Lifting Galois representations over arbitrary number fields

Yoshiyuki Tomiyama

September 18, 2008

Abstract

It is proved that every two-dimensional residual Galois representation of the absolute Galois group of an arbitrary number field lifts to a characteristic zero $p$-adic representation, if local lifting problems at places above $p$ are unobstructed.

1 Introduction

Let $k$ be a finite field of characteristic $p \geq 3$. Let $K$ be a number field of finite degree over $\mathbb{Q}$ and $G_K$ its absolute Galois group Gal($\bar{K}/K$). We consider continuous representations

$$\bar{\rho}: G_K \to GL_2(k).$$

The central question that we study in this paper is the existence of a lift of $\bar{\rho}$ to $W(k)$, the ring of Witt vectors of $k$. This question has been motivated by a conjecture of Serre ([S1]), that is, all odd absolutely irreducible continuous representations $\rho: G_\mathbb{Q} \to GL_2(k)$ are modular of prescribed weight, level and character. This predicts the existence of a lift to characteristic zero. This conjecture was proved by Khare and Wintenberger in [KW1,KW2]. In [K], Khare proved the existence of lifts to $W(k)$ for any $\rho: G_K \to GL_2(k)$ which are reducible. Ramakrishna proved under very general conditions on $\rho$ that there exist lifts to $W(k)$ for $K = \mathbb{Q}$ in [R1,R2]. Gee’s results ([G]) imply that there exist lifts to $W(k)$ for $p \geq 5$ and $K$ satisfying $[K(\mu_p): K] \geq 3$, where $\mu_p$ is the group of $p$-th roots of unity. Böckle and Khare have proved the general $n$-dimensional case for function fields in [BK]. In this paper, we extend Theorem 1 of [R1] to arbitrary number fields. In particular, we will omit the condition $[K(\mu_p): K] \geq 3$. Hence we can take the field $K$ to be $\mathbb{Q}(\mu_p)^+$, the totally real subfield of $\mathbb{Q}(\mu_p)$.

For a place $v$ of $K$, let $K_v$ be the completion of $K$ at $v$, and let $G_v$ be its absolute Galois group Gal($\bar{K}_v/K_v$). Let $Ad^0 \bar{\rho}$ be the set of all trace zero two-by-two matrices over $k$ with Galois action through $\bar{\rho}$ by conjugation. Our main result is the following:

Theorem. Let $K$ be a number field, and let $\bar{\rho}: G_K \to GL_2(k)$ be a continuous representation with coefficients in a finite field $k$ of characteristic $p \geq 7$. Assume that $H^2(G_v, Ad^0 \bar{\rho}) = 0$ for each places $v | p$. Then $\bar{\rho}$ lifts to a continuous
representation \( \rho : G_K \to \text{GL}_2(\text{W}(k)) \) which is unramified outside a finite set of places of \( K \).

Our method used in the proof is essentially that of Ramakrishna [R1, R2]. In this paper, we follow the more axiomatic treatment presented in [T]. In Section 2, we recall a criterion of Ramakrishna [R2] and Taylor [T] for lifting problems. In Section 3, we define good local lifting problems at certain unramified places and ramified places not dividing \( p \), which will be used in Section 4. In Section 4, we prove Theorem by using the criterion in Section 2 and local lifting problems in Section 3.

Throughout this paper, we assume that \( p \) is a prime \( \geq 7 \).

2 A criterion for lifting problems

In this section we recall a criterion of Ramakrishna [R2] and Taylor [T] for a lifting from a fixed residual Galois representation to a \( p \)-adic Galois representation.

Let \( k \) be a finite field of characteristic \( p \). Throughout this paper, we consider a continuous representation \( \bar{\rho} : G_K \to \text{GL}_2(k) \).

Let \( S \) denote a finite set of places of \( K \) containing the places above \( p \), the infinite places and the places at which \( \bar{\rho} \) is ramified, and let \( K_S \) denote the maximal algebraic extension of \( K \) unramified outside \( S \). Thus \( \bar{\rho} \) factors through \( \text{Gal}(K_S/K) \). Put \( G_{K,S} = \text{Gal}(K_S/K) \). For each place \( v \) of \( K \), we fix an embedding \( \bar{K} \subset \bar{K}_v \). This gives a corresponding continuous homomorphism \( G_v \to G_{K,S} \).

Let \( A \) be the category of complete noetherian local rings \( (R, m_R) \) with residue field \( k \) where the morphisms are homomorphisms that induce the identity map on the residue field.

Fix a continuous homomorphism \( \delta : G_{K,S} \to W(k)^\times \), and for every \( (R, m_R) \in \mathcal{A} \) let \( \delta_R \) be the composition \( \delta_R : G_{K,S} \to W(k)^\times \to R^\times \). Suppose \( \bar{\rho} : G_{K,S} \to \text{GL}_2(k) \) has \( \text{det} \bar{\rho} = \delta_k \).

By a \( \delta \)-lift (resp. \( \delta |_{G_v}, \)-lift) of \( \bar{\rho} \) (resp. \( \bar{\rho} |_{G_v} \)) we mean a continuous representation \( \rho : G_{K,S} \to \text{GL}_2(R) \) (resp. \( \rho_v : G_v \to \text{GL}_2(R) \)) for some \( (R, m_R) \in \mathcal{A} \) such that \( \rho \mod m_R = \bar{\rho} \) (resp. \( \rho_v \mod m_R = \bar{\rho} |_{G_v} \)) and \( \text{det} \rho = \delta_R \) (resp. \( \text{det} \rho_v = \delta_R |_{G_v} \)). Let \( \text{Ad}^0 \rho \) be the set of all trace zero two-by-two matrices over \( k \) with Galois action through \( \bar{\rho} \) by conjugation.

