irreducible representation which satisfies*

i) *for every K-prime $\mathfrak{p}$ of residue characteristic p, the restriction of ρ to a decomposition group at $\mathfrak{p}$ is potentially semi-stable,*
ii) *ρ is unramified outside a finite set S of primes of K.*

Then ρ is (Tate-twist of) a subquotient of the action of $\mathrm{Gal}(\overline{K}/K)$ *on the étale cohomology of some smooth projective variety over K.*

The study of this conjecture, indeed of the entire subject of p-adic Galois representations, is governed by a "tame-wild dichotomy." In particular, the state of our knowledge and available tools and examples are quite rich (poor) depending on whether the set S where the representation is ramified contains (wild case) or does not contain (tame case) places of residue characteristic p. This is so largely because representations arising from étale cohomology are typically wild; for recent advances regarding Conjecture 1.1 "on the wild side," see Taylor [**T**] and Kisin [**Ki**] (as well as the corresponding "Featured" Math Reviews).

Since tame representations are automatically potentially semi-stable (by a theorem of Grothendieck [**ST**, Appendix]), a consequence of the Fontaine-Mazur conjecture (when we assume some standard conjectures in algebraic geometry – see Kisin-Wortmann [**KW**] for more details) is the following (cf. [**FM**, Conj. 5a]).

***Conjecture 1.2* (Tame Fontaine-Mazur).** — *If ρ is a p-adic representation of* $\mathrm{Gal}(\overline{K}/K)$ *unramified outside S where*

i) *S contains no primes dividing p, and*
ii) *S is finite,*

then the image of ρ is finite.

Some preliminary evidence for Conjecture 1.2 exists (Boston [**B1**], Hajir [**H1**], Wingberg [**W**]). In Section 3, we will describe a new purely group-theoretical approach to this conjecture for $K = \mathbb{Q}$ due to Boston.

2. A result of Khare, Larsen, and Ramakrishna

One-dimensional p-adic representation with finite image are well-understood, thanks to class field theory; the study of those with infinite image, which is essentially the study of $\mathbb{Z}_p$-extensions, was pioneered by Iwasawa in the 1960's. One knows, for example, that a $\mathbb{Z}_p$-extension, is unramified at primes of residue characteristic different from p; moreover, since $\mathbb{Z}_p$ is abelian, a $\mathbb{Z}_p$-extension cannot be everywhere unramified (by the finiteness of the class number). Thus, condition i) cannot be dropped from Conjecture 1.2, and moreover condition ii) holds automatically for 1-dimensional representations.

Fontaine and Mazur ask in [**FM**, p. 44] whether condition ii) of Conjecture 1.1 holds automatically for every semi-simple n-dimensional p-adic representation. The answer to this question for $n = 2$ was shown to be negative by Ramakrishna [**R1**]. In that paper he also constructed, under GRH, an irreducible 2-dimensional representation ramified at infinitely many primes but potentially semistable at p. In [**KR**], Khare and Ramakrishna gave such a construction unconditionally; in so doing, they showed that the two conditions i) and ii) in Conjecture 1.1 are independent. We should mention also that in [**KR**], Khare and Rajan showed that the set of primes ramified in a semi-simple representation is always of density 0.

The next natural question along the same lines is whether condition ii) in Conjecture 1.2 is necessary. We say a representation is *deeply ramified* at a prime if it does not vanish on any of the corresponding higher ramification groups of finite index (in the upper numbering, say). The question on the necessity of condition ii) in Conjecture 1.2 can be rephrased as follows.

Question 2.1. — *Is there a p-adic representation ramified at infinitely many primes of a number field K but not deeply ramified at p?*

In a recent preprint, Khare, Larsen, and Ramakrishna [**KLR**] give a positive answer to the above question, at least for $n = 2, p \geq 7$. I hasten to point out that this is but one small application of their striking main theorem, an existence theorem for 2-dimensional p-adic representations, which under mild hypotheses, allows one to fix the characteristic polynomial of Frobenius at a density 1 set of primes, at the cost of introducing ramification at an infinite (density 0) set of primes. For more details, the reader is referred to the preprint [**KLR**].

