ON MOD 3 GALOIS REPRESENTATIONS WITH CONDUCTOR 4

HYUNSUK MOON

(Communicated by Ken Ono)

Abstract. The non-existence is proved of 2-dimensional mod 3 irreducible representations of \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) of Artin conductor dividing 4.

Let \( G_\mathbb{Q} \) be the absolute Galois group \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) of \( \mathbb{Q} \). For any prime number \( \ell \), let \( \overline{\mathbb{F}}_\ell \) denote an algebraic closure of the finite field \( \mathbb{F}_\ell \) of \( \ell \) elements. In this paper, we prove the non-existence of certain mod 3 Galois representations:

**Theorem 1.** There exist no irreducible representations \( \rho : G_\mathbb{Q} \to \text{GL}_2(\mathbb{F}_3) \) with \( N(\rho) \) dividing 4.

Here, \( N(\rho) = \prod_{p \nmid 3} p^{n_p(\rho)} \) is the Artin conductor of \( \rho \) outside 3 ([7], §1.2; the definition of the exponent \( n_p(\rho) \) will be recalled below). This proves a special case of Serre’s conjecture ([7]). Indeed, the conjecture predicts that if such a representation is odd, then up to twist by a power of the mod 3 cyclotomic character, it comes from a cuspidal eigenform of level 4 and weight \( \leq 4 \), but there are no such forms.

Khare ([3]) proved the level 1 case of Serre’s conjecture by induction on the primes. Our result may serve as a first step of such an inductive proof of the level 4 case of Serre’s conjecture if Khare’s proof can be extended to this case.

Serre’s conjecture is known to be true if \( \rho \) is odd and its image \( \text{Im}(\rho) \) of \( \rho \) is solvable ([5], Thm. 4). So, it remains for us to prove the theorem in the following two cases: (i) \( \text{Im}(\rho) \) is non-solvable, (ii) \( \rho \) is even and \( \text{Im}(\rho) \) is solvable.

Our strategy in case (i) is basically the same as in [10]; that is to deduce a contradiction by comparing two kinds of inequalities of the opposite direction for the discriminant of the field corresponding to the kernel of \( \rho \) — one from above (the refined Tate bound ([5], Thm. 3) and the other from below (the Odlyzko bound [6]). A new ingredient in this paper is the estimate of the prime-to-3 part of the discriminant (Lemma 4). The case (ii) is settled by class field theory with the help of known results ([9]) on solvable subgroup of \( \text{GL}_2(\mathbb{F}_\ell) \) and Jones’ table ([2]) of number fields.

In Section 1, we analyze the ramification of \( \rho \) at 2. The proof of the theorem is given in Section 2.

Received by the editors March 2, 2006 and, in revised form, July 24, 2006.

2000 Mathematics Subject Classification. Primary 11F80, 11S15.

*Note added in proof: Serre’s conjecture has recently been proved completely by Khare and Wintenberger independently of our work.
1. Ramification at 2

Let $D_p (\subset G_0)$ be the decomposition subgroup for a choice of an extension of the prime ideal $(p)$ to $\overline{\mathbb{Q}}$, and $I_p$ its inertia subgroup. For a continuous representation $\rho : D_p \to \text{GL}(V)$, where $V$ is a finite-dimensional $\overline{\mathbb{F}}_\ell$-vector space with $\ell \neq p$, we define the exponent of Artin conductor of $\rho$ by

$$\nu_p(\rho) := \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim_{\overline{\mathbb{F}}_\ell}(V/V^{G_i}).$$

Here, $G_i$ is the $i$th ramification subgroup of $G := \text{Im}(\rho)$.

**Lemma 2.** Let $p$ and $\ell$ be two distinct prime numbers, and let $\rho : D_p \to \text{GL}_2(\overline{\mathbb{F}}_\ell)$ be a continuous representation with $\nu_p(\rho) = 2$. If $\rho$ is wildly ramified at $p$, then it is a direct sum of two characters, one of which is unramified and the other has exponent of Artin conductor 2. In particular, if $\rho$ is irreducible, then it is tamely ramified at $p$.

**Remark.** This lemma holds true if $D_p$ is the absolute Galois group of any complete discrete valuation field with finite residue field of characteristic $p$.

**Proof.** Suppose $\rho$ is wildly ramified at $p$, so that $\dim(V^{G_1}) < 2$. By assumption, we have

$$(*) \quad \nu_p(\rho) = \dim(V/V^{G_0}) + \frac{1}{(G_0 : G_1)} \dim(V/V^{G_1}) + \cdots = 2.$$

