Journal of Number Theory **75**, 47–52 (1999)
Article ID jnth.1998.2318, available online at http://www.idealibrary.com on IDEAL®

The Nonexistence of Certain Galois Extensions Unramified Outside 5

Sharon Brueggeman

Department of Mathematics, The University of Illinois, Urbana, Illinois 61801

Received October 20, 1997; revised July 10, 1998

Communicated by J. Tate

Let ρ be a two-dimensional semisimple odd representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ over a finite field of characteristic 5 which is unramified outside 5. Assuming the GRH, we show in accordance with a conjecture by Serre that $\rho = \chi_5^a \oplus \chi_5^b$, where $a+b$ is odd.

1. INTRODUCTION

Let l be prime. Let $\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(2, \overline{F_l})$ be a semisimple odd Galois representation which is unramified outside l. Serre [8] conjectured that any such representation is modular. In fact, this is a special case of the conjecture he published in 1987 [9]. He wrote of this conjecture in a letter to Tate in 1973 who replied with a proof of the conjecture when $l=2$ [12] which uses a discriminant estimate. Serre observed that improvements in lower bounds for discriminants of number fields allow Tate's proof to extend to the case $l=3$ [8]. In 1976, using asymptotic estimates, Odlyzko [4] explained why further improvements would not extend Tate's argument to prove the case $l=5$ unless the Generalized Riemann Hypothesis (GRH) is assumed. Recently Shepherd-Barron and Taylor [10] showed that if $\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(2,5)$ is unramified at 3 and has determinant the cyclotomic character then $\bar{\rho}$ is modular.

Assuming the GRH, we prove this conjecture of Serre for $l=5$. We let G be the finite group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})/\mathrm{Ker}(\bar{\rho})$ and let ρ be the corresponding faithful representation of G. First we assume that G is solvable. In this case we find one possible group, all of whose odd representations are indeed modular. Then we assume G is nonsolvable and like Tate we limit the size of the Galois group by using a discriminant estimate. Next we use the Feit–Thompson Theorem [2] and Dickson's classification [1] of linear groups to reduce to two possible Galois groups. We then bound the absolute discriminant for each of these groups. Finally Pohst's database

0022-314X/99 $30.00

[7] shows that these absolute discriminants do not occur with these Galois groups.

Our main theorem is the following:

THEOREM 1.1. *Assume the GRH. Let G be the Galois group of a finite Galois extension $K/\mathbb{Q}$ which is unramified outside 5. Let $\rho: G \hookrightarrow GL(2, \overline{F_5})$ be a faithful semisimple odd representation. Then $\rho = \chi_5^a \oplus \chi_5^b$ for $a = 0$ or 2 and $b = 1$ or 3, where χ_5 is the cyclotomic character.*

Remark. The groups $GL(2, 5^n)$ embed in $GL(2, \overline{F_5})$ in the obvious way. Since $\rho(G)$ is finite, given G we pick n so that $\rho: G \hookrightarrow GL(2, 5^n)$.

2. SOLVABLE GROUPS

Throughout this section we suppose G is solvable. First we show that the order of G is relatively prime to 5.

LEMMA 2.1. *Let G, K and ρ be as above. Then 5 does not divide $|G|$.*

Proof. Suprunenko [11] has shown, for any prime p, that a maximal irreducible solvable subgroup of $GL(2, p^n)$ has order $2(p^n-1)^2$, $2(p^{2n}-1)$ or $24(p^n-1)$. When $\rho(G)$ is an irreducible subgroup of $GL(2, 5^n)$, the lemma follows immediately by taking $p = 5$. When $\rho(G)$ is a reducible subgroup, semisimplicity implies that G is isomorphic to a diagonal matrix group. So G embeds in $F_{5^n}^* \oplus F_{5^n}^*$ which has no elements of order 5. ∎

Now let G' be the commutator subgroup of G and let F' be the corresponding subfield of K.

LEMMA 2.2. *Let G, K and ρ be as above. Then $F' = \mathbb{Q}(\zeta_5)$.*

Proof. Since $F'/\mathbb{Q}$ is an abelian extension unramified outside 5, Kronecker–Weber implies F' is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_{5^r})$ and G/G' is isomorphic to a quotient of $(\mathbb{Z}/5^r)^* \cong \mathbb{Z}/4 \times Z/5^{r-1}$. By Lemma 2.1, $r = 1$. Since $\mathrm{Det}(\rho)$ is an odd Dirichlet character of conductor 5, $\mathrm{Det}(\rho) = \chi_5$ or χ_5^3. Hence $F' = \mathbb{Q}(\zeta_5)$. ∎

Next we investigate G'/G''. We will show that this quotient is trivial. So $F' = K$. The odd representations of $G = \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ are precisely those listed in Theorem 1.1.