***Theorem 2.2* (Khare-Larsen-Ramakrishna).** — *Suppose $\overline{\rho}$: $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is a surjective residual representation unramified at $p \geq 7$. Then there exists a surjective characteristic 0 lift $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{SL}_2(\mathbb{Z}_p)$ of $\overline{\rho}$ such that, letting $K = \overline{\mathbb{Q}}^{\ker \overline{\rho}} \subset L = \overline{\mathbb{Q}}^{\ker \rho}$ be the fields cut out by $\overline{\rho}$ and ρ respectively, there are infinitely many K-primes which ramify tamely in L/K whereas all the K-primes of residue characteristic p split completely in L/K.*

One interpretation of this theorem is that Conjectures 1.1 and 1.2 are "taut," you can drop neither the local condition i) nor the global one ii). Let us put it another way: *The Fontaine-Mazur Conjecture does not reduce in a simple way to a local problem.*

In an attempt to flesh out a little the meaning of the above, admittedly vague, statement, let us recall a theorem of Sen [**S**]. Suppose F is a finite extension of $\mathbb{Q}_p$ and E/F is a totally ramified infinite extension with p-adic Lie Galois group $\mathrm{Gal}(E/F)$. Then E/F is deeply ramified, i.e. the filtration of $\mathrm{Gal}(E/F)$ by (upper-numbering) higher ramification groups does not stop after finitely many steps; when this is not so, we call the ramification "shallow." In particular, tame ramification is always shallow.

Now, suppose the answer to Question 2.1 were negative. Then, Conjecture 1.2 would have reduced to the following problem (a global version of Sen's Theorem): Suppose K is a number field, and L/K is an infinite extension with p-adic Lie Galois group. Show that for some prime $\mathfrak{P}$ of L of residue characteristic p, the local extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is deeply ramified. The Khare-Larsen-Ramakrishna Theorem shows that to the hypotheses of this problem, one *must* add that L/K is ramified at only a finite set of primes. Exactly how this global (tame) property would force deep (wild) ramification is not at all clear.

Let us approach the above discussion on a slightly different tack, from which one may catch a glimpse of a pheonomenon possibly responsible for the global-local interaction at play. The root discriminant of a number field is defined to be the nth root of the absolute value of its discriminant, where n is the degree of the number field. Let K be a number field and L an infinite extension of it. We say L/K is *asymptotically good* if there is no infinite sequence of distinct intermediate subfields of L/K with root discriminant tending to infinity, otherwise we call L/K *asymptotically bad.*

If L/K is ramified at infinitely many primes ("horizontally infinitely ramified"), then it is asymptotically bad. Similarly, if L/K is deeply ramified at some prime ("vertically infinitely ramified"), then it is asymptotically bad also. On the other hand, if the ramification is horizontally and vertically finite, then the extension is asymptotically good; for a precise bound, see [**HM2**, Theorem 4.2]. Since a shallow p-adic representation is potentially tame (essentially by Sen's theorem, see [**HM2**, §7]), we obtain an alternate description of Conjecture 1.2.

Theorem 2.3 **(Hajir-Maire [HM2]).** — *The Tame Fontaine-Mazur Conjecture holds if and only if infinite p-adic Lie extensions of number fields are always asymptotically bad.*

Given a number field K and a p-adic Galois representation ρ of $\mathrm{Gal}(\overline{K}/K)$ with infinite image, the Tame Fontaine-Mazur Conjecture asserts that ρ is either vertically or horizontally infinitely ramified. The above Theorem unifies these two notions of "infinitely ramified" under one umbrella: that of the rate of growth of the root discriminant. This reinterpretation suggests that it might prove profitable to study the problem *analytically* via the zeta and L-functions whose functional equations capture subtle information about the growth of root discriminants in the tower cut out by ρ.

3. Boston's experiment

Throughout this section, we assume S is finite and contains no primes of residue characteristic p. Then $G_{K,S}$ is a finitely generated profinite group. To see this, recall that by the Burnside Basis Theorem, the minimal number of generators of a pro-p group G is the same as that of its maximal abelian quotient G^{ab}. By class field theory, $G_{K,S}^{\mathrm{ab}}$ is canonically isomorphic to the p-Sylow subgroup of the ray class group of K modulo $\mathfrak{P}_S := \prod_{\mathfrak{p}\in S}\mathfrak{p}$, hence finite. Moreover, if H is an open (equivalently finite-index) subgroup of $G_{K,S}$, and $K' = K_S^H$ is its corresponding fixed field, then $H = G_{K',S'}$ where S' is the set of places of K' lying over those in S (since $K_S = K'_{S'}$). Thus, $G_{K,S}$ satisfies the property Boston calls FIFA ("Finite Index → Finite Abelianization"), which is also called FAB elsewhere in the literature: every subgroup of finite index has finite abelianization.