This implies that $\dim(V^{G_0}) = 1$. Then $V$ is reducible as a representation of $D_p$, because $G_0$ is normal in $G$ and hence $G$ stabilizes $V^{G_0}$. We may assume that $\rho$ is of the form

$$\rho = \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

where $\phi_i : D_p \to \overline{\mathbb{F}}_\ell^\times$ are characters of $D_p$ and $\phi_1$ is unramified. Let $\rho^{ss} = \begin{pmatrix} \phi_1 & 0 \\ 0 & \phi_2 \end{pmatrix}$ be the semisimplification of $\rho$ and put $G^{ss} := \text{Im}(\rho^{ss})$. Then $G$ sits in a short exact sequence

$$1 \to H \to G \to G^{ss} \to 1,$$

where $H = G \cap \{ (1, *) \}$ is the kernel of the natural homomorphism $G \to G^{ss}$. Note that $G^{ss}$ is abelian of order prime to $\ell$, and $H$ is an elementary abelian $\ell$-group of rank at most 2. Let $H_0 := H \cap G_0$. If $H_0 \neq 1$, then it is mapped by the projection $G_0 \to G_0/G_1$ to the unique $\ell$-Sylow subgroup of the tame inertia group $G_0/G_1$. Let $G_0^p$ be the inverse image in $G_0$ of the maximal prime-to-$\ell$ subgroup of the cyclic group $G_0/G_1$. Then $H_0$ and $G_0^p$ are both normal in $G_0$, $H_0 G_0^p = G_0$, and $H_0 \cap G_0^p = 1$. Hence we have $G_0 = H_0 \times G_0^p$. But this is impossible, because any two non-trivial elements of the form $(1, *)$, one of order $\ell$ and the other of order prime to $\ell$, do not commute. (Note that $G_0^p \neq 1$, as $G_1 \neq 1$.) Hence $H_0 = 1$ and $G_0$ has order prime to $\ell$. Next we argue in the same way with $G/G_0$ in place of $G_0/G_1$. If $H \neq 1$, then it is mapped by the projection $G \to G/G_0$ to the unique $\ell$-Sylow subgroup of $G/G_0$. Let $G^p$ be the inverse image in $G$ of the maximal prime-to-$\ell$ subgroup of the cyclic group $G/G_0$. Then $H$ and $G^p$ are both normal in $G$, $H G^p = G$, and $H \cap G^p = 1$. Hence $G = H \times G^p$. But this is again impossible by the same reason as above. Hence $H = 1$ and $G = G^{ss}$ is semisimple. $\square$
The next lemma in group theory is proved in §§19–21 of [9], and it is used in the proof of Lemma 4 and in Section 2.

**Lemma 3.** Let $G$ be an irreducible solvable subgroup of $\text{GL}_2(\mathbb{F}_\ell)$ and $\overline{G}$ the image of $G$ in $\text{PGL}_2(\mathbb{F}_\ell)$. Then $G$ is either of the following two types.

(a) Imprimitive case: $G$ is isomorphic to a subgroup of the wreath product $\mathbb{F}_\ell^\times \wr (\mathbb{Z}/2\mathbb{Z})$.

(b) Primitive case: $\overline{G}$ sits in an exact sequence

$$1 \to \overline{A} \to \overline{G} \to \overline{\Pi} \to 1,$$

where $\overline{A}$ is isomorphic to a subgroup of $(\mathbb{Z}/2\mathbb{Z})^{\#2}$ and the conjugate action of $\overline{\Pi}$ on $\overline{A}$ is faithful, so that $\overline{\Pi}$ is identified with a subgroup of $\text{Aut}(\overline{A})$. In particular, $\overline{G}$ is either a 2-group or isomorphic to the symmetric group $S_4$ or the alternating group $A_4$.

In the special case $p = 2$ and $\ell = 3$, Lemma 2 can be strengthened as follows.

**Lemma 4.** Let $\rho : D_2 \to \text{GL}_2(\mathbb{F}_3)$ be a continuous representation with $n_2(\rho) = 2$. Then it is a direct sum of two characters, one of which is unramified and the other has exponent of Artin conductor 2. If $G_i$ denotes the $i$th ramification subgroup of $G := \text{Im}(\rho)$, then one has $G_0 = G_1 \simeq \mathbb{Z}/2\mathbb{Z}$ and $G_2 = 1$. The different of the extension $K/Q_{22}$ corresponding to $\text{Ker}(\rho)$ is (2).

**Remark.** This lemma holds true if $D_2$ is the absolute Galois group of any complete discrete valuation field with residue field $\mathbb{F}_2$.

**Proof.** We first show that $\rho$ cannot be irreducible. Suppose $\rho$ is irreducible. Then by Lemma 2 it is tamely ramified. In particular, $G$ is meta-abelian. By Lemma 3, $G$ is an extension of an elementary abelian 2-group $\overline{G}$ of rank at most 2 by an abelian group $H$ of order prime to 3. Since $\rho$ is tamely ramified, the extension $F/Q_{22}$ corresponding to $\overline{G}$ is unramified and $\overline{G} \simeq \mathbb{Z}/2\mathbb{Z}$. Now $H$ is the Galois group of a tamely ramified abelian extension of $F$. Since the residue field of $F$ is $\mathbb{F}_4$, the inertia subgroup $H_0$ of $H$ is a quotient of $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$. Since $H$ has order prime to 3, we must have $H_0 = 1$. This contradicts the assumption that $n_2(\rho) = 2$.