LEMMA 2.3. *Let G and K be as above. Then $[G': G'']$ divides 4.*

Proof. Let $\mathfrak{O}$ be the ring of integers in $F' = \mathbb{Q}(\zeta_5)$. Since 5 is totally ramified in F', there is a unique prime $\mathfrak{p}$ of $\mathfrak{O}$ lying above 5. We know that $\mathbb{Q}(\zeta_5)$ has class number one. By class field theory [3], the Galois group of the maximal abelian extension of F' with degree prime to 5 and unramified outside $\mathfrak{p}$ is a quotient of $(\mathfrak{O}/\mathfrak{p})^* \cong F_5^*$. Thus G'/G'' is cyclic of order dividing 4. ∎

LEMMA 2.4. *Let G be as above. G is abelian.*

Proof. If G is a reducible semisimple subgroup of $GL(2, 5^n)$, then G is abelian. Hence we may assume that G is irreducible. By Lemmas 2.2 and 2.3, G/G'' is a 2-group. Since there is only one quadratic extension of $\mathbb{Q}$ unramified outside 5, G/G'' has only one normal subgroup of index 2 which must therefore be its Frattini subgroup. By the Burnside Basis Theorem [6], G/G'' is cyclic. Hence $G' = 1$. ∎

This proves Theorem 1.1 in the case G is solvable. Note that this part of the proof does not depend on the GRH.

3. NONSOLVABLE GROUPS

For the rest of the paper we assume $G = \mathrm{Gal}(K/\mathbb{Q})$ is nonsolvable. Let $g = |G|$ and let d be the discriminant of $K/\mathbb{Q}$.

First suppose $K/\mathbb{Q}$ is tamely ramified at 5. Tameness and Minkowski's estimate imply that

$$5^g \geqslant |d| \geqslant \left(\frac{\pi e^2}{4}\right)^g \frac{1}{2\pi g e^{1/6g}}. \tag{1}$$

Hence $|G| = g < 37$ and G is solvable. Contradiction.

Now we assume that $K/\mathbb{Q}$ has wild ramification of degree 5^m. Using an embedding of G in $GL(2, \overline{F_5})$, Tate [12] showed that

$$g(2 + \tfrac{1}{5} - \tfrac{1}{4}5^{1-m}) \log 5 \geqslant \log |d|. \tag{2}$$

Assuming the GRH, Poitou [5] showed that

$$\log |d| \geqslant g\left(3.801 - \frac{20.766}{(\log g)^2} - \frac{157.914(1 + 1/g)}{(\log g)^3\left(1 + \dfrac{\pi^2}{(\log g)^2}\right)^2}\right). \tag{3}$$

After rearranging (2) and (3), we obtain

$$\frac{11}{5}(\log 5)\, g \geqslant g\left(3.801 - \frac{20.766}{(\log g)^2} - \frac{157.914(1+1/g)}{(\log g)^3\left(1+\frac{\pi^2}{(\log g)^2}\right)^2}\right) + \frac{\log 5}{4}\frac{g}{5^{m-1}}. \tag{4}$$

LEMMA 3.1. *Let G be as above. Then $|G| \leqslant 75602$.*

Proof. Since G is nonsolvable, Burnside's p^aq^b theorem implies that $|G|$ has at least 3 prime factors. Since 5^m divides g, 5 divides $g/5^{m-1}$. Hence $g/5^{m-1} \geqslant 2 \times 3 \times 5 = 30$. Setting $g/5^{m-1} = 30$ in (4), we have a contradiction for $g \geqslant 75603$. ∎

Consider $\rho: G \hookrightarrow GL(2, 5^n)$. Since ρ is faithful, for brevity, we write G for $\rho(G)$. Note $G/(G \cap SL(2, 5^n))$, which embeds in $GL(2, 5^n)/SL(2, 5^n)$, is cyclic. Hence $G \cap SL(2, 5^n)$ is nonsolvable. By the Feit and Thompson Theorem [2], $|G \cap SL(2, 5^n)|$ is even. Since $-I$ is the only element of order 2 in $SL(2, k)$ for any field k with $\operatorname{char} k \neq 2$, $\{\pm I\}$ is a subgroup of G.

LEMMA 3.2. *Let $\pi: GL(2, 5^n) \to PGL(2, 5^n)$ be the canonical map and let G be as above. Then $\pi(G)$ is isomorphic to $PGL(2, 5)$ or $PSL(2, 5)$.*

Proof. By Dickson [1], the nonsolvability of G implies that $\pi(G)$ is conjugate in $PGL(2, \overline{F_5})$ to $PGL(2, 5^r)$ or $PSL(2, 5^r)$ for some r. Note that $|PSL(2, 5^3)| > 75602$. By Lemma 3.1, $r = 2$ or $r = 1$. Assume $r = 2$. Observe that $|G| = |\pi(G)| \times |\operatorname{Ker} \pi_{|G}|$ where $\operatorname{Ker} \pi_{|G} \supseteq \{\pm I\}$. If $\pi(G) \cong PGL(2, 5^2)$ we have $g \geqslant 15600 \times 2 = 31200$. If $\pi(G) \cong PSL(2, 5^2)$ and $|\operatorname{Ker} \pi_{|G}| > 2$ we have $g \geqslant 7800 \times 4 = 31200$. In either case, $g/5^{m-1} \geqslant 31200/5 = 6240$ and inequality (4) yields the contradiction $110471.818 \geqslant 111324.055$.

