Bull. Korean Math. Soc. **44** (2007), No. 1, pp. 173–176

ON FOUR-DIMENSIONAL MOD 2 GALOIS REPRESENTATIONS AND A CONJECTURE OF ASH ET AL.

HYUNSUK MOON

ABSTRACT. The non-existence is proved of four-dimensional mod 2 semi-simple representations of Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ which are unramified outside 2.

1. Introduction

Let $G_{\mathbb{Q}}$ be the absolute Galois group Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ of the rational number field $\mathbb{Q}$ and $\overline{\mathbb{F}}_p$ an algebraic closure of the finite prime field $\mathbb{F}_p$ of p elements. In this paper, we prove the following:

Theorem. *There exist no semisimple Galois representations*

$$\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_4(\overline{\mathbb{F}}_2)$$

which are unramified outside 2 *and such that the field* $K/\mathbb{Q}$ *corresponding to the kernel of* ρ *is totally real.*

The Theorem settles a special case of a conjecture of Ash-Sinnott ([2]) and of Ash-Doud-Pollack ([1]), in the same way as Tate's non-existence theorem in the two-dimensional case ([9]) settled a special case of Serre's conjecture ([8]). Let us recall the conjecture: Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ be a continuous semisimple representation. They assume that the image of a complex conjugation by ρ satisfies the parity condition that it is conjugate to $\pm\mathrm{diag}(1,-1,1,-1,\ldots)$; thus in characteristic 2 it is the identity matrix. Then they conjecture that ρ comes from a cohomology eigenclass in the cohomology group $H^*(\Gamma_0(N), V(\varepsilon))$ of the congruence subgroup $\Gamma_0(N)$ of $\mathrm{SL}_n(\mathbb{Z})$ with coefficient module $V(\varepsilon)$, which is a finite-dimensional $\overline{\mathbb{F}}_p$-vector space constructed from certain data derived from ρ. Here N is the Artin conductor of ρ outside p and $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ is the Nebentype character associated with ρ. This is a higher dimensional generalization of Serre's conjecture ([8]). We look at the case $p = 2$, $n = 3, 4$, and $N = 1$. Note that, if $p = 2$, the parity condition means that the field corresponding to Ker (ρ) is totally real (i.e., ρ is unramified at the infinite

Received July 26, 2006.
2000 *Mathematics Subject Classification.* 11R32, 11S15.
Key words and phrases. mod p Galois representation, Ash's conjecture, Odlyzko's bound.
This research was supported by Kyungpook National University Research Fund, 2006.

place). Our theorem states that a ρ as in the conjecture does not exist so that the conjecture is true.

Khare ([5]) proved the $N = 1$ case of Serre's conjecture. In his proof, Tate's result ([9] for $p = 2$) and some others ([8] for $p = 3$, [3] for $p = 5$) were used as the first step of a kind of induction on the prime p. Thus our result is expected to play the same role as Tate's in the four-dimensional case.

In [6], the author proved the finiteness of the set of isomorphism classes of semisimple representations as in the above Theorem. In the present paper, we prove that the set is in fact empty, employing basically the same method but with the help of Odlyzko's precise table of discriminant bounds and some group theory as new ingredients.

2. Proof of the Theorem

The non-existence of four-dimensional semisimple representations is reduced to the non-existence of irreducible representations of dimension less than or equal to 4. By the result of Tate ([9]), it is sufficient to show that there are no irreducible three- and four-dimensional representations. So in the following, let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{\mathbb{F}}_2)$ be a three- or four-dimensional irreducible representation unramified outside 2.

The key to the proof is the comparison of two kinds of inequalities of the opposite direction for the discriminant of the field corresponding the $\mathrm{Ker}(\rho)$. We estimate the discriminant from above in terms of the invariant "p-length" of the Galois group $\mathrm{Im}(\rho)$. Let us recall the definition ([6]):

Definition. Let G be a finite group and l a positive integer. We say that G has *p-length* $\leq l$ if there exists a sequence of subgroups

$$S = S^{(1)} \supset S^{(2)} \supset \cdots \supset S^{(l)} \supset S^{(l+1)} = \{1\}$$

such that

S is a p-Sylow subgroup of G,

$S^{(i+1)}$ is normal in $S^{(i)}$ and

$S^{(i)}/S^{(i+1)}$ is an elementary p-group for all $1 \leq i \leq l$.