In a remarkable computer experiment, Boston [**B2**] has determined for the first time, albeit conjecturally, a family of examples of infinite $G_{K,S}$ admitting an *explicit* presentation in terms of generators and relations. Prior to his work, the information available on infinite tame fundamental groups was always fragmentary and circumstantial. To my knowledge, no one had even written down a *guess* for what a single specific such group might be.

As discussed earlier, by contrast, the study of p-adic Galois representations ramified at primes of residue characteristic p, many of which arise from algebraic geometry and modular forms, has been at the forefront of the advance of knowledge in algebaric number theory. Boston's work, therefore, has the potential of opening a vista in a part of the subject where the standard methods are predicted (by the Fontaine-Mazur Conjecture) to play a minor role. As such, it is a psychological as well as scientific breaktrough, in the sense that it renders tangible certain objects that in all previous experience had seemed visible only hazily and from a remote distance. This is especially so, as the glimpses provided by Boston's experiment point the way to connections with a circle of ideas where exciting new developments are taking place, namely quantum field theory, multi-zeta values, and the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$.

3.1. Boston's experiment begins by restricting attention to the simplest base field, namely $\mathbb{Q}$, and taking stock of all group-theoretical facts that we know about tame $G_{\mathbb{Q},S}$ with S finite. We have already mentioned that it has property FIFA. By localizing at the ramifying primes, and using the fact that the ring of integers of our base has finite unit group $\{\pm 1\}$, one can show that $G_{\mathbb{Q},S}$ has p-deficiency 0, meaning it has a pro-p presentation with d generators and d relations, where $S = \{\infty, p_1, \ldots, p_d\}$ consists of d distinct finite primes as well as the archimedean prime ∞ (which we include for convenience if $p = 2$). The triviality of the unit group modulo torsion as well as that of the class group make this a most favorable situation since we know, in a sense, where *all* the global relations originate. Namely we have one global relation coming from the local relation at each ramified prime. What these global relations exactly *are* we do not know (at the outset), of course. More details will be given momentarily in the proof of Theorem 3.2 below.

Boston observes that the presentation of $G_{\mathbb{Q},S}$ dating back to [**Sh**] and [**Ko**] (see also [**Fr**]) can be written in a more pleasant form, motivating the following definition and ensuing theorem.

Definition 3.1. — *Suppose $\boldsymbol{m} = (m_1, \dots, m_d) = (p^{r_1}, \dots, p^{r_d})$ is a d-tuple of positive powers of p. We say a pro-p group G* has a Boston presentation of type $\boldsymbol{m}$ *if it is isomorphic to*

$$\Gamma(\boldsymbol{\alpha}; \boldsymbol{m}) := \langle x_1, \dots, x_d : x_i^{\alpha_i} = x_i^{1+m_i}, 1 \le i \le d \rangle_p,$$

for some d-tuple $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_d)$ of words in the free pro-p group on $x_1, \dots, x_d$. If, in addition, G is FIFA *(every subgroup of finite index has finite abelianization), then we say G is an* NT-group.

Remark. The index p decorating the above presentation is a reminder that this presentation takes place in the category of pro-p groups. In other words, our group is the quotient of $F_d^{\text{pro-}p}$, the free pro-p group on d generators $x_1, \dots, x_d$, by the closed normal subgroup generated by relations $x_i^{\alpha_i} = x_i^{1+m_i}$; here we are using the conjugation notation $x^\alpha = \alpha^{-1} x \alpha$. Note that the maximal abelian quotient of $\Gamma(\boldsymbol{\alpha}, \boldsymbol{m})$ is $\mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_d$.

Theorem 3.2. — *Let $p_1, \dots, p_d$ be d distinct primes congruent to* 1 *modulo p. Put $S = \{\infty, p_1, \dots, p_d\}$. Let $\boldsymbol{m} = (m_1, \dots, m_d)$, where m_i is the highest power of p dividing $p_i - 1$. For $p = 2$, we assume that each $m_i \ge 4$. Then $G_{\mathbb{Q},S}$ is an NT-group of type $\boldsymbol{m}$.*

Démonstration. — By [**Ko**, §11], $G_{\mathbb{Q},S}$ has a presentation of the form

$$\langle s_1, \dots, s_d : s_i^{\delta_i} = s_i^{p_i}, 1 \le i \le d \rangle_p. \tag{1}$$

The relation $s_i^{\delta_i} = s_i^{p_i}$ says that conjugation by δ_i has the same effect on s_i as raising it to the p_ith power, so conjugation by a power of δ_i raises s_i to that power of p_i, i.e.