Definition 1. For a place \( v \) of \( K \), we say that a pair \( (\mathcal{C}_v, L_v) \), where \( \mathcal{C}_v \) is a collection of \( \delta |_{G_v} \)-lifts of \( \bar{\rho} |_{G_v} \) and \( L_v \) is a subspace of \( H^1(G_v, \text{Ad}^0 \rho) \), is locally admissible if it satisfies the following conditions:

(P1) \( (k, \bar{\rho} |_{G_v}) \in \mathcal{C}_v \).

(P2) The set of \( \delta |_{G_v} \)-lifts in \( \mathcal{C}_v \) to a fixed ring \( (R, m_R) \in \mathcal{A} \) is closed under conjugation by elements of \( 1 + M_2(m_R) \).

(P3) If \( (R, \rho) \in \mathcal{C}_v \) and \( f : R \to S \) is a morphism in \( \mathcal{A} \) then \( (S, f \circ \rho) \in \mathcal{C}_v \).
(P4) Suppose that \((R_1, \rho_1)\) and \((R_2, \rho_2)\) \(\in\mathcal{C}_v\), and \(I_1\) (resp. \(I_2\)) is an ideal of \(R_1\) (resp. \(R_2\)) and that \(\phi : R_1/I_1 \sim \sim R_2/I_2\) is an isomorphism such that \(\phi(\rho_1 (\text{mod} \ I_1)) = \rho_2 (\text{mod} \ I_2)\). Let \(R_3\) be the fiber product of \(R_1\) and \(R_2\) over \(R_1/I_1 \sim \sim R_2/I_2\). Then \((R_3, \rho_1 \otimes \rho_2) \in \mathcal{C}_v\).

(P5) If \((R, m_R, \rho)\) is a \(\delta|\mathcal{G}_v\)-lift of \(\bar{\rho}|\mathcal{G}_v\) such that each \((R/m_R^n, \rho (\text{mod} \ m_R^n))\) \(\in\mathcal{C}_v\) then \((R, \rho) \in \mathcal{C}_v\).

(P6) For \((R, m_R) \in \mathcal{A}\), suppose that \(I\) is an ideal of \(R\) with \(m_R I = (0)\). If \((R/I, \rho) \in \mathcal{C}_v\) then there is a \(\delta|\mathcal{G}_v\)-lift of \(\bar{\rho}|\mathcal{G}_v\) to \(R\) such that \((R, \bar{\rho}) \in \mathcal{C}_v\) and \(\bar{\rho} (\text{mod} \ I) = \rho\).

(P7) Suppose that \(((R, m_R), \rho_1)\) and \((R, \rho_2)\) are \(\delta|\mathcal{G}_v\)-lifts of \(\bar{\rho}\) with \((R, \rho_1) \in \mathcal{C}_v\), and that \(I\) is an ideal of \(R\) with \(m_R I = (0)\) and \(\rho_1 (\text{mod} \ I) = \rho_2 (\text{mod} \ I)\).
We shall denote by \([\rho_2 - \rho_1]\) an element of \(H^1(G_v, Ad^0 \bar{\rho}) \otimes k\) defined by \(\sigma \mapsto \rho_2(\sigma)\rho_1(\sigma)^{-1} - 1\). Then \([\rho_2 - \rho_1] \in L_v \otimes k\) if and only if \((R, \rho_2) \in \mathcal{C}_v\).

Remark 1. Note that we do regard \(\mathcal{C}_v\) as a functor from \(\mathcal{A}\) to the category of sets.

Let \(S_l\) be the subset of \(S\) consisting of finite places. Throughout this section, suppose that for each \(v \in S_l\) a locally admissible pair \((\mathcal{C}_v, L_v)\) is given.

Let \(\bar{\chi}_p : G_K \rightarrow k^\times\) be the mod \(p\) cyclotomic character. For the \(k[G_K]\)-module \(Ad^0 \bar{\rho}\), by \(Ad^0 \bar{\rho}(i)\) for \(i \in \mathbb{Z}\) we denote the twist of \(Ad^0 \bar{\rho}\) by the \(i\)th tensor power of \(\bar{\chi}_p\), and by \(Ad^0 \bar{\rho}^* := \text{Hom}(Ad^0 \bar{\rho}, k)\) we denote its dual representation. The \(G_K\)-equivariant trace pairing \(Ad^0 \bar{\rho} \times Ad^0 \bar{\rho} \rightarrow k : (A, B) \rightarrow \text{Trace}(AB)\) is perfect. In particular, \(Ad^0 \bar{\rho} \cong Ad^0 \bar{\rho}^*\) as representations. Thus \(Ad^0 \bar{\rho}(1) \cong Ad^0 \bar{\rho}^*(1)\) as representations. By the Tate local duality this induces a perfect pairing
\[ H^1(G_v, Ad^0 \bar{\rho}) \times H^1(G_v, Ad^0 \bar{\rho}(1)) \rightarrow H^2(G_v, k(1)) \cong k. \]

**Definition 2.** A \(\delta\)-lift of type \((\mathcal{C}_v)_{v \in S_l}\) is a \(\delta\)-lift such that \(\rho|\mathcal{G}_v \in \mathcal{C}_v\) for all \(v \in S_l\).

**Definition 3.** We define the Selmer group \(H^1_{\{L_v\}}(G_K, S, Ad^0 \bar{\rho})\) to be the kernel of the map
\[ H^1(G_K, S, Ad^0 \bar{\rho}) \rightarrow \bigoplus_{v \in S_l} H^1(G_v, Ad^0 \bar{\rho})/L_v \]
and the dual Selmer group \(H^1_{\{L^*_v\}}(G_K, S, Ad^0 \bar{\rho}(1))\) to be the kernel of the map
\[ H^1(G_K, S, Ad^0 \bar{\rho}(1)) \rightarrow \bigoplus_{v \in S_l} H^1(G_v, Ad^0 \bar{\rho}(1))/L^*_v \]
where \(L^*_v \subset H^1(G_v, Ad^0 \bar{\rho}(1))\) is the annihilator of \(L_v \subset H^1(G_v, Ad^0 \bar{\rho})\) under the above pairing.

