九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Lifting Galois representations over arbitrary number fields<br>Tomiyama，Yoshiyuki<br>Faculty of Mathematics，Kyushu University

https：／／hdl．handle．net／2324／12551

出版情報：MI Preprint Series．2008－6，2008－10－24．九州大学大学院数理学研究院
バージョン：
権利関係：

# MI Preprint Series 

Kyushu University
The Grobal COE Program
Math-for-Industry Education \& Research Hub

# Lifting Galois representations over arbitrary number fields Yoshiyuki Tomiyama 

MI 2008-6
( Received October 24, 2008 )

Faculty of Mathematics
Kyushu University
Fukuoka, JAPAN

# Lifting Galois representations over arbitrary number fields 

Yoshiyuki Tomiyama

September 16, 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 $\mathbf{k}$ 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 $\operatorname{group} \operatorname{Gal}(\bar{K} / K)$. We consider continuous representations

$$
\bar{\rho}: G_{K} \rightarrow \mathrm{GL}_{2}(\mathbf{k}) .
$$

The central question that we study in this paper is the existence of a lift of $\bar{\rho}$ to $W(\mathbf{k})$, the ring of Witt vectors of $\mathbf{k}$. This question has been motivated by a conjecture of Serre ([S1]), that is, all odd absolutely irreducible continuous representations $\bar{\rho}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_{2}(\mathbf{k})$ 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 $W(\mathbf{k})$ for any $\bar{\rho}: G_{K} \rightarrow \mathrm{GL}_{2}(\mathbf{k})$ which are reducible. Ramakrishna proved under very general conditions on $\bar{\rho}$ that there exist lifts to $W(\mathbf{k})$ for $K=\mathbb{Q}$ in [R1,R2]. Gee's results ([G]) imply that there exist lifts to $W(\mathbf{k})$ for $p \geq 5$ and $K$ satisfying $\left[K\left(\mu_{p}\right): K\right] \geq 3$, where $\mu_{p}$ is the group of $p$-th roots of unity. Böckle and Khare have proved the general $n$-dimensional case for function field in $[\mathrm{BK}]$. In this paper, we extend Theorem 1 of [R1] to arbitrary number fields. In particular, we will omit the condition $\left[K\left(\mu_{p}\right): K\right] \geq 3$. Hence we can take the field $K$ to be $\mathbb{Q}\left(\mu_{p}\right)^{+}$, the totally real subfield of $\mathbb{Q}\left(\mu_{p}\right)$.

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 $\operatorname{Gal}\left(\bar{K}_{v} / K_{v}\right)$. Let $\operatorname{Ad}^{0} \bar{\rho}$ be the set of all trace zero two-by-two matrices over $\mathbf{k}$ with Galois action through $\bar{\rho}$ by conjugation. Our main result is the following:

Theorem. Let $K$ be a number field, and let $\bar{\rho}: G_{K} \rightarrow \mathrm{GL}_{2}(\mathbf{k})$ be a continuous representation with coefficients in a finite field $\mathbf{k}$ of characteristic $p \geq 7$. Assume that $H^{2}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)=0$ for each places $v \mid p$. Then $\bar{\rho}$ lifts to a continuous
representation $\rho: G_{K} \rightarrow \mathrm{GL}_{2}(W(\mathbf{k}))$ 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 $\mathbf{k}$ be a finite field of characteristic $p$. Throughout this paper, we consider a continuous representation

$$
\bar{\rho}: G_{K} \rightarrow \mathrm{GL}_{2}(\mathbf{k})
$$

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 $\operatorname{Gal}\left(K_{S} / K\right)$. Put $G_{K, S}=\operatorname{Gal}\left(K_{S} / K\right)$. For each place $v$ of $K$, we fix an embedding $\bar{K} \subset \bar{K}_{v}$. This gives a corresponding continuous homomorphism $G_{v} \rightarrow G_{K, S}$.

Let $\mathcal{A}$ be the category of complete noetherian local rings $\left(R, \mathfrak{m}_{R}\right)$ with residue field $\mathbf{k}$ where the morphisms are homomorphisms that induce the identity map on the residue field.

