A remark on a finiteness conjecture on mod p Galois representations by C. Khare

by

Gebhard Böckle

Department of Mathematics, ETH Zürich, HG G 66.4, Rämistrasse 101

8092 Zürich, Switzerland, email: boeckle@math.ethz.ch

November 29 2000

Abstract

The following conjecture on finiteness of mod p Galois representations was formulated by C. Khare in a recent article: Let $\mathbb{F}$ denote the algebraic closure of a finite field. Then for each number field K, each integer n, and each ideal $\mathfrak{n}$ of the ring of integers of K there are only finitely many isomorphism classes of continuous semisimple n-dimensional representations of the absolute Galois group G_K of K over $\bar{\mathbb{F}}_p$ whose prime to-p conductor is bounded by $\mathfrak{n}$. We show, as was conjectured by Khare, that the above is implied by the seemingly weaker conjecture where the prime-to-p conductor is assumed to be trivial, provided one considers all number fields simultaneously.

1 Introduction

We fix some notation: Let p be a prime and $\mathbb{F}$ the algebraic closure of the field of p elements equipped with the discrete topology. For a number field K, let S_0 be the set of places of K above p together with all infinite places, and S any finite set of places of K containing S_0. By $G_{K,S}$ we denote the Galois group of the maximal algebraic extension of K which is unramified outside S and we regard $G_{K,S}$ as a topological group with respect to its profinite topology. For any field F, we denote by G_F its absolute Galois group. For a place v of K, let K_v be the completion of K at v. Via an extension of v to the algebraic closure $\bar{K}$ of K, we fix an embedding from $\bar{K}$ to $\bar{K}_v$, and thus obtain a decomposition group at v as the image of the corresponding map $G_{K_v} \to G_K \to G_{K,S}$.

In [2], Conj. 2.2, essentially the following conjecture is stated (cf. loc. cit., Rem. 2 after Prop. 2.5):

Conjecture 1 There are only finitely many isomorphism classes of continuous semisimple representations $\rho\colon G_{K,S} \to \mathrm{GL}_n(\mathbb{F})$, such that the prime-to-p Artin conductor of ρ is bounded.

In Remark 2 following [2], Conj. 2.2, the following weaker conjecture is formulated and the question is raised whether, in a suitable sense, it is indeed equivalent to the above conjecture:

Conjecture 2 There are only finitely many isomorphism classes of continuous semisimple irreducible representations $\rho\colon G_{K,S_0} \to \mathrm{GL}_n(\mathbb{F})$.

Here we will prove the following result, which answers the above question in the affirmative.

Theorem 3 *Fix a positive integer n_0. If Conjecture 2 holds for all number fields and all positive $n \le n_0$, then Conjecture 1 holds for all number fields and all positive $n \le n_0$.*

The idea of the proof is to use the bound on the Artin conductor for a finite place $v \in S - S_0$ to show that there exists a finite extension L_v of K_v inside $\bar{K}_v$, which only depends on the conductor at v and on n_0 but not on ρ, such that the restriction of ρ to G_{L_v} is unramified. This will be carried out in Section 2. Once this is known, we can construct a finite extension E of K, independently of ρ, such that ρ restricted to G_E is unramified outside S_0. As will be shown in Section 3, the theorem will follows rapidly.

Remark 4 The above theorem should be thought of as a theoretical result. In practise, in order to establish cases of Conjecture 1, it seems easier to work over smaller fields. For example, assuming Serre's conjecture, in the case $n = 2$, $K = \mathbb{Q}$ and ρ odd, Conjecture 1 was shown to hold in [2]. If one follows the proof of Theorem 3, then one could also prove this by proving Conjecture 2 for $n = 2$ over arbitrary number fields, which seems to us a much more ambitious project.

2 Local analysis

Throughout this section, we fix a local field F of residue characteristic different from p and a continuous Galois representation $\rho\colon G_F \to \mathrm{GL}_n(\mathbb{F})$. Note that F may have positive characteristic! By $I = I_F$ the inertia subgroup of G_F is denoted and by $I^w = I_F^w$ the wild inertia subgroup of I. We use π to denote a uniformizer of F and $\mathfrak{p}$ as its maximal ideal.

Let $\mathfrak{p}^f = \mathfrak{p}^{f(\rho,F)}$ denote the conductor of ρ (as a representation of G_F). Recall that the f was defined as follows: Let F' denote the splitting field of ρ, which is finite because $\mathbb{F}$ is discrete, G_F compact and ρ continuous. Let V denote the representation module underlying ρ. Define $G := \mathrm{Gal}(F'/F)$ and denote by G_i the i-th higher ramification group. Then

$$f = \sum_{i \ge 0} \frac{1}{[G_0 : G_i]} \mathrm{codim}(V^{G_i}).$$

Proposition 5 *Fix positive integers f_0 and n_0. Then there exists a finite field extension L of F such that for any $\rho\colon G_F \to \mathrm{GL}_n(\mathbb{F})$ as above with conductor $\mathfrak{p}^f \supset \mathfrak{p}^{f_0}$ and $n \le n_0$, the restriction of ρ to G_L is unramified.*

We will prove this in various stages.