**Proposition 1.** Keep the above notation and assumptions. If
\[ H^1_{\{L^*_v\}}(G_K, S, Ad^0 \bar{\rho}(1)) = 0, \]
then there exists a \(\delta\)-lift of \(\bar{\rho}\) to \(W(k)\) of type \((\mathcal{C}_v)_{v \in S_l}\).
Proof. By Theorem 4.50 of [H] we have the exact sequence
\[ H^1(G_{K,S}, \text{Ad}^0 \bar{\rho}) \rightarrow \bigoplus_{v \in S_t} H^1(G_v, \text{Ad}^0 \bar{\rho})/L_v \rightarrow H^1_{\{L_v\}}(G_{K,S}, \text{Ad}^0 \bar{\rho}(1))^* \]
\[ \rightarrow H^2(G_{K,S}, \text{Ad}^0 \bar{\rho}) \rightarrow \bigoplus_{v \in S_t} H^2(G_v, \text{Ad}^0 \bar{\rho}). \]

Consequently, we see that the map \( \alpha \) is surjective and the map \( \beta \) is injective. Now we construct \( \delta \)-lifts \( \delta \rho \) of \( \bar{\rho} \) to \( W(\mathbf{k})/p^n \) of type \( (\mathcal{C}_v)_{v \in S_t} \) inductively. By the condition (P1), there is nothing to prove for \( n = 1 \). Assume that there is a \( \delta \)-lift \( \rho_{n-1} \) of \( \bar{\rho} \) to \( W(\mathbf{k})/p^{n-1} \) of type \( (\mathcal{C}_v)_{v \in S_t} \). By the condition (P6), for each \( v \in S_t \) we can lift \( \rho_{n-1}|_{G_v} \) to a continuous homomorphism \( \rho_v : G_v \rightarrow \text{GL}_2(W(\mathbf{k})/p^n) \) such that \( (W(\mathbf{k})/p^n, \rho_v) \in \mathcal{C}_v \). Thus we can lift \( \rho_{n-1} \) to a continuous homomorphism \( \rho : G_{K,S} \rightarrow \text{GL}_2(W(\mathbf{k})/p^n) \) by injectivity of the map \( \beta \). By surjectivity of the map \( \alpha \) we may find a class \( \phi \in H^1(G_{K,S}, \text{Ad}^0 \bar{\rho}) \) mapping to
\[(|\rho_v - \rho|_{G_v}) \text{ mod } L_v \in \bigoplus_{v \in S_t} H^1(G_v, \text{Ad}^0 \bar{\rho})/L_v.\]

We define \( \rho_n := (1 + \phi)\rho \). By the condition (P7) the representation \( \rho_n \) is a \( \delta \)-lift of \( \bar{\rho} \) to \( W(\mathbf{k})/p^n \) of type \( (\mathcal{C}_v)_{v \in S_t} \). The induction is now complete. Then we have a \( \delta \)-lift of \( \bar{\rho} \) to \( W(\mathbf{k}) \) of type \( (\mathcal{C}_v)_{v \in S_t} \) by the condition (P5) and the proposition is proved. \( \square \)

3 Local lifting problems

For a place \( v \) of \( K \), consider a continuous homomorphism
\[ \bar{\rho}_v : G_v \rightarrow \text{GL}_2(\mathbf{k}). \]

We denote by \( \hat{\varepsilon} : G_v \rightarrow W(\mathbf{k})^\times \) the Teichmüller lift for any character \( \varepsilon : G_v \rightarrow \mathbf{k}^\times \) and \( \hat{\rho} \in W(\mathbf{k}) \) the Teichmüller lift for any element \( \mu \) of \( \mathbf{k} \). Let \( \chi_p \) be the \( p \)-adic cyclotomic character.

In this section, for ramified places not dividing \( p \) and certain unramified places, we construct a good locally admissible pairs \( (\mathcal{C}_v, L_v) \) with the \( \delta_v := {\text{det}}_{\mathbf{k}} \hat{\rho}_v \hat{\chi}_p \chi_p \), which will be used in Section 4. Let \( I_v \) be the inertia subgroup of \( G_v \). We distinguish following three cases.

3.1 Case I

Suppose \( \bar{\rho}_v \) is unramified and \( v \nmid p \). Suppose that
\[ \bar{\rho}_v(s) = \begin{pmatrix} \lambda & \bar{\lambda} \\ 0 & \lambda \end{pmatrix} \]
and \( q_v \equiv 1 \) mod \( p \), where \( \lambda \) is an element of \( \mathbf{k}^\times \) and \( s \) is a lift of the Frobenius automorphism in \( G_v/I_v \) and \( q_v \) is the order of the residue field of \( K_v \). Note that any \( \delta_v \)-lift of \( \bar{\rho}_v \) factors through the Galois group \( \text{Gal}(K_v^\text{tr}/K_v) \) of the maximal tamely ramified extension \( K_v^\text{tr} \) of \( K_v \). Let \( P_v \) be the wild inertia subgroup of
Moreover, if \( \rho \in \text{Gal}(K_v^1/K_v) \) is generated topologically by \( s \) and \( t \) with the relation \( \rho s t^{-1} = t^3 \). We now define a homomorphism \( \rho_v : G_v \to \text{Gal}(K_v^1/K_v) \to \text{GL}_2(W(\mathfrak{k})[[X]]) \) by

\[
s \mapsto \begin{pmatrix} \lambda q_v & \hat{\lambda} \\ 0 & \hat{\lambda} \end{pmatrix}
\]

and

\[
t \mapsto \begin{pmatrix} 1 & X \\ 0 & 1 \end{pmatrix}.
\]