Fix a continuous homomorphism $\delta: G_{K, S} \rightarrow W(\mathbf{k})^{\times}$, and for every $\left(R, \mathfrak{m}_{R}\right) \in$ $\mathcal{A}$ let $\delta_{R}$ be the composition $\delta_{R}: G_{K, S} \rightarrow W(\mathbf{k})^{\times} \rightarrow R^{\times}$. Suppose $\bar{\rho}: G_{K, S} \rightarrow$ $\mathrm{GL}_{2}(\mathbf{k})$ has $\operatorname{det} \bar{\rho}=\delta_{\mathbf{k}}$.

By a $\delta$-lift (resp. $\left.\delta\right|_{G_{v}}$-lift) of $\bar{\rho}$ (resp. $\left.\bar{\rho}\right|_{G_{v}}$ ) we mean a continuous representation $\rho: G_{K, S} \rightarrow \mathrm{GL}_{2}(R)$ (resp. $\rho_{v}: G_{v} \rightarrow \mathrm{GL}_{2}(R)$ ) for some $\left(R, \mathfrak{m}_{R}\right) \in \mathcal{A}$ such that $\rho\left(\bmod \mathfrak{m}_{R}\right)=\bar{\rho}\left(\right.$ resp. $\left.\rho_{v}\left(\bmod \mathfrak{m}_{R}\right)=\left.\bar{\rho}\right|_{G_{v}}\right)$ and $\operatorname{det} \rho=\delta_{R}$ (resp. $\operatorname{det} \rho_{v}=\left.\delta_{R}\right|_{G_{v}}$ ). Let $\operatorname{Ad}^{0} \bar{\rho}$ be the set of all trace zero two-by-two matrices over $\mathbf{k}$ with Galois action through $\bar{\rho}$ by conjugation.

Definition 1. For a place $v$ of $K$, we say that a pair $\left(\mathcal{C}_{v}, L_{v}\right)$, where $\mathcal{C}_{v}$ is a collection of $\left.\delta\right|_{G_{v}}$-lifts of $\left.\bar{\rho}\right|_{G_{v}}$ and $L_{v}$ is a subspace of $H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)$, is locally admissible if it satisfies the following conditions:
$(\mathrm{P} 1)\left(\mathbf{k},\left.\bar{\rho}\right|_{G_{v}}\right) \in \mathcal{C}_{v}$.
(P2) The set of $\left.\delta\right|_{G_{v}}$-lifts in $\mathcal{C}_{v}$ to a fixed ring $\left(R, \mathfrak{m}_{R}\right) \in \mathcal{A}$ is closed under conjugation by elements of $1+\mathrm{M}_{2}\left(\mathfrak{m}_{R}\right)$.
(P3) If $(R, \rho) \in \mathcal{C}_{v}$ and $f: R \rightarrow S$ is a morphism in $\mathcal{A}$ then $(S, f \circ \rho) \in \mathfrak{C}_{v}$.
(P4) Suppose that $\left(R_{1}, \rho_{1}\right)$ and $\left(R_{2}, \rho_{2}\right) \in \mathcal{C}_{v}$, and $I_{1}$ (resp. $\left.I_{2}\right)$ is an ideal of $R_{1}$ (resp. $R_{2}$ ) and that $\phi: R_{1} / I_{1} \xrightarrow{\sim} R_{2} / I_{2}$ is an isomorphism such that $\phi\left(\rho_{1}\left(\bmod I_{1}\right)\right)=\rho_{2}\left(\bmod I_{2}\right)$. Let $R_{3}$ be the fiber product of $R_{1}$ and $R_{2}$ over $R_{1} / I_{1} \xrightarrow{\sim} R_{2} / I_{2}$. Then $\left(R_{3}, \rho_{1} \oplus \rho_{2}\right) \in \mathcal{C}_{v}$.
(P5) If $\left(\left(R, \mathfrak{m}_{R}\right), \rho\right)$ is a $\left.\delta\right|_{G_{v}}$-lift of $\left.\bar{\rho}\right|_{G_{v}}$ such that each $\left(R / \mathfrak{m}_{R}^{n}, \rho\left(\bmod \mathfrak{m}_{R}^{n}\right)\right) \in$ $\mathcal{C}_{v}$ then $(R, \rho) \in \mathcal{C}_{v}$.
(P6) For $\left(R, \mathfrak{m}_{R}\right) \in \mathcal{A}$, suppose that $I$ is an ideal of $R$ with $\mathfrak{m}_{R} I=(0)$. If $(R / I, \rho) \in \mathcal{C}_{v}$ then there is a $\left.\delta\right|_{G_{v}}$-lift $\tilde{\rho}$ of $\left.\bar{\rho}\right|_{G_{v}}$ to $R$ such that $(R, \tilde{\rho}) \in \mathcal{C}_{v}$ and $\tilde{\rho}(\bmod I)=\rho$.
(P7) Suppose that $\left(\left(R, \mathfrak{m}_{R}\right), \rho_{1}\right)$ and $\left(R, \rho_{2}\right)$ are $\left.\delta\right|_{G_{v}}$-lifts of $\bar{\rho}$ with $\left(R, \rho_{1}\right) \in \mathcal{C}_{v}$, and that $I$ is an ideal of $R$ with $\mathfrak{m}_{R} I=(0)$ and $\rho_{1}(\bmod I)=\rho_{2}(\bmod I)$. We shall denote by $\left[\rho_{2}-\rho_{1}\right.$ ] an element of $H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right) \otimes_{\mathbf{k}} I$ defined by $\sigma \mapsto \rho_{2}(\sigma) \rho_{1}(\sigma)^{-1}-1$. Then $\left[\rho_{2}-\rho_{1}\right] \in L_{v} \otimes_{\mathbf{k}} I$ if and only if $\left(R, \rho_{2}\right) \in \mathcal{C}_{v}$.