$$\delta_i^{-n} s_i \delta_i = s_i^{p_i^n}. \tag{2}$$

Our assumptions on p_i imply that it generates the same subgroup of $\mathbb{Z}_p^\times$ as $1+m_i$. Therefore, there is some $\nu_i \in \mathbb{Z}_p$ such that $p_i^{\nu_i} = 1+m_i$. By (2), when we let $\alpha_i = \delta_i^{\nu_i}$, we obtain the desired shape for the relations. □

3.2. Theorem 3.2 is the starting point of Boston's experiment, which is predicated on (a) the daring assumption (or hope) that $G_{\mathbb{Q},S}$ admits a presentation $\Gamma(\boldsymbol{\alpha}, \boldsymbol{m})$ where $\boldsymbol{\alpha}$ consists of relatively short words in the free group, as well as (b) the equally important insight that this type of presentation and the property of being FIFA *together* may go rather far toward characterizing a pro-2 group!

To maximize the range of computations, we take $K = \mathbb{Q}$, $p = 2$, $S = \{\infty, p_1, \dots, p_d\}$, where the p_i are distinct odd primes. We look for the simplest situation where $G_{\mathbb{Q},S}$ is infinite and seek to learn what kind of group we get in that case. If $d = 1$, i.e. $S = \{\infty, p_1\}$, then $G_{\mathbb{Q},S}$ is cyclic, hence finite, so we take $d = 2$, $S = \{\infty, p_1, p_2\}$.

That NT-groups of type $(2, 2)$ are finite follows from a classic result of Taussky-Todd, so one of our ramifying primes, say p_1, should be taken 1 modulo 4. If $p_2 \equiv 3 \pmod 4$, then $G_{\mathbb{Q},S}$ is of type $(2, 4)$; a separate experiment using his method with Leedham-Green [**BL**] leads Boston to suspect that NT-groups of type $(2, 4)$ are always finite. This brings us to NT-groups of type $(4, 4)$, which correspond to the choice

$$p_1 \equiv p_2 \equiv 5 \pmod 8. \tag{3}$$

Boston uses the software package MAGMA to perform the calculations to be described presently. Perhaps we should note here that, in practice, one works in MAGMA with the *discrete* free group and considers only those subgroups with core of 2-power index – these correspond to subgroups of the pro-2 completion of the free discrete group. (The core of H in G is the intersection of all G-conjugates of H).

Given a finite presentation for a group G and a small positive integer n (say less than 5), MAGMA can compute the list of all subgroups H of G of index 2^n and determine for each whether the maximal abelian pro-2 quotient of H is finite or not. We are most interested in *infinite* fundamental groups so would like to eliminate those groups $G = \Gamma(\alpha_1, \alpha_2; 4, 4)$ which are finite. To this end, consider the "2-central series" of G, $P_n(G) = P_n$, defined as follows. Let $P_0 = G$, and for $n \geq 0$, put $P_{n+1} = P_n^2[P_n, G]$; here P_n^2 and $[P_n, G]$ are, respectively, the *closed* sugbroup generated by the squares of elements of P_n, respectively commutators of P_n and G. For later reference, also define the graded $\mathbb{F}_2$-Lie algebra $\mathfrak{g} = \oplus_{n \geq 0} P_n/P_{n+1}$ with the natural bracket coming from the commutator. The maximal 2-class n quotient of G is $Q_n = G/P_n(G)$. If Q_n is strictly smaller than Q_{n+1} for $n < 64$, we consider it a good bet (for α_1, α_2 of short length) that $\Gamma(\alpha_1, \alpha_2; 4, 4)$ is probably infinite. (In any given case, we have number-theoretic as well as group-theoretic criteria which we can hope to apply to verify the infinitude of the groups in question.)

Boston thus sets up algorithm `IFF(L,C,D)`, an "infinite/FIFA filter," with parameters L, C, D (for length, class, and depth) as follows. We let α_1, α_2 run over all words in $F_2^{\text{pro-2}}$ of length at most L, and discard any $G = \Gamma(\alpha_1, \alpha_2; 4, 4)$ for which either

i) [infinite] $|P_n(G))| = |P_{n+1}(G)|$ for some $n \leq C$,
ii) [FIFA] G has some subgroup of index 2^n, $n \leq D$, with infinite abelian pro-2 quotient.