The images of \( s \) and \( t \) satisfy the relation \( sts^{-1} = t^3 \). We define a pair \((\mathcal{C}_v, L_v)\). The functor \( \mathcal{C}_v : \mathcal{A} \to \text{Sets} \) is given by

\[
\mathcal{C}_v(R) := \{ \rho : G_v \to \text{GL}_2(R) \mid \text{there are } \alpha \in \text{Hom}_\mathcal{A}(W(\mathfrak{k})[[X]], R) \text{ and } M \in 1 + M_2(\mathfrak{m}_R) \text{ such that } \rho = M(\alpha \circ \rho_v)M^{-1} \}.
\]

Moreover, if \( \rho_0 : G_v \to \text{GL}_2(\mathfrak{k}[X]/(X^2)) \) denotes the trivial lift of \( \rho_v \), we define a subspace \( L_v \subset H^1(G_v, \text{Ad}^0 \tilde{\rho}_v) \) to be the set

\[
\{ [c] \in H^1(G_v, \text{Ad}^0 \tilde{\rho}_v) \mid (1 + Xc)\rho_0 \in \mathcal{C}_v(\mathfrak{k}[X]/(X^2)) \}.
\]

**Lemma 1.** We have
(i) \( \dim_k L_v = \dim_k H^1(G_v/I_v, \text{Ad}^0 \tilde{\rho}_v) = 1 \).
(ii) The pair \((\mathcal{C}_v, L_v)\) satisfies the conditions (P1)-(P7) of Definition 1.

**Proof.** (i) First we prove that \( \dim_k H^1(G_v/I_v, \text{Ad}^0 \tilde{\rho}_v) = 1 \). By Proposition 18 of [S2] the dimension of \( H^1(G_v/I_v, \text{Ad}^0 \tilde{\rho}_v) \) is the same as that of \( H^0(G_v, \text{Ad}^0 \tilde{\rho}_v) \).

Thus it suffices to show that \( H^0(G_v, \text{Ad}^0 \tilde{\rho}_v) \) is one-dimensional. This follows from

\[
\begin{pmatrix} \lambda & \lambda \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} 1/\lambda & -1/\lambda \\ 0 & 1/\lambda \end{pmatrix} = \begin{pmatrix} a + c & -2a + b - c \\ c & -(a + c) \end{pmatrix},
\]

where \( a, b, c \in \mathfrak{k} \).

Next we prove that \( \dim_k L_v = 1 \). Let \( f_1 : W[[X]] \to \mathfrak{k}[X]/(X^2) \) be the morphism in \( \mathcal{A} \) determined by \( f_1(X) = X \). We define \( \rho_1 : G_v \to \text{GL}_2(\mathfrak{k}[X]/(X^2)) \) by the composition \( f_1 \circ \rho_v \). The images of \( s \) and \( t \) satisfy the relation \( sts^{-1} = t^3 \).

Let \( c_1 \) be the 1-cocycle corresponding to \( \rho_1 \). The space \( L_v \) is spanned by the class of \( c_1 \). Thus we have \( \dim_k L_v = 1 \).

(ii) The conditions (P1), (P2), (P3), (P6) and (P7) follow from the definition of \((\mathcal{C}_v, L_v)\).

First we prove the condition (P4). Suppose that we have rings \((R_1, \mathfrak{m}_{R_1}), (R_2, \mathfrak{m}_{R_2}) \in \mathcal{A}\), lifts \( \rho_1 \in \mathcal{C}_v(R_1) \), ideals \( I_1 \subset R_1 \), and an identification \( \phi : R_1/I_1 \cong R_2/I_2 \) under which \( \rho_1 \pmod{I_1} = \rho_2 \pmod{I_2} \). Take \( \alpha_i \in \text{Hom}_\mathcal{A}(W(\mathfrak{k})[[X]], R_i) \) and \( M_i \in 1 + M_2(\mathfrak{m}_{R_i}) \) such that \( \rho_i = M_i(\alpha_i \circ \rho_v)M_i^{-1} \), \( i = 1, 2 \). We claim that there exist \( \alpha \in \text{Hom}_\mathcal{A}(W(\mathfrak{k})[[X]], R_3) \) and \( M \in 1 + M_2(\mathfrak{m}_{R_3}) \) such that \( M(\alpha \circ \rho_v)M^{-1} = \rho_1 \oplus \rho_2 \). By conjugating \( \rho_1 \) by some lift of \( M_2 \pmod{I_2} \) to \( R_1 \), we may assume that \( M_2 = 1 \). Since \( \alpha_1 \circ \rho_v(s) = \alpha_2 \circ \rho_v(s) \), the matrix \( M_1 \pmod{I_1} \) commutes with \( (\alpha_1 \pmod{I_1}) \circ \rho_v(s) \). Let

\[
\begin{pmatrix} 1 + m_1 & m_2 \\ 0 & 1 + m_3 \end{pmatrix} \in 1 + M_2(\mathfrak{m}_{R_1}) \text{ be a lift of } M_1 \pmod{I_1}.
\]

Put \( M_1' := \begin{pmatrix} 1 + m_1 & m_2 \\ 0 & 1 + m_3 - x \end{pmatrix} \), \ldots
where $x := (q_v - 1)m_2 - m_1 + m_3$. Note that $x \in I_1$. Then $M'_1 \in 1 + M_2(\mathfrak{m}_{R_v})$ commutes with $\alpha_1 \circ \rho_v(s)$. We now replace $M_1$ by $\tilde{M}_1 := M_1M'_1^{-1}$ and $\alpha_1$ by some $\tilde{\alpha}_1 : W(k)[[X]] \to R_1$ such that $\tilde{M}_1(\tilde{\alpha}_1 \circ \rho_v)\tilde{M}_1^{-1} = M_1(\alpha_1 \circ \rho_v)M_1^{-1}$.

Defining $M := (\tilde{M}_1, 1) \in 1 + M_2(\mathfrak{m}_{R_v})$ and $\alpha := (\tilde{\alpha}_1, \alpha_2) : W(k)[[X]] \to R_3$, the condition (P4) is verified.