Remark 1. Note that we do regard $\mathcal{C}_{v}$ as a functor from $\mathcal{A}$ to the category of sets.

Let $S_{\mathrm{f}}$ be the subset of $S$ consisting of finite places. Throughout this section, suppose that for each $v \in S_{\mathrm{f}}$ a locally admissible pair $\left(\mathcal{C}_{v}, L_{v}\right)$ is given.

Let $\bar{\chi}_{p}: G_{K} \rightarrow \mathbf{k}^{\times}$be the $\bmod p$ cyclotomic character. For the $\mathbf{k}\left[G_{K}\right]-$ module $\operatorname{Ad}^{0} \bar{\rho}$, by $\operatorname{Ad}^{0} \bar{\rho}(i)$ for $i \in \mathbb{Z}$ we denote the twist of $\operatorname{Ad}^{0} \bar{\rho}$ by the $i$ th tensor power of $\bar{\chi}_{p}$, and by $\operatorname{Ad}^{0} \bar{\rho}^{*}:=\operatorname{Hom}\left(\operatorname{Ad}^{0} \bar{\rho}, \mathbf{k}\right)$ we denote its dual representation. The $G_{K}$-equivariant trace pairing $\operatorname{Ad}^{0} \bar{\rho} \times \operatorname{Ad}^{0} \bar{\rho} \rightarrow \mathbf{k}:(A, B) \mapsto$ Trace $(A B)$ is perfect. In particular, $\operatorname{Ad}^{0} \bar{\rho} \cong \operatorname{Ad}^{0} \bar{\rho}^{*}$ as representations. Thus $\operatorname{Ad}^{0} \bar{\rho}(1) \cong \operatorname{Ad}^{0} \bar{\rho}^{*}(1)$ as representations. By the Tate local duality this induces a perfect pairing

$$
H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right) \times H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) \rightarrow H^{2}\left(G_{v}, \mathbf{k}(1)\right) \cong \mathbf{k}
$$

Definition 2. A $\delta$-lift of type $\left(\mathcal{C}_{v}\right)_{v \in S_{\mathrm{f}}}$ is a $\delta$-lift such that $\left.\rho\right|_{G_{v}} \in \mathcal{C}_{v}$ for all $v \in S_{\mathrm{f}}$.