Lemma 6 *Under the hypothesis of the above proposition, there exists a finite Galois extension F_1 of F depending only on n_0 such that for all ρ as in the proposition, the order of $\rho(G_{F_1})$ is prime to p.*

Proof: Denote by H the image of ρ and by $H^{(p)}$ a p-Sylow subgroup. Note that $H^w := \rho(I^w)$ is a normal subgroup of H of order prime to p, as the residue characteristic of F is different from p. Hence H^w and $H^{(p)}$ have trivial intersection and therefore $H^{(p)} \cong H^{(p)}H^w/H^w \subset H/H^w$ is a quotient of the pro-p Sylow subgroup of G_F/I^w, which is isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_p$. Thus there exists $s, t \in H^{(p)}$, which are possibly trivial, such that $H^{(p)} = \{s^i t^j : 0 \leq i < p^l, 0 \leq j \leq p^m\}$ for suitable l, m.

An element of $\mathrm{GL}_n(\mathbb{F})$ of p-power order has order dividing p^c where $c := [\log_p n] + 1$, as can be seen by considering its Jordan canonical form. Applying this observation to s, t, yields that $H^{(p)}$ has order at most p^{2c}. Let π be a uniformizer of F and let F' be the unique unramified extension of F of order p^c. Then we may choose $F_1 := F'(\zeta_{p^c}, \pi^{1/p^c})$ for the lemma to hold. ∎

Lemma 7 *Under the hypothesis of Proposition 5, there exists a finite Galois extension F_2 of F depending only on n_0 such that for all ρ as in the proposition, the group $\rho(G_{F_2})$ is abelian.*

Proof: With F_1 from the previous lemma, it follows that the order of $\rho(G_{F_1})$ is prime to p. By a profinite version of the Lemma of Schur-Zassenhaus, the restriction $\rho_{|G_{F_1}}$ admits a lift to a continuous representation $\rho' \colon G_{F_1} \to \mathrm{GL}_n(C)$ for some finite extension C of $\mathbb{Q}_p$ such that the orders of $\rho(G_{F_1})$ and of $\rho'(G_{F_1})$ agree. Via an embedding of C into the complex numbers, $\rho(G_{F_1})$ admits a complex representation of dimension at most n_0.

By Jordan's theorem, there exists a constant r, which only depends on n_0 such that $\rho(G_{F_1})$ posseses a normal abelian subgroup of index at most r (cf. [1]). As is well known, there exists a finite extension F_2' of F_1 which contains the fixed field of any open subgroup of G_{F_1} of index at most r. Choosing F_2 to be the Galois closure of F_2' over F, the lemma follows. ∎

Proof of Proposition 5: Let $\rho \colon G_F \to \mathrm{GL}_n(\mathbb{F})$ be a representation of G_F of conductor $f \leq f_0$ and assume that $n \leq n_0$. Then the restriction of ρ to G_{F_2}, with F_2 from the previous lemma, is abelian. Let F' be the splitting field of F. As the i-th higher ramification group of $\mathrm{Gal}(F'/F_2)$ is contained in that of $\mathrm{Gal}(F'/F)$, it follows immediately that the conductor of $\rho_{|G_{F_2}}$ contains $\mathfrak{P}^{f_0}$, where $\mathfrak{P}$ is the maximal ideal of the ring of integers of F_2. By local class field theory, there exists a finite extension L of F_2, which depends only on f_0 and F_2, such that L/F is Galois and $\rho_{|G_L}$ is unramified. ∎

3 The proof of main result

With the technical proposition from the previous section, we can immediately proceed to the proof of our main result.

Proof of Theorem 3: Fix a positive integer n_0, bounding the dimension of ρ, and an ideal $\mathfrak{n}$ of the ring of integers $\mathcal{O}$ of K, dividing the prime-to-p conducter of ρ. Recall that the prime-to-p conductor of ρ is defined as the product

$$\prod_{v\in S-S_0} \mathfrak{p}_v^{f(K_v,\rho_{|G_{K_v}})},$$

where $\mathfrak{p}_v$ is the prime ideal in $\mathcal{O}$ corresponding to the place v.

Using Proposition 5, we choose for each $v \in S - S_0$ a finite extension L_v of K_v such that ρ restricted to G_{L_v} is unramified. Note that the fields L_v only depend on n_0 and on the order of $\mathfrak{n}$ at v. Any finite extension of K_v can be obtained via completion of a finite Galois extension of K. Thus we can choose a finite Galois extension L of K, depending only on n_0 and $\mathfrak{n}$, such that the restriction of ρ to G_L is unramified at all place not above p or ∞.

Let ρ' be the semisimplification of $\rho_{|G_L}$. As we assume Conjecture 2 to hold, ρ' belongs to a finite set of representations. Hence there exists a finite extension L' of L, independently of ρ, such that $\rho(G_{L'}) \subset \mathrm{GL}_n(\mathbb{F})$ is a p-group and such that $\rho_{|G_{L'}}$ is unramified outside the places above p and ∞. As the pro-p completion of G_{L',S_0} is topologically finitely generated, and as the unipotent radical of $\mathrm{GL}_{n_0}(\mathbb{F})$ has nilpotency degree at most $[\log_p n_0] + 1$, there exists a finite extension L'' of L', Galois over K, such that ρ restricted to L'' is trivial. The choice of L'' depends only on L' and on n_0, and hence only on $\mathfrak{n}$ and n_0. This shows that any ρ as above is an irreducible representation of the finite group $\mathrm{Gal}(L''/K)$ of dimension at most n_0. Hence the set of all such ρ is finite. ∎

References

[1] G. Anderson, D. Blasius, R. Coleman, G. Zettler, *On representations of the Weil group with bounded conductor*, Forum Math. **6**, no. 5, (1994), 537–545.

[2] C. Khare, *Conjectures on Finiteness of mod p Galois representations*, J. Ramanujan Math. Soc. **15** No. 1 (2000), 23–42.