PROOF OF A CONJECTURE OF WONG CONCERNING
OCTAHEDRAL GALOIS REPRESENTATIONS OF PRIME
POWER CONDUCTOR

KEVIN CHILDERS AND DARRIN DOUD

Abstract. We prove a conjecture of Siman Wong concerning octahedral Ga-
ois representations of prime power conductor.

1. Introduction

Let \( \bar{\mathbb{Q}} \) denote an algebraic closure of \( \mathbb{Q} \), and write \( G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \). In this paper
a Galois representation is defined as a continuous representation \( \rho : G_{\mathbb{Q}} \to \text{GL}(2, \mathbb{C}) \).
It is well known that such a representation must have finite image. In fact, if
\( \pi : \text{GL}(2, \mathbb{C}) \to \text{PGL}(2, \mathbb{C}) \) is the standard quotient map, \( \tilde{\rho} = \pi \circ \rho \) has an image
that is either cyclic or isomorphic to a dihedral group, \( A_4 \), \( S_4 \), or \( A_5 \). A Galois
representation is said to be odd if it maps complex conjugation to a nonscalar
matrix, and is said to be even otherwise. Given a projective representation \( \tilde{\rho} : G_{\mathbb{Q}} \to \text{PGL}(2, \mathbb{C}) \), a lift of \( \tilde{\rho} \) will be any Galois representation \( \rho : G_{\mathbb{Q}} \to \text{GL}(2, \mathbb{C}) \)
such that \( \tilde{\rho} = \pi \circ \rho \).

A Galois representation is ramified at \( p \) if the image of an inertia group at \( p \)
under \( \rho \) is nontrivial. The conductor of a Galois representation is a product of
powers of primes at which it is ramified. For tamely ramified primes, the exponent
of \( p \) in this product is easily described: if we let \( G_{\mathbb{Q}} \) act on \( \mathbb{C}^2 \) via \( \rho \), the exponent
of \( p \) in the conductor is the codimension of the fixed space of inertia at \( p \). [3, p. 527]

Given a projective representation \( \tilde{\rho} : G_{\mathbb{Q}} \to \text{PGL}(2, \mathbb{C}) \), Serre [4, §6.2] defines the
conductor of \( \tilde{\rho} \) as a product over all primes \( p \) of local conductors. For each prime
\( p \), let \( \tilde{\rho}_p = \tilde{\rho}|_{D_p} \) be the restriction of \( \tilde{\rho} \) to a decomposition group at \( p \). The local
conductor at \( p \) is the minimum conductor of all lifts to \( \text{GL}(2, \mathbb{C}) \) of \( \tilde{\rho}_p \). Each of
these local conductors is a power of \( p \); for unramified primes the exponent is 0, and
for tamely ramified \( p \) the exponent is 1 if the image of \( \tilde{\rho}_p \) is cyclic and 2 otherwise
[4, §6.3].

Because our Galois representations have domain \( G_{\mathbb{Q}} \), we may also describe the
conductor of a projective representation \( \tilde{\rho} \) as the minimum of the conductors of all
the lifts of \( \tilde{\rho} \) [4, §6.2].

Serre [4] classified all odd projective Galois representations of prime conductor,
More recently, Siman Wong [7] studied octahedral representations (representations
with projective image isomorphic to \( S_4 \)) of prime power conductor and made the
following conjecture about these representations:

\[ \text{Date: February 5, 2015.} \]
Theorem 1.1. [7, Conjecture 2] Let $K_4/Q$ be an $S_4$-quartic field such that $|d_{K_4}|$ is a power of a prime $p > 3$. Let $K_3/Q$ be a cubic subfield of the Galois closure of $K_4/Q$. Denote by $\tilde{\rho}$ the projective 2-dimensional Artin representation associated to $K_4/Q$.

1. Suppose $K_3/Q$ is totally real. If $\tilde{\rho}$ has conductor $p^2$, then $v_p(d_{K_4}) = 1$.
2. Suppose $K_3/Q$ is not totally real. If $\tilde{\rho}$ has conductor $p^2$ then $v_p(d_{K_4}) = 3$, otherwise $v_p(d_{K_4}) = 1$.

In this paper, we apply techniques of Serre to prove Wong’s conjecture (see Section 3).

2. Background

For a number field $K$, we will denote the discriminant of $K$ by $d_K$. We note that Stickelberger’s criterion [1, p. 67] implies that for any number field $K$, $d_K$ is congruent to 0 or 1 modulo 4. All discriminants that we consider will be odd, so we will always have $d_K \equiv 1 \pmod{4}$.

Throughout this paper, $K_4/Q$ will denote a field extension of degree 4 with Galois group $S_4$ and discriminant a power of a prime $p > 3$. We will denote by $K_3/Q$ a cubic subextension of the splitting field of $K_4/Q$.

Given $K_4/Q$, there will be an associated projective Galois representation $\tilde{\rho}: G_Q \rightarrow \text{PGL}(2, \mathbb{C})$ with image isomorphic to $S_4$. Since $K_4$ is ramified only at $p$, $\tilde{\rho}$ will be ramified only at $p$ and (since it must be tamely ramified) will have conductor $p$ or $p^2$. In many cases, the following lemmas will help us to determine the conductor of $\tilde{\rho}$. Note that we call a projective representation $\tilde{\rho}$ odd if the image of complex conjugation is nontrivial (i.e. if every lift $\rho$ of $\tilde{\rho}$ is odd).