In practice, memory constraints and the complexity of calculations allows only small values of L, C, D, so what has been described is a simplification of the process Boston actually employed, which involves using low values of L, C, D at first, (say $L = 10$, $C = 7$, $D = 3$), then running the remaining candidates into a similar filter with slightly higher values of C and D, and so on. Happily, this process eliminated in a single overnight calculation a huge number (but, even more happily, not all!) of some 15,000 candidates. There remained 92 groups (all of large 2-class and satisfying FIFA to a large depth). Here appeared **the first surprise:** All of the survivors of the infinite-FIFA filter turned out to be extremely similar to each other, which similarity is most succinctly and elegantly expressed in the fact that they all (appear) to have the same Lie algebra $\mathfrak{g}$! We will elaborate more on this a little later.

Now let us move on to **the second surprise.** MAGMA has a facility for replacing a given presentation of a group by a simpler one. When Boston ran this for the survivors of his filter, he found that they all admit a presentation of type $\Gamma(\alpha, 1; 4, 4)$! (Here, "1" is the identity element of $F_2^{\text{pro-}p}$). In other words, Boston obtained in every case a presentation

$$G \cong \langle x, y : x^{\varphi} = x^5, y^4 = 1\rangle_2, \tag{4}$$

for $\varphi \in \mathcal{F}$, a certain subset of the free pro-2 group on 2 generators. This was yet another pleasant discovery since one expected every tame fundamental group to have non-trivial torsion; in particular, since every open subgroup is a tame fundamental group, the expectation is that tame fundamental groups are "torsion-riddled", i.e. every open subgroup has non-trivial torsion (another conjecture of Boston).

The shortest elements in $\mathcal{F}$ have length 6 (48 of them), including y^2xyxy and $y^2xyx^{-1}y^{-1}$. There are 2^8 of length 7, $2^6 \cdot 3 \cdot 5$ of length 8, $2^6 \cdot 3^2 \cdot 5$ of length 9, and $2^8 \cdot 5 \cdot 7$ of length 10. In all of these cases, the three index 2 subgroups of the group (4) all have abelianization $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$. Moreover, in all these cases one can show that G is infinite, for there is an index 4 subgroup H with generator- and relation-rank both equal to 4, so the Golod-Shafarevich bound ($r > d^2/4$ for a finite p-group) applies.

An important problem is to understand the class $\mathcal{F}$ of elements which appear in torsion-presentations of NT-groups of type $[4, 4]$ (and more general ones). In particular, we may ask

Question 3.3. — *For a fixed type $\boldsymbol{m} = (m_1, \ldots, m_d)$, is there a class $\mathcal{F}_d$ of elements of $(F_d^{pro\text{-}p})^{d-1}$ such that every infinite NT-group G of type $\boldsymbol{m}$ has a presentation of type*

$$G \approx \Gamma(\alpha_1, \ldots, \alpha_{d-1}, 1; \boldsymbol{m})$$

with $(\alpha_1, \ldots, \alpha_{d-1}) \in \mathcal{F}_d$?

Summarizing some of the experimental findings so far, we have

Conjecture 3.4. — (a) *There exists a subset $\mathcal{F}$ of the free pro-2 group on 2 generators such that every infinite NT-group of type* $(4, 4)$ *admits a presentation* $\Gamma(\varphi, 1, ; 4, 4)$*, i.e. of type (4), with $\varphi \in \mathcal{F}$.*

Moreover, for any such group G,
(b) *the dimensions of graded pieces of G, namely* $\log_2 |P_n(G)/P_{n+1}(G)|$, *is the sequence (5) to be described below.*
(c) *the index* 2 *subgroups of G all have abelianization* $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$.
(d) *G has a subgroup of index* 4 *of generator rank and relation rank both equal to* 4.

3.3. To return to our original arithmetic problem, given a pair of primes p_1, p_2, satisfying (3), we *know* that $G_{\mathbb{Q},\{\infty,p_1,p_2\}}$ is NT of type $(4, 4)$, so, according to the results of the experiment, we *expect* that if it is infinite, then it has a presentation (4) for some $\varphi \in \mathcal{F}$. Given such a p_1, p_2, what is a possible such φ? Already, given such a pair, it is not necessarily easy to determine whether the corresponding tame fundamental group will be infinite or not (we can definitely check that it is sometimes finite, however).

We can begin to answer this question by comparing the abelianization of subgroups of small index. Namely, if H is a subgroup of index 2^n in $G_{\mathbb{Q},S}$, then H^{ab} is isomorphic to the 2-part of the S-ray class group of the degree 2^n field fixed by H. Using class field theory, one can show that the three quadratic extensions inside $\mathbb{Q}_S$ (namely $\mathbb{Q}(\sqrt{p_1}), \mathbb{Q}(\sqrt{p_2}), \mathbb{Q}(\sqrt{p_1 p_2})$) all have 2-ray class group mod S of type $\mathbb{Z}/2 \times \mathbb{Z}/4 \times \mathbb{Z}/4$ if and only if one of the primes (say p_1) is a quartic residue modulo the other but not vice versa. Given Conjecture 3.4, therefore, together with this bit of arithmetic input, we find a surprisingly simple (conjectural) answer to our question about which prime pairs give infinite $G_{\mathbb{Q},\{\infty,p_1,p_2\}}$.