Thus $\rho$ is reducible, and we may assume that $\rho$ is of the form

$$\rho = \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix},$$

where $\psi_1 : D_2 \to \mathbb{F}_3^\times$ are characters of $D_2$. They factor through the abelianization $D_2^{ab}$ of $D_2$. Since the inertia subgroup of $D_2^{ab}$ is isomorphic to the pro-2 group $\mathbb{Z}_2^\times$, these characters are either unramified or wildly ramified. Since $n_2(\rho) = 2$, the only possible case is that $\psi_1$ is unramified and $\psi_2$ is wildly ramified (if $* = 0$, then the role of $\psi_1$ and $\psi_2$ may be exchanged). By Lemma 2 we have $* = 0$ and $\rho \simeq \psi_1 \otimes \psi_2$. Then since $n_2(\rho) = n_2(\psi_2) = 2$, it follows that $G_0 = G_1 \simeq \mathbb{Z}_2^\times/(1 + 2\mathbb{Z}_2^\times) \simeq \mathbb{Z}/2\mathbb{Z}$ and $G_2 = 1$. The statement on the different follows by the Führerdiskriminantenproduktformel [8] Ch. VI. §3, Cor. 2 to Prop. 6]

2. **Proof of the theorem**

Now we can prove the theorem. Suppose there were a $\rho$ as in the theorem. Since the case $N(\rho)|2$ was done in [4], we may assume $N(\rho) = 4$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(i) Assume $G := \text{Im}(\rho)$ is non-solvable. Let $K$ be the field corresponding to the kernel of $\rho$. Let $n := [K : \mathbb{Q}]$, and $|d_K|^{1/n}$ denote the root discriminant of $K$. By Theorem 3 in [251–253 of [1]], the 3-part of $|d_K|^{1/n}$ is bounded by $3^{2^{\frac{1}{n}} - \frac{1}{m}}$, where $m$ is the wild ramification index of $K/\mathbb{Q}$ at 3. By Lemma 4, the 2-part of $|d_K|^{1/n}$ is 2. All together, we have

$$|d_K|^{1/n} \leq 3^{2^{\frac{1}{n}} - \frac{1}{m}} \cdot 2$$

If $3^\mu$ is the exact power of 3 dividing the order of $G$, then by §251–253 of [1], the projective image $\overline{G}$ of $G$ in $\text{PGL}_2(\mathbb{F}_3)$ is isomorphic to either $\text{PGL}_2(\mathbb{F}_3\nu)$ or $\text{PSL}_2(\mathbb{F}_3\nu)$. Thus we have $n = |G| \geq |\text{PSL}_2(\mathbb{F}_3\nu)|$. Note that we have $\mu \geq 2$ because $\overline{G}$ is solvable if $\mu = 1$. By [4], we have

$$|d_K|^{1/n} > \begin{cases} 19.567 & \text{if } n \geq 360 = |\text{PGL}_2(\mathbb{F}_3\nu)|, \\ 22.021 & \text{if } n \geq 9828 = |\text{PSL}_2(\mathbb{F}_3\nu)|. \end{cases}$$

Comparing these two sets of inequalities, we obtain contradictions.

(ii) Assume $\rho$ is even and $G = \text{Im}(\rho)$ is solvable. Note that, since $\rho$ is even, it maps the complex conjugation to $\pm(1 \ 1)$, so that the field $K$ cut out by $\rho$ is totally real or CM. We shall show that there exists no such extension $K/\mathbb{Q}$.

If either $G$ is of type (a) in Lemma 3 or $G$ is of type (b) in Lemma 3 and $\overline{G}$ is a 2-group, then $K$ contains a non-trivial abelian extension of degree prime to 3 over a real quadratic field $F$. Since $K$ is unramified outside $\{2, 3\}$ and its conductor (or, exactly speaking, the conductor of $\rho$) at 2 is $2^2$, $F$ is the field $\mathbb{Q}(\sqrt{3})$. Then $K/F$ is unramified at 2 since $K/\mathbb{Q}$ has ramification index 2 at the prime 2 (Lemma 4). Since any ray class group of $F$ of 3-power conductor has 3-power order, there are no non-trivial abelian extensions of $F$ which are unramified outside 3 and of degree prime to 3.

Suppose now that $G$ is of type (b) in Lemma 3 and $\overline{G}$ is isomorphic to $S_4$ or $A_4$. According to [2], there are three $S_4$-extensions (resp. one $A_4$-extension) of $\mathbb{Q}$ which are unramified outside $\{2, 3\}$ and whose ramification index at 2 divides 2. However, each of these fields has 2-component of the root discriminant greater than 2, which contradicts Lemma 4.

References


DEPARTMENT OF MATHEMATICS, COLLEGE OF NATURAL SCIENCES, KYUNGPOOK NATIONAL UNIVERSITY, DAEGU 702-701, KOREA

E-mail address: hsmoon@knu.ac.kr