Definition 3. We define the Selmer group $H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right)$ to be the kernel of the map

$$
H^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right) \rightarrow \bigoplus_{v \in S_{\mathrm{f}}} H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right) / L_{v}
$$

and the dual Selmer group $H_{\left\{L_{\frac{1}{v}}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)$ to be the kernel of the map

$$
H^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) \rightarrow \bigoplus_{v \in S_{\mathrm{f}}} H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) / L_{v}^{\perp}
$$

where $L_{v}^{\perp} \subset H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)$ is the annihilator of $L_{v} \subset H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)$ under the above pairing.

Proposition 1. Keep the above notation and assumptions. If

$$
H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)=0
$$

then there exists a $\delta$-lift of $\bar{\rho}$ to $W(\mathbf{k})$ of type $\left(\mathrm{C}_{v}\right)_{v \in S_{\mathrm{f}}}$.

Proof. By Theorem 4.50 of $[\mathrm{H}]$ we have the exact sequence

$$
\begin{aligned}
H^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right) & \alpha \\
& \left.\rightarrow H_{v \in S_{\mathrm{f}}} H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right) / L_{v} \rightarrow H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right) \stackrel{\beta}{\longrightarrow}(1)\right)^{*} \\
& \bigoplus_{v \in S_{\mathrm{f}}} H^{2}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)
\end{aligned}
$$

Consequently, we see that the map $\alpha$ is surjective and the map $\beta$ is injective. Now we construct $\delta$-lifts $\rho_{n}$ of $\bar{\rho}$ to $W(\mathbf{k}) / p^{n}$ of type $\left(\mathcal{C}_{v}\right)_{v \in S_{\mathrm{f}}}$ 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 $\left(\mathcal{C}_{v}\right)_{v \in S_{\mathrm{f}}}$. By the condition (P6), for each $v \in S_{\mathrm{f}}$ we can lift $\rho_{n-1} \mid G_{v}$ to a continuous homomorphism $\rho_{v}: G_{v} \rightarrow$ $\mathrm{GL}_{2}\left(W(\mathbf{k}) / p^{n}\right)$ such that $\left(W(\mathbf{k}) / p^{n}, \rho_{v}\right) \in \mathcal{C}_{v}$. Thus we can lift $\rho_{n-1}$ to a continuous homomorphism $\rho: G_{K, S} \rightarrow \mathrm{GL}_{2}\left(W(\mathbf{k}) / p^{n}\right)$ by injectivity of the map $\beta$. By surjectivity of the map $\alpha$ we may find a class $\phi \in H^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right)$ mapping to

$$
\left(\left[\rho_{v}-\left.\rho\right|_{G_{v}}\right] \bmod L_{v}\right)_{v \in S_{\mathrm{f}}} \in \bigoplus_{v \in S_{\mathrm{f}}} H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right) / L_{v}
$$

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 $\left(\mathcal{C}_{v}\right)_{v \in S_{\mathrm{f}}}$. The induction is now complete. Then we have a $\delta$-lift of $\bar{\rho}$ to $W(\mathbf{k})$ of type $\left(\mathcal{C}_{v}\right)_{v \in S_{\mathrm{f}}}$ by the condition (P5) and the proposition is proved.

## 3 Local lifting problems

For a place $v$ of $K$, consider a continuous homomorphism

$$
\bar{\rho}_{v}: G_{v} \rightarrow \mathrm{GL}_{2}(\mathbf{k}) .
$$

We denote by $\widehat{\varepsilon}: G_{v} \rightarrow W(\mathbf{k})^{\times}$the Teichmüller lift for any character $\varepsilon: G_{v} \rightarrow$ $\mathbf{k}^{\times}$and $\widehat{\mu} \in W(\mathbf{k})$ 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 $\left(\mathcal{C}_{v}, L_{v}\right)$ with the $\delta_{v}:=$ $\widehat{\operatorname{det}} \bar{\rho} v \widehat{\bar{\chi}}_{p}^{-1} \chi_{p}$, 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

$$
\bar{\rho}_{v}(s)=\left(\begin{array}{cc}
\lambda & \lambda \\
0 & \lambda
\end{array}\right)
$$