Conjecture 3.5. — *Given distinct primes* $p_1, p_2 \equiv 5 \pmod 8$, *the maximal* 2*-extension of* $\mathbb{Q}$ *unramified outside* $S = \{\infty, p_1, p_2\}$ *is infinite if and only if* $\left(\dfrac{p_1}{p_2}\right)_4 = -\left(\dfrac{p_2}{p_1}\right)_4$. *In this case,* $G_{\mathbb{Q},S}$ *is of type (4) for some* $\varphi \in \mathcal{F}$.

Improvements of the Golod-Shafarevich bound due to Kuhnt [**Ku**] are in fact strong enough to prove the "if part" of the first sentence in the above conjecture. The "only if part" is theoretically susceptible to verification by the computational method of Boston and Leedham-Green, though the calculations appear prohibitively long. The point that should be emphasized is the remarkable fact that we arrived at this arithmetic conjecture via a purely group-theoretical experiment!

Now, although the 92 survivors of `IFF(10,63,4)` are all rather similar, some of them can be immediately eliminated as contenders for identification with a $G_{\mathbb{Q},S}$ by pursuing further the abelianization of subgroups/class groups connection. Namely, the subgroup fixing the quartic subfield of $\mathbb{Q}(\zeta_{p_2})$ (recall our convention that p_2 is not a fourth power modulo p_1) has abelianization $(\mathbb{Z}/4)^4$ (again by computing the 2-ray class group modulo p_1p_2 of this field) and this eliminates a number of groups of type (4) from consideration. Further winnowing of this sort by going to degree 8 fields is also possible.

What emerges then is that, in this way, given a set $S = \{\infty, p_1, p_2\}$ as in Conjecture 3.5, (examples of such prime pairs are $(5, 61)$, $(13, 29)$, $(29, 53)$, $(37, 53)$), we come up with a small list of candidate elements $\varphi \in \mathcal{F}$ such that $G_{\mathbb{Q},S}$ is possibly isomorphic to (4). At the moment, there is no way to be sure if a particular φ is the right one. But it is a rather remarkable experience to make the purely group-theoretical and "elementary" calculation of the abelianization of small-index subgroups of a given group of type (4), then to do the highly non-trivial ray class group calculations and observe the exact matchings that occur repeatedly.

When witnessing the correspondence of the data from ray class groups with that coming from abelianizations of finite index subgroups, I had the distinct impression of experiencing a "reciprocity law," in the same sense that the modularity of elliptic curves over $\mathbb{Q}$ is a reciprocity law: Namely, on the modular side, one has "elementary" algorithms for calculating a basis of eigenforms of fixed weight (2) and level (say N), and on the arithmetic side, one has the more challenging arithmetic problem of listing all elliptic curves over $\mathbb{Q}$ of conductor N.

Perhaps a more accurate analogy for describing Conjecture 3.4 is to compare the information we would then have about the ray class groups of conductor p_1p_2 in this infinite (non-abelian, tame) tower with the celebrated result of Iwasawa specifying the growth of the p-rank of the class groups of conductor 1 in (abelian, wild) $\mathbb{Z}_p$-extensions. In the tame case, the presentation (4) would codify in one neat package (albeit in a less explicit form than Iwasawa's wonderful formula) a huge amount of information about ray class groups of the stories of the tower.

3.4. While the *arithmetic* problem described in the previous paragraph (of determining an exact presentation for even one pair p_1, p_2 as above) is a subtle and interesting problem, we should not lose sight of the more fundamental expectation that *all* of these groups have the same Lie algebra over $\mathbb{F}_p$, because practically any *group-theoretical* question we are interested in is captured by the Lie algebra, including whether or not the group has infinite analytic (p-adic Lie) quotients (Fontaine-Mazur). So, let us now turn to perhaps the biggest and most exciting **third surprise**, namely what emerges as a prime suspect for the common Lie algebra of infinite NT-groups of type $(4,4)$.