Lemma 2.1 (Serre). [4, p. 248] Let $\tilde{\rho}$ be any 2-dimensional projective representation of $G_Q$, and $p$ any prime number. Let $i_p = [\tilde{\rho}(I_p)]$, where $I_p$ denotes the inertia group at $p$. Assume that $i_p$ is prime to $p$ and $i_p \geq 3$. Then the conductor of $\tilde{\rho}$ is exactly divisible by $p$ if and only if $i_p|(p-1)$.

Theorem 2.2 (Serre). [4, Theorem 8] Let $K_4/Q$ be an $S_4$-quartic field such that $|d_{K_4}|$ is a power of a single prime $p \equiv 3 \pmod{4}$. Denote by $\tilde{\rho}$ the projective 2-dimensional Artin representation associated to $K_4/Q$, and assume that $\tilde{\rho}$ is odd. Then $\tilde{\rho}$ has conductor $p$ if and only if $d_{K_4} = -p$.

Wong’s conjecture [7, Conjecture 2] relates the $p$-adic valuation of the conductor of $\tilde{\rho}$ to the $p$-adic valuation of $d_{K_4}$. Lemma 2.3 demonstrates that the only possible values $v_p(d_{K_4})$ can take are 1 and 3.

Lemma 2.3. Let $K_4/Q$ be an $S_4$-quartic field such that $|d_{K_4}|$ is a power of a prime $p > 3$. Denote by $e_p$ the ramification index of any prime lying over $p$ in the splitting field of $K_4/Q$. Then $v_p(d_{K_4})$ is either 1 (and $e_p = 2$) or 3 (and $e_p = 4$).

Proof. If there are $g$ primes above $p$ and each has ramification index $e_i$ and inertial degree $f_i$, we know that $4 = e_1 f_1 + \cdots + e_g f_g$ [2, p. 65]. Since the extension is tamely ramified, we have $v_p(d_{K_4}) = (e_1 - 1)f_1 + \cdots + (e_g - 1)f_g$ [5, p. 58]. The following table shows all possible splitting of $p$-adic $K_4$ with ramification, and corresponding discriminants. All $f_i = 1$ unless otherwise noted.
Factorization of $p\mathcal{O}_{K_4}$

<table>
<thead>
<tr>
<th>$e_1 = 2, e_2 = e_4 = 1$</th>
<th>$v_p(d_{K_4})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_1 = 2, f_1 = 2$</td>
<td>2</td>
</tr>
<tr>
<td>$e_1 = 3, e_2 = 1$</td>
<td>2</td>
</tr>
<tr>
<td>$e_1 = e_2 = 2$</td>
<td>2</td>
</tr>
<tr>
<td>$e_1 = 4$</td>
<td>3</td>
</tr>
</tbody>
</table>

Since $p^2 \equiv 1 \pmod{4}$, $v_p(d_{K_4}) = 2$ implies that $d_{K_4} = p^2$ by Stickelberger’s criterion, and $\text{Gal}(K_4/\mathbb{Q})$ will be a subgroup of $A_4$, which is not permitted. Hence, we have that $v_p(d_{K_4})$ is 1 or 3, and we obtain the values of $e_p$ from the table.

Wong’s conjecture involves determining whether the cubic subfield $K_3/\mathbb{Q}$ contained in the Galois closure of $K_4/\mathbb{Q}$ is totally real or complex. The following Lemma interprets this information only in terms of $p \bmod{4}$.

**Lemma 2.4.** Let $K_3/\mathbb{Q}$ be a cubic field extension with Galois group $S_3$, ramified only at a prime $p > 3$. Then $K_3$ is totally real if and only if $p \equiv 1 \pmod{4}$.

**Proof.** Let $p^* = (-1)^{(p-1)/2} p$. Then $p^* \equiv 1 \pmod{4}$. Denote by $L$ the splitting field of $K_3/\mathbb{Q}$, and by $K_2$ the unique quadratic subfield of $L$. Then $K_2 = \mathbb{Q}(\sqrt{p^*})$ is real quadratic if $p \equiv 1 \pmod{4}$ (i.e. $p^* > 0$), and imaginary quadratic if $p \equiv 3 \pmod{4}$ (i.e. $p^* < 0$). Since $L/K_2$ has odd degree, $L$ is totally real if and only if $K_2$.

**3. PROOF OF THE CONJECTURE**

**Proof of Theorem 1.1:** Assume that $K_3/\mathbb{Q}$ is totally real and that $v_p(d_{K_4}) \neq 1$. Then by Lemma 2.4, $p \equiv 1 \pmod{4}$ and by Lemma 2.3 and Stickelberger’s criterion, $d_{K_4} = p^3$ and $e_p = 4$. Since $e_p \geq 3$ and $e_p | (p - 1)$, Lemma 2.1 implies that the conductor of $\tilde{\rho}$ is $p$, proving (1).

Next, suppose that $K_3/\mathbb{Q}$ is not totally real and $v_p(d_{K_4}) \neq 3$. Then $p \equiv 3 \pmod{4}$, $v_p(d_{K_4}) = 1$, and $d_{K_4} = -p$ with $e_p = 2$. By Theorem 2.2, $\tilde{\rho}$ has conductor $p$, and (2) is proven.

**REFERENCES**