Next we prove the condition (P5). Suppose that we have a ring $R \in A$ and a $\delta_v$-lift $\rho$ of $\tilde{\rho}_v$ to $R$ such that each $\rho \pmod{\mathfrak{m}_R^n} \in \mathcal{C}_v(R/\mathfrak{m}_R^n)$. Put $\rho_n := \rho \pmod{\mathfrak{m}_R^n}$. Take $\alpha_n \in \text{Hom}_A(W(k)[[X]], R/\mathfrak{m}_R^n)$ and $M_n \in 1 + M_2(\mathfrak{m}_R/\mathfrak{m}_R^n)$ such that $\rho_n = M_n(\alpha_n \circ \rho_v)M_n^{-1}$. We claim that there exist $\alpha \in \text{Hom}_A(R, R)$ and $M \in 1 + M_2(\mathfrak{m}_R)$ such that $M(\alpha \circ \rho_v)M^{-1} = \rho$. Put $S_n := \{(\alpha'_n, M'_n) | \rho_n = M'_n(\alpha'_n \circ \rho_v)M'_n^{-1}\}$. Since $\mathcal{C}_v(R/\mathfrak{m}_R^n)$ is finite, $S_n$ is finite. For each $n$, $S_n$ is not empty set. Thus $\lim_{\longrightarrow} S_n$ is not empty set, the condition (P5) is verified.

3.2 Case II

Suppose $\tilde{\rho}_v$ is ramified and $v \nmid p$. In addition, suppose $\tilde{\rho}_v(I_v)$ is of order prime to $p$. Define the functor $\mathcal{C}_v : A \to \text{Sets}$ by

$$\mathcal{C}_v(R) := \{\rho : G_v \to \text{GL}_2(R) | \rho \pmod{\mathfrak{m}_R} = \tilde{\rho}_v, \rho(I_v) = \tilde{\rho}_v(I_v), \det \rho = \delta_v\}.$$ Moreover, if $\rho_0 : G_v \to \text{GL}_2(k[X]/(X^2))$ denotes the trivial lift of $\tilde{\rho}_v$, we define a subspace $L_v \subset H^1(G_v, \text{Ad}^0 \tilde{\rho}_v)$ to be the set

$$\{[c] \in H^1(G_v, \text{Ad}^0 \tilde{\rho}_v) | (1 + Xc)\rho_0 \in \mathcal{C}_v(k[X]/(X^2))\}.$$ 

Lemma 2. We have

(i) $\dim_k L_v = \dim_k H^0(G_v, \text{Ad}^0 \tilde{\rho}_v)$.

(ii) The pair $(\mathcal{C}_v, L_v)$ satisfies the conditions (P1)-(P7) of Definition 1.

Proof. This lemma follows from the definitions and the Schur-Zassenhaus theorem.

3.3 Case III

Suppose $\tilde{\rho}_v$ is ramified and $v \nmid p$. In addition, suppose the order of $\tilde{\rho}_v(I_v)$ is divisible by $p$. By Lemma 3.1 of [G], since $p \geq 7$, we may assume that $\tilde{\rho}_v$ is given by the form

$$\tilde{\rho}_v = \begin{pmatrix} \varphi \chi_p & \gamma \\ 0 & \varphi \end{pmatrix},$$

for a character $\varphi : G_v \to k^*$ and a nonzero continuous function $\gamma : G_v \to k$.

The functor $\mathcal{C}_v : A \to \text{Sets}$ is given by

$$\mathcal{C}_v(R) := \{\rho : G_v \to \text{GL}_2(R) \mid \text{there are } \tilde{\gamma} \in \text{Map}(G_v, R) \text{ and } M \in 1 + M_2(\mathfrak{m}_R) \text{ such that } \rho = M \begin{pmatrix} \varphi \chi_p & \tilde{\gamma} \\ 0 & \varphi \end{pmatrix} M^{-1}, \tilde{\gamma} \pmod{\mathfrak{m}_R} = \gamma\}.$$ Moreover, if $\rho_0 : G_v \to \text{GL}_2(k[X]/(X^2))$ denotes the trivial lift of $\tilde{\rho}_v$, we define a subspace $L_v \subset H^1(G_v, \text{Ad}^0 \tilde{\rho}_v)$ to be the set

$$\{[c] \in H^1(G_v, \text{Ad}^0 \tilde{\rho}_v) | (1 + Xc)\rho_0 \in \mathcal{C}_v(k[X]/(X^2))\}.$$
Lemma 3. We have
(i) \( \dim_k L_v = \dim_k H^0(G_v, \text{Ad}^0 \bar{\rho}_v) \).
(ii) The pair \((C_v, L_v)\) satisfies the conditions (P1)-(P7) of Definition 1.

Proof. The proof of this lemma is almost identical argument as in [T, Section 1(E3)].

4 Lifting theorem over arbitrary number fields

In this section, we give a generalization of Theorem 1 of [R1] to arbitrary number fields.

We define \( \delta : G_{K,S} \to W(k) \times \) by \( \boxed{\det \bar{\rho} \chi_p^{-1}} \). Throughout this section, we consider lifts of a fixed determinant \( \delta \) and we always assume the following:

- The order of the image of \( \bar{\rho} \) is divisible by \( p \).