First of all, the dimension of its graded pieces is given by the sequence

$$\mathcal{S} : (\log_2 |P_n(G)/P_{n+1}(G)|)_n,$$

which for each of the 92 survivors of IFF is computed to be

$$\mathcal{S} : 3,3,3,3,2,4,4,6,6,8,8,12,12,17,17,25,25,36,54,54,79,79,\cdots \tag{5}$$

When shorn of the repetitions, the sequence of $\mathcal{S}$ receives one hit from the Neil Sloane Sequence Database [**Sl**]: It is A001461, which occurs in a preprint [**Br**] of Broadhurst on multizeta values with connections to knots and quantum field theory.

It is also combinatorial in nature, being the number of certain necklaces. For lack of space, we do not elaborate on this connection here, but mention only that aperiodic binary necklaces of length n are in a natural bijective correspondence with irreducible polynomials of degree n over $\mathbb{F}_2$. It is highly suggestive that that there is an $\mathbb{F}_p$- Lie algebra operating in the background in the theory of multizeta values, namely the free Lie algebra with one generator in degree 1 and one in degree 2; its graded pieces have the same dimensions as the observed dimensions for the NT-groups of type $(4, 4)$, namely (5). Another candidate is the permutation group algebra of Cameron, see Gilbey [**G**].

3.5. A surprising outcome of Boston's experiment is a purely group-theoretical program for attacking Conjecture 1.2 for base field $\mathbb{Q}$. Namely, Step 1: for a fixed type $\boldsymbol{m}$, there are only finitely many Lie algebras which occur as the $\mathbb{F}_p$-Lie algebra of NT-groups of type $\boldsymbol{m}$; and Step 2: the Lie algebra of an infinite NT-group has no analytic quotients.

For the particular case of $p = 2$ and $S = \{\infty, p_1, p_2\}$, there is a strong possibility that $G_{\mathbb{Q},S}$ is torsion-riddled, which would immediately show that it has no infinite analytic quotients. Boston conjectures, again based on strong experimental evidence, that every group of type (4) is just-infinite. See [**B2**] for more details on this and a number of other interesting questions/conjectures.

3.6. In conclusion, Boston's experiment has revealed that the group-theoretical information stemming from algebraic number theory that we have had about tame fundamental groups for the last forty years is perhaps of sufficient strength to convert most problems of interest about them (such as Fontaine-Mazur) into interesting problems purely in group theory. It also demonstrates once again how numerical experimentation combined with bold but carefully chosen assumptions can at times shed light on previously impervious number-theoretical problems and open up new avenues of research.

3.7. Note added in proof.— In their very striking recent work, Labute [**La**] and Labute-Minac [**La-Mi**] confirm some of Boston's predictions. In particular, for odd primes p, Labute gives examples of finite sets S away from p such that the cohomological dimension of $G_{\mathbb{Q},S}$ is 2! In particular, tame finitely ramified pro-p extensions of $\mathbb{Q}$ are not always torsion-riddled as previously expected.

Références

[B1] N. Boston, Some cases of the Fontaine-Mazur conjecture. II. J. Number Theory 75 (1999), no. 2, 161–169. MR1681626 (2000b:11124)

[B2] N. Boston, Reducing the Fontaine-Mazur conjecture to group theory, preprint, 10pp, 2003.

[BL] N. Boston, C. Leedham-Green, Explicit computation of Galois p-groups unramified at p. J. Algebra 256 (2002), no. 2, 402–413. MR1939112 (2003k:12004)

[Br] D. Broadhurst, On the enumeration of irreducible k-fold Euler sums and their roles in knot theory and field theory, preprint 34pp., arxiv.org: hep-th/9604128, 22 April 1996.

[CG] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields. Invent. Math. 124 (1996), no. 1-3, 129–174. MR1369413 (97b:11079)

[F] J.-M. Fontaine, Représentations ℓ-adiques potentiellement semi-stables. (French) [Potentially semistable ℓ-adic representations] Priodes p-adiques (Bures-sur-Yvette, 1988). Astrisque No. 223, (1994), 321–347. MR1293977 (95k:14031)

[FM] J.-M. Fontaine and B. Mazur, Geometric Galois representations. Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 41–78, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995. MR1363495 (96h:11049)

[Fr] A. Fröhlich, Central extensions, Galois groups, and ideal class groups of number fields. Contemporary Mathematics, 24. American Mathematical Society, Providence, RI, 1983. MR0720859 (85c:11101)

[G] J. D. Gilbey, Permutation group algebras, J. Alg. Combinatorics, 19 (2004), 25–45