Then we obtained the following estimation:

Proposition. *Let $K/\mathbb{Q}$ be a finite Galois extension of degree n with Galois group G. Suppose G has p-length $\leq l$. Then the p-part of the discriminant d_K of $K/\mathbb{Q}$ divides p^{cn} where c is the largest integer smaller than*

$$l + 1 + \frac{l}{p-1}.$$

Since the p-Sylow subgroup of a finite subgroup of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ is conjugate to a subgroup of the group of all upper triangular matrices with 1 on the diagonal, we remark the p-length of $\mathrm{GL}_n(\overline{\mathbb{F}}_p)$ is less than or equal to $\lceil \log_2 n \rceil$, where $\lceil \alpha \rceil$

denotes the integer satisfying $\alpha \leq \lceil \alpha \rceil \leq \alpha + 1$ (cf. [6], §3). Since $n = 3, 4$ now, our $G = \mathrm{Im}(\rho)$ has 2-length ≤ 2.

In the other direction, we use the lower bound for discriminants by Odlyzko ([7]). In particular, for totally real fields K with $n = [K : \mathbb{Q}]$, we have

$$\begin{aligned} |d_K|^{1/n} &> 2.222 \qquad \text{if } n \geq 2, \\ |d_K|^{1/n} &> 9.279 \qquad \text{if } n \geq 7, \\ |d_K|^{1/n} &> 32.209 \qquad \text{if } n \geq 44. \end{aligned}$$

Now we prove the non-existence of ρ. Let K be the corresponding field to $\mathrm{Ker}\,(\rho)$. Let $n = [K : \mathbb{Q}]$ and $G := \mathrm{Im}(\rho)$. By the remark after the Proposition, G has 2-length ≤ 2. If G has 2-length 0, then K is tamely ramified at 2 so that the discriminant d_K satisfies

$$|d_K|^{1/n} < 2.$$

Comparing with the Odlyzko bound, we have a contradiction if $n \geq 2$. If G has 2-length 1, then the Proposition says that d_K satisfies

$$|d_K|^{1/n} < 2^3 = 8.$$

Comparing with the Odlyzko bound, we have a contradiction if $n \geq 7$. Since the only non-abelian group S_3 of order < 7 has irreducible representations only of dimension 1 and 2, such a ρ does not exist. If G has 2-length 2, we have

$$|d_K|^{1/n} < 2^5 = 32.$$

Comparing with the Odlyzko bound, we have a contradiction if $n \geq 44$. Since the 2-Sylow group of G is non-abelian, the 2-part of the order of G is greater than or equal to 8. Also, G is not a 2-group because a p-group has no non-trivial irreducible representations in characteristic p. Therefore, if $n < 44$, the order of G is $8 \cdot 3$ or $8 \cdot 5$. Then the 2-Sylow subgroup has index 3 or 5, and there should be a finite extension $K/\mathbb{Q}$ of degree 3 or 5 unramified outside 2. However, there are no such extensions ([4]). Hence we obtain contradictions. □

References

[1] A. Ash, D. Doud, and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), no. 3, 521–579.

[2] A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod-p cohomology of* $\mathrm{GL}(n, \mathbb{Z})$, Duke Math. J. **105** (2000), no. 1, 1–24.

[3] S. Brueggeman, *The nonexistence of certain Galois extensions unramified outside* 5, J. Number Theory **75** (1999), no. 1, 47–52.

[4] J. Jones, *Tables of number fields with prescribed ramification*, `http://math.la.asu.edu/~jj/numberfields`, 1998.

[5] C. Khare, *Serre's modularity conjecture: the level one case*, Duke Math. J. **134** (2006), no. 3, 557–589.

[6] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), no. 1, 156–165.

[7] A. M. Odlyzko, *Discriminant bounds*, tables dated Nov. 29, 1976, unpublished, appeared in `http://www.dtc.umn/~odlyzko/unpublished/discr.bound.table2`.

[8] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.

[9] J. Tate, *The non-existence of certain Galois extensions of* Q *unramified outside* 2, Arithmetic geometry (Tempe, AZ, 1993), 153–156, Contemp. Math., 174, Amer. Math. Soc., Providence, RI, 1994.

Department of Mathematics
College of Natural Sciences
Kyungpook National University
Daegu 702-701, Korea
E-mail address: `hsmoon@knu.ac.kr`