By the Schur-Zassenhaus theorem, if the order of the image of \( \bar{\rho} \) is prime to \( p \), we can find a lift to \( W(k) \) of \( \bar{\rho} \). Since \( p \geq 7 \) and the order of the image of \( \bar{\rho} \) is divisible by \( p \), we see from Section 260 of [D] that the image of \( \bar{\rho} \) is contained in the Borel subgroup of \( GL_2(k) \) or the projective image of \( \bar{\rho} \) is conjugate to either \( PGL_2(F_r) \) or \( PSL_2(F_{p^r}) \) for some \( r \in \mathbb{Z}_{>0} \). In the Borel case, by Theorem 2 of [K] we have a lift of \( \bar{\rho} \) to \( W(k) \). Thus we may assume that the projective image of \( \bar{\rho} \) is equal to \( PSL_2(F_r) \) or \( PGL_2(F_{p^r}) \). Then, by Lemma 17 of [R1], \( \text{Ad}^0 \bar{\rho} \) is an irreducible \( G_{K,S} \)-module. (Note that one may replace the assumption that the image of \( \bar{\rho} \) contains \( SL_2(k) \) in [R1] with the assumption that the projective image of \( \bar{\rho} \) contains \( PSL_2(F_p) \) without affecting the proof.) The irreducibility of \( \text{Ad}^0 \bar{\rho} \) implies that of \( \text{Ad}^0 \bar{\rho}(1) \).

Let \( K(\text{Ad}^0 \bar{\rho}) \) be the fixed field of \( \text{Ker(Ad}^0 \bar{\rho}) \). Put \( E = K(\text{Ad}^0 \bar{\rho})K(\mu_p) \) and \( D = K(\text{Ad}^0 \bar{\rho}) \cap K(\mu_p) \).

Lemma 4. We have
\[ H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}) = H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}(1)) = 0. \]

Proof. First we prove that \( H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}) = 0 \). It suffices to show that \( H^1(\text{SL}_2(F_{p^r}), \text{Ad}^0 \bar{\rho}) = 0 \) and \( H^1(\text{GL}_2(F_{p^r}), \text{Ad}^0 \bar{\rho}) = 0 \), where \( \text{GL}_2(F_{p^r}) \) and \( \text{SL}_2(F_{p^r}) \) act on \( \text{Ad}^0 \bar{\rho} \) by conjugation. By Lemma 2.48 of [DDT], we see \( H^1(\text{SL}_2(F_{p^r}), \text{Ad}^0 \bar{\rho}) = 0 \). Since the index of \( \text{SL}_2(F_{p^r}) \) in \( \text{GL}_2(F_{p^r}) \) is prime to \( p \), we have \( H^1(\text{GL}_2(F_{p^r}), \text{Ad}^0 \bar{\rho}) = 0 \).

Next we prove that \( H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}(1)) = 0 \). As \( D \subset K(\mu_p) \), we see \( \text{Gal}(K(\text{Ad}^0 \bar{\rho})/D) \) contains the commutator subgroup of \( \text{Gal}(K(\text{Ad}^0 \bar{\rho})/K) \). Since the projective image of \( \bar{\rho} \) is equal to \( PSL_2(F_{p^r}) \) or \( PGL_2(F_{p^r}) \), we see this commutator subgroup is just \( PSL_2(F_{p^r}) \). Thus \( \text{Gal}(K(\text{Ad}^0 \bar{\rho})/K)/\text{PSL}_2(F_{p^r}) \to \text{Gal}(D/K) \) is surjective, and so \( [D : K] = 1 \) or 2. Assume that \( [K(\mu_p) : K] = 1 \), then \( H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}(1)) \) is isomorphic to \( H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}) \). Consequently \( H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}(1)) = 0 \).

Assume that \( [K(\mu_p) : K] \geq 3 \), or \( [K(\mu_p) : K] = 2 \) and \( [D : K] = 1 \). We apply the inflation-restriction sequence to \( \text{Gal}(E/K) \) and its normal subgroup \( \text{Gal}(E/K(\text{Ad}^0 \bar{\rho})) \). Since \( \text{Gal}(K_S/E) \) fixes \( \text{Ad}^0 \bar{\rho}(1) \) we see \( \text{Ad}^0 \bar{\rho}(1)^{\text{Gal}(E/K(\text{Ad}^0 \bar{\rho}))} = \text{Ad}^0 \bar{\rho}(1)^{\text{Gal}(K_S/K(\text{Ad}^0 \bar{\rho}))} = \text{Ad}^0 \bar{\rho}(1)^{\text{Gal}(K_S/K(\text{Ad}^0 \bar{\rho}))} \). We get the exact sequence
\[
0 \to H^1(\text{Gal}(K(\text{Ad}^0 \bar{\rho})/K), \text{Ad}^0 \bar{\rho}(1)^{\text{Gal}(K_S/K(\text{Ad}^0 \bar{\rho}))}) \to H^1(\text{Gal}(E/K), \text{Ad}^0 \bar{\rho}(1)) \to H^1(\text{Gal}(E/K(\text{Ad}^0 \bar{\rho})), \text{Ad}^0 \bar{\rho}(1)^{\text{Gal}(K(\text{Ad}^0 \bar{\rho}))/K}).
\]
The last term is trivial as $\text{Gal}(E/K(\text{Ad}^0 \tilde{\rho}))$ has order prime to $p$. As $\text{Gal}(K_S/K(\text{Ad}^0 \tilde{\rho}))$ acts trivially on $\text{Ad}^0 \tilde{\rho}$ we see the action of $\text{Gal}(K_S/K(\text{Ad}^0 \tilde{\rho}))$ is $\chi_p|_{\text{Gal}(K_S/K(\text{Ad}^0 \tilde{\rho}))}$, which is nontrivial, so $\text{Ad}^0 \tilde{\rho}(1)\text{Gal}(K_S/K(\text{Ad}^0 \tilde{\rho})) = 0$. Thus the left term in the sequence is trivial, so $H^1(\text{Gal}(E/K), \text{Ad}^0 \tilde{\rho}(1)) = 0$.