[GS] E.S. Golod and I.R. Shafarevich,. On the class field tower. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 28 1964 261–272. English translation in: I.R. Shafarevich, Collected mathematical papers. Springer-Verlag, Berlin, 1989. MR0161852 (28 #5056)

[H1] F. Hajir, On the growth of p-class groups in p-class field towers. J. Algebra 188 (1997), no. 1, 256–271. MR1432356 (98a:11151)

[HM1] F. Hajir and C. Maire, Asymptotically good towers of global fields. European Congress of Mathematics, Vol. II (Barcelona, 2000), 207–218, Progr. Math., 202, Birkhuser, Basel, 2001. MR1905361 (2003g:11127)

[HM2] F. Hajir and C. Maire, Extensions of number fields with wild ramification of bounded depth. Int. Math. Res. Not. 2002, no. 13, 667–696. MR1890847 (2002m:11096)

[KR] C. Khare and C. S. Rajan The density of ramified primes in semisimple p-adic Galois representations. Internat. Math. Res. Notices 2001, no. 12, 601–607. MR1836789 (2002e:11066

[K1] C. Khare, Limits of residually irreducible p-adic Galois representations. Proc. Amer. Math. Soc. 131 (2003), no. 7, 1999–2006. MR1963742 (2003m:11190)

[KLR] C. Khare, M. Larsen, R. Ramakrishna, Constructing semi-simple p-adic Galois representations with prescribed properties, preprint, 32 pp., `arxiv:math.NT03093283 v1, 17 Sep 2003`

[KR] C. Khare and R. Ramakrishna, Finiteness of Selmer groups and deformation rings. Invent. Math. 154 (2003), no. 1, 179–198. MR2004459 (2004g:11042)

[KW] M. Kisin and S. Wortmann, A note on Artin motives. Math. Res. Lett. 10 (2003), no. 2-3, 375–389. MR1981910 (2004d:14018)

[Ki] M. Kisin, Overconvergent modular forms and the Fontaine-Mazur conjecture. Invent. Math. 153 (2003), no. 2, 373–454. MR1992017 (2004f:11053)

[Ko] H. Koch, Galois theory of p-extensions. With a foreword by I. R. Shafarevich. Translated from the 1970 German original by Franz Lemmermeyer. With a postscript by the author and Lemmermeyer. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. MR1930372 (2003f:11181)

[Ku] T. Kuhnt, Generalizations of Golod-Shafarevich and applications, PhD dissertation, UIUC, 2002.

[La] J. Labute, Mild pro-p groups and Galois groups of p-extensions of $\mathbb{Q}$, preprint, 25 pp., 2005.

[La-Mi] J. Labute and J. Minac, Mild pro-2 groups and 2-extensions of $\mathbb{Q}$ with restricted ramification, work in progress.

[R1] R. Ramakrishna, Deforming an even representation. Invent. Math. 132 (1998), no. 3, 563–580. MR1625720 (99h:11128

[R2] R. Ramakrishna, Lifting Galois representations. Invent. Math. 138 (1999), no. 3, 537–562. MR1719819 (2000j:11167)

[R3] R. Ramakrishna, Infinitely ramified Galois representations. Ann. of Math. (2) 151 (2000), no. 2, 793–815. MR1765710 (2001e:11057)

[S] S. Sen, Ramification in p-adic Lie extensions. Invent. Math. 17 (1972), 44–50. MR0319949 (47 #8490)

[Sl] N. Sloane, The On-Line Encyclopedia of Integer Sequences, `http://www.research.att.com/~njas/sequences/index.html`

[ST] J-P. Serre and J. Tate, Good reduction of abelian varieties. Ann. of Math. (2) 88 1968 492–517. MR0236190 (38 #4488)

[Sh] I. R. Shafarevich, Extensions with given ramification points (Russian), Publ. Math. IHES **18**, 295-319 (1964), English translation in: Collected mathematical papers. Springer-Verlag, Berlin, 1989. MR0977275 (89m:01142)

[T] R. Taylor, Remarks on a conjecture of Fontaine and Mazur. J. Inst. Math. Jussieu 1 (2002), no. 1, 125–143. MR1954941 (2004c:11082)

[Ts] T. Tsuji, p-adic Hodge theory in the semi-stable reduction case. Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998). Doc. Math. 1998, Extra Vol. II, 207–216. MR1648071 (99g:14020)

[W] K. Wingberg, On the Fontaine-Mazur conjecture for CM-fields. Compositio Math. 131 (2002), no. 3, 341–354. (2003i:11165)

Farshid Hajir, Department of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003-9318 USA • *E-mail :* hajir@math.umass.edu