If $\pi(G) \cong PSL(2, 5^2)$ and $\operatorname{Ker} \pi_{|G} = \{\pm I\}$ then the inequality does not fail. Instead we show that $G \subseteq SL(2, 25)$ in which case ρ would be even. Since $G \cap SL(2, 25)$ is normal in G and $G/\{\pm I\}$ is simple, $G \cap SL(2, 25) = G$ or $= \{\pm I\}$. Since $G \cap SL(2, 25)$ is nonsolvable, $G \cap SL(2, 25) = G$. That is, $G \subseteq SL(2, 25)$. ∎

We have shown $\pi(G)$ is isomorphic to either $PGL(2, 5) \cong S_5$ or $PSL(2, 5) \cong A_5$. Since G has a quotient isomorphic to one of these groups, K has a subfield with said Galois group. We let K be this subfield and show it fails the ramification hypothesis. In either case, K is the splitting field of a quintic polynomial over $\mathbb{Q}$.

Now that we have limited the possible groups, we use Tate's formula in the reverse direction to bound the discriminant. First we take $\mathrm{Gal}(K/\mathbb{Q}) \cong A_5$ and $m = 1$. By Tate [12],

$$|d(K/\mathbb{Q})| \leqslant 5^{60(2+1/5-1/4)} = 5^{117}.$$

Let L be a subfield of K of degree 5 over $\mathbb{Q}$. Then

$$d(K/\mathbb{Q}) = \mathrm{Norm}_{L/\mathbb{Q}}(d(K/L)) \times d(L/\mathbb{Q})^{12}.$$

So $|d(L/\mathbb{Q})| \leqslant 5^{117/12} = 5^{9.75}$. Similarly for $\mathrm{Gal}(K/\mathbb{Q}) \cong S_5$, $|d(L/\mathbb{Q})| \leqslant 5^{9.75}$.

Finally we verify that there is no quintic field with Galois group isomorphic to S_5 or A_5 and discriminant equal to $\pm 5^m$ where $m \leqslant 9$. We immediately eliminate $m \leqslant 4$ because 5^4 is less than the minimal absolute discriminant (1609) of a degree 5 number field [7]. Then we use Kash 1.8 to access the database maintained by Pohst in Berlin. There we find quintic fields with these discriminants but the largest Galois group among them has order 20. This completes the proof of Theorem 1.1.

Note. This proof cannot be extended to include $l = 7$. Inequality (4) becomes

$$\frac{15}{7}(\log 7)\, g \geqslant g\left(3.801 - \frac{20.766}{(\log g)^2} - \frac{157.914(1+1/g)}{(\log g)^3\left(1+\dfrac{\pi^2}{(\log g)^2}\right)^2}\right) + \frac{\log 7}{6}\frac{g}{7^{m-1}}.$$

Since $\frac{15}{7}(\log 7) > 3.801 + \frac{1}{6}\log 7$, we would not get the contradiction.

REFERENCES

1. L. E. Dickson, "Linear Groups," Dover, New York, 1958.
2. W. Feit and J. Thompson, Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.
3. S. Lang, "Algebraic Number Theory," Springer-Verlag, New York, 1994.
4. A. M. Odlyzko, Lower bounds for discriminants of number fields, *Acta Arith.* **29** (1976), 275–286.
5. G. Poitou, Sur les petits discriminants, *Sém. Delange–Pisot–Poitou* **18** (1976-7), 6-01–6-18.
6. D. J. S. Robinson, "A Course in the Theory of Groups," Springer-Verlag, New York, 1993.

7. A. Schwarz, M. Pohst, and F. Diaz Y Diaz, A table of quintic number fields, *Math. Comp.* **63** (1994), 361–376.
8. J.-P. Serre, "Oeuvres," Vol. III, p. 710, Springer-Verlag, Berlin, 1986.
9. J.-P. Serre, Sur les representations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$), *Duke Math. J.* **54** (1987), 179–230.
10. N. I. Shepherd-Barron and R. Taylor, *mod* 2 and *mod* 5 Icosahedral Representations, *J. Amer. Math. Soc.* **10** (1979), 283–298.
11. D. A. Suprunenko, "Matrix Groups," Am. Math. Soc., Providence, 1976.
12. J. Tate, The non-existence of certain Galois extensions of $\mathbb{Q}$ unramified outside 2, *Contemp. Math.* **174** (1994), 153–156.