Assume that $[K(\mu_p) : K] = 2$ and $[D : K] = 2$, then we have $K(\mu_p) = D$. Note that $\text{PSL}_2(\mathbb{F}_{p^r})$ has no non-trivial abelian quotients. If the projective image of $\tilde{\rho}$ is $\text{PSL}_2(\mathbb{F}_{p^r})$ for some $r \in \mathbb{Z}_{>0}$, then $\text{Gal}(E/K)$ has no non-trivial abelian quotients. This contradicts the assumption that $[K(\mu_p) : K] = 2$. Hence, we assume that the projective image of $\tilde{\rho}$ is $\text{PGL}_2(\mathbb{F}_{p^r})$ for some $r \in \mathbb{Z}_{>0}$. Since the index of $\text{PSL}_2(\mathbb{F}_{p^r})$ in $\text{PGL}_2(\mathbb{F}_{p^r})$ is equal to the index of $\text{Gal}(E/K(\mu_p))$ in $\text{Gal}(E/K)$, $\text{Gal}(E/K(\mu_p))$ is isomorphic to $\text{PSL}_2(\mathbb{F}_{p^r})$. We have

$$H^1(\text{Gal}(E/K), \text{Ad}^0 \tilde{\rho}(1)) \hookrightarrow H^1(\text{Gal}(E/K(\mu_p)), \text{Ad}^0 \tilde{\rho}(1)).$$

Since $\text{Ad}^0 \tilde{\rho}(1)$ is isomorphic to $\text{Ad}^0 \tilde{\rho}$ as a $\text{Gal}(E/K(\mu_p))$-module and the cohomology group $H^1(\text{Gal}(E/K(\mu_p)), \text{Ad}^0 \tilde{\rho})$ is zero, the proof is complete.

**Lemma 5.** If a pair $(C_w, L_w)$ which is locally admissible is given for each $v \in S_1$ and each elements $\phi \in H^1_{\{\lambda\}}(G_{K,S}, \text{Ad}^0 \tilde{\rho}(1))$ and $\psi \in H^1_{\{\lambda\}}(G_{K,S}, \text{Ad}^0 \tilde{\rho})$ are not zero, then we can find a prime $w \notin S$ and a locally admissible pair $(C_w, L_w)$ such that

1. $\dim_k H^1(G_w/I_w, \text{Ad}^0 \tilde{\rho}) = \dim_k L_w = 1$,
2. the image of $\psi$ in $H^1(G_w/I_w, \text{Ad}^0 \tilde{\rho})$ is not zero,
3. the image of $\phi$ in $H^1(G_w/I_w, \text{Ad}^0 \tilde{\rho}(1))/L_w$ is not zero.

**Proof.** Note that Lemma 4 implies that the restrictions of the cocycles $\psi$ and $\phi$ are non-zero homomorphisms $\phi : \text{Gal}(K_S/E) \to \text{Ad}^0 \tilde{\rho}(1)$ and $\psi : \text{Gal}(K_S/E) \to \text{Ad}^0 \tilde{\rho}$. Let $E_\phi$ and $E_\psi$ be the fixed fields of the respective kernels. Then, $\text{Gal}(E_\phi/E) \to \text{Ad}^0 \tilde{\rho}(1)$ and $\text{Gal}(E_\psi/E) \to \text{Ad}^0 \tilde{\rho}$ are injective homomorphisms of $\mathbb{F}_p[G_{K,S}]$-modules. Since $\text{Ad}^0 \tilde{\rho}$ is irreducible $G_{K,S}$-module, these morphisms are injective, and we see $E_\phi \cap E_\psi = E_\phi(= E_\phi)$ or $E$. If the intersection is $E$, then $\text{Gal}(E_\phi/E_\psi) = \text{Gal}(E_\phi/E) \times \text{Gal}(E_\psi/E)$. If the intersection is $E_\psi$, then $\text{Gal}(E_\phi/E_\psi)$ is isomorphic to $\text{Gal}(E_\phi/E) \times \text{Gal}(E_\phi/E)$. Therefore, $\text{Gal}(E_\phi/E_\psi)$ may be regarded as a $k[\text{Gal}(E/K)]$-module, moreover, natural homomorphisms $\text{Gal}(E_\phi/E_\psi) \to \text{Ad}^0 \tilde{\rho}(1)$ and $\text{Gal}(E_\phi/E_\psi) \to \text{Ad}^0 \tilde{\rho}$ are surjective. Since $\text{PSL}_2(\mathbb{F}_{p^r})$ has no non-trivial abelian quotients, the image of the morphism $\tilde{\rho} \times \chi_p : G_{K,S} \to \text{PSL}_2(k) \times k^\times$ contains $\text{PSL}_2(\mathbb{F}_{p^r}) \times 1$, where $\tilde{\rho}$ is the projective image of $\rho$ and $\chi_p$ is the mod $p$ cyclotomic character of $G_{K,S}$. Thus there is an element $\sigma \in \text{Gal}(E/K)$ such that $\chi_p(\sigma) = 1$ and $\tilde{\rho}(\sigma) = \left( \begin{array}{cc} \lambda & \lambda \\ 0 & \lambda \end{array} \right)$, for some element $\lambda \in k^\times$. We denote by $\tilde{\sigma}$ a lift to $\text{Gal}(E_\phi/E_\psi/K)$ of $\sigma$. Let $L$ be the subset of $\text{Ad}^0 \tilde{\rho}$ whose elements have the form

$$\left( \begin{array}{cc} * & * \\ 0 & * \end{array} \right)$$

and let $L'$ be the subset of $\text{Ad}^0 \tilde{\rho}(1)$ whose elements have the form

$$\left( \begin{array}{cc} * & * \\ 0 & * \end{array} \right).$$

Since $L$ and $L'$ are two-dimensional, there exists $\tau \in \text{Gal}(E_\phi/E_\psi/E)$ such that $\psi(\tau) \notin -\psi(\tilde{\sigma}) + L$ and $\phi(\tau) \notin -\phi(\tilde{\sigma}) + L'$.

By the Cebotarev density theorem, we can choose a place $w \notin S$ which is unramified in $E_\phi/E_\psi/K$ such that $\text{Frob}_w = \tau \tilde{\sigma}$. Take $C_w$ and $L_w$ as in Case I. By Lemma 1 of this paper and Lemma 4.8 of [BK], it follows that $(w, C_w, L_w)$
has the desired properties. (Note that one may replace function fields in [BK] with number fields without affecting the proof.)

