Séminaires & Congrès
11, 2005, p. 111–124

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

by

Farshid Hajir

Abstract. — In this paper, we examine some recent results concerning Galois groups of tamely ramified pro-p extensions of numbers fields.

Résumé **(Groupes de Galois pro-p modérés : un survol des travaux récents).** — Dans cet article, on examine quelques résultats récents au sujet des groupes de Galois des extensions pro-p modérées des corps des nombres.

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.

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

2000 ***Mathematics Subject Classification.*** — 11R37.
Key words and phrases. — 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.

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 key 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 [**KRm**], 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 $n = 2$, $p \geqslant 7$. 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* $p \geqslant 7$. *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