**Lemma 6.** Suppose that one is given locally admissible pairs \((C_v, L_v)_{v \in S_1}\) such that

\[
\sum_{v \in S_t} \dim_k L_v \geq \sum_{v \in S} \dim_k H^0(G_v, Ad^0 \bar{\rho}).
\]

Then we can find a finite set of places \(T \supset S\) and locally admissible pairs \((C_v, L_v)_{v \in T \setminus S}\) such that

\[
H^1_{\{L_v\}}(G_{K,T}, Ad^0 \bar{\rho}(1)) = 0.
\]

**Proof.** Suppose that \(0 \neq \phi \in H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1))\). By the assumption of the lemma and Theorem 4.50 of [H], we see that \(\dim_k H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}) \geq \dim_k H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1))\). Then we can find \(0 \neq \psi \in H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho})\).

Thus we can find a place \(w \notin S\) and a locally admissible pair \((C_w, L_w)\) such that

1. \(\dim_k H^1(G_w/I_w, Ad^0 \bar{\rho}) = \dim_k L_w\),
2. \(H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}) \to H^1(G_w/I_w, Ad^0 \bar{\rho})\) is surjective,
3. the image of \(\phi\) in \(H^1(G_w, Ad^0 \bar{\rho}(1))/L_w^+\) is not zero.

by Lemma 5. We have an injection

\[
H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1)) \to H^1_{\{L_v\} \cup \{H^1(G_w, Ad^0 \bar{\rho}(1))\}}(G_{K,S \cup \{w\}}, Ad^0 \bar{\rho}(1))
\]

and we see that its cokernel has order equal to

\[
\#\text{Coker}(H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}) \to H^1(G_w/I_w, Ad^0 \bar{\rho})),
\]

by applying Theorem 4.50 of [H] to

\[
H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1))
\]

and

\[
H^1_{\{L_v\} \cup \{H^1(G_w, Ad^0 \bar{\rho}(1))\}}(G_{K,S \cup \{w\}}, Ad^0 \bar{\rho}(1)).
\]

Thus

\[
H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1)) = H^1_{\{L_v\} \cup \{H^1(G_w, Ad^0 \bar{\rho}(1))\}}(G_{K,S \cup \{w\}}, Ad^0 \bar{\rho}(1)),
\]

and we obtain an exact sequence

\[
0 \to H^1_{\{L_v\} \cup \{L_w\}}(G_{K,S \cup \{w\}}, Ad^0 \bar{\rho}(1)) \to H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1))
\]

\[
\to H^1(G_w, Ad^0 \bar{\rho}(1))/L_w^+.
\]

Hence \(\phi \notin H^1_{\{L_v\} \cup \{L_w\}}(G_{K,S \cup \{w\}}, Ad^0 \bar{\rho}(1)) \subset H^1_{\{L_v\}}(G_{K,S}, Ad^0 \bar{\rho}(1))\). The lemma will follow by repeating such a computation. 

Let \(S'\) denote the set of places of \(K\) consisting of the places above \(p\), the infinite places and the places at which \(\bar{\rho}\) is ramified.
Proof of Theorem. This follows almost at once from Proposition 1 and Lemma 6. For each places $v$ satisfying $v \in S'_f$ and $v \nmid p$, take $C_v$ and $L_v$ as in Case II or Case III. For places $v | p$, take $C_v$ and $L_v$ as the collection of all $\delta|G_v$-lifts of $\bar{\rho}|G_v$ and $H^1(G_v, \text{Ad}^0 \bar{\rho})$, respectively. By Theorem 4.52 of [H] and the assumption of Theorem, we have

$$\sum_{v|p} \dim_k L_v = \sum_{v|p} \dim_k H^0(G_v, \text{Ad}^0 \bar{\rho}) + \sum_{v|p} [K_v : \mathbb{Q}_p] \dim_k \text{Ad}^0 \bar{\rho}$$

and thus we obtain

$$\sum_{v \in S'_f} \dim_k L_v \geq \sum_{v \in S'} \dim_k H^0(G_v, \text{Ad}^0 \bar{\rho}).$$

\[ \square \]

References

[BK] G. Böckle and C. Khare, *Mod $\ell$ representations of arithmetic fundamental groups, I*, Duke Math. J. **129** (2005), 337-369

[D] L. E. Dickson, *Linear Groups*, B. G. Teubner (1901)

[DDT] H. Darmon, F. Diamond, R. Taylor, *Fermat’s Last Theorem*, in: “Elliptic Curves, Modular Forms, and Fermat’s Last Theorem”, J. Coates and S.-T. Yau (eds.), Internat. Press, Cambridge, MA, 1995 pp. 2-140

[G] T. Gee, *Companion forms over totally real fields, II*, Duke Math. J. **136** (2007), 275-284

[H] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Stud. Adv. Math., vol. 69, Cambridge Univ. Press, Cambridge, 2000.

[K] C. Khare, *Base Change, Lifting and Serre’s Conjecture*, J. Number Theory **63** (1997), 387-395

[KW1] C. Khare and J.-P. Wintenberger, *Serre’s modularity conjecture (I)*, preprint

[KW2] C. Khare and J.-P. Wintenberger, *Serre’s modularity conjecture (II)*, preprint

[R1] R. Ramakrishna, *Lifting Galois representations*, Invent. Math. **138** (1999), 537-562

[R2] R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, Ann. of Math. **156** (2002), 115-154

[S1] J.-P. Serre, *Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)*, Duke Math. J. **54** (1987), 179-230

[S2] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, Berlin, 1997, Translated from the French by Patrick Ion

[T] R. Taylor, *On icosahedral Artin representations, II*, Amer. J. Math. **125** (2003), 549-566

10