and $q_{v} \equiv 1 \bmod p$, 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 $\operatorname{Gal}\left(K_{v}^{\mathrm{t}} / K_{v}\right)$ of the maximal tamely ramified extension $K_{v}^{\mathrm{t}}$ of $K_{v}$. Let $P_{v}$ be the wild inertia subgroup of
$G_{v}$. Let $t$ be a topological generator of $I_{v} / P_{v}$. The Galois group $\operatorname{Gal}\left(K_{v}^{\mathrm{t}} / K_{v}\right)$ is generated topologically by $s$ and $t$ with the relation $s t s^{-1}=t^{q_{v}}$. We now define a homomorphism $\rho_{v}: G_{v} \rightarrow \operatorname{Gal}\left(K_{v}^{\mathrm{t}} / K_{v}\right) \rightarrow \mathrm{GL}_{2}(W(\mathbf{k})[[X]])$ by

$$
s \mapsto\left(\begin{array}{cc}
\widehat{\lambda} q_{v} & \hat{\lambda} \\
0 & \hat{\lambda}
\end{array}\right)
$$

and

$$
t \mapsto\left(\begin{array}{cc}
1 & X \\
0 & 1
\end{array}\right)
$$

The images of $s$ and $t$ satisfy the relation $s t s^{-1}=t^{q_{v}}$. We define a pair $\left(\mathcal{C}_{v}, L_{v}\right)$. The functor $\mathcal{C}_{v}: \mathcal{A} \rightarrow$ Sets is given by

$$
\begin{gathered}
\mathcal{C}_{v}(R):=\left\{\rho: G_{v} \rightarrow \mathrm{GL}_{2}(R) \mid \text { there are } \alpha \in \operatorname{Hom}_{\mathcal{A}}(W(\mathbf{k})[[X]], R)\right. \text { and } \\
\left.M \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R}\right) \text { such that } \rho=M\left(\alpha \circ \rho_{v}\right) M^{-1}\right\} .
\end{gathered}
$$

Moreover, if $\rho_{0}: G_{v} \rightarrow \mathrm{GL}_{2}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)$ denotes the trivial lift of $\bar{\rho}_{v}$, we define a subspace $L_{v} \subset H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$ to be the set

$$
\left\{[c] \in H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right) \mid(1+X c) \rho_{0} \in \mathcal{C}_{v}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)\right\}
$$

Lemma 1. We have
(i) $\operatorname{dim}_{\mathbf{k}} L_{v}=\operatorname{dim}_{\mathbf{k}} H^{1}\left(G_{v} / I_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)=1$.
(ii) The pair $\left(\mathrm{C}_{v}, L_{v}\right)$ satisfies the conditions $(\mathrm{P} 1)-(\mathrm{P} 7)$ of Definition 1.

Proof. (i) First we prove that $\operatorname{dim}_{\mathbf{k}} H^{1}\left(G_{v} / I_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)=1$. By Proposition 18 of [S2] the dimension of $H^{1}\left(G_{v} / I_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$ is the same as that of $H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$. Thus it suffices to show that $H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$ is one-dimensional. This follows from

$$
\left(\begin{array}{cc}
\lambda & \lambda \\
0 & \lambda
\end{array}\right)\left(\begin{array}{cc}
a & b \\
c & -a
\end{array}\right)\left(\begin{array}{cc}
1 / \lambda & -1 / \lambda \\
0 & 1 / \lambda
\end{array}\right)=\left(\begin{array}{cc}
a+c & -2 a+b-c \\
c & -(a+c)
\end{array}\right)
$$

where $a, b, c \in \mathbf{k}$.
Next we prove that $\operatorname{dim}_{\mathbf{k}} L_{v}=1$. Let $f_{1}: W[[X]] \rightarrow \mathbf{k}[X] /\left(X^{2}\right)$ be the morphism in $\mathcal{A}$ determined by $f_{1}(X)=X$. We define $\rho_{1}: G_{v} \rightarrow \mathrm{GL}_{2}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)$ by the composition $f_{1} \circ \rho_{v}$. The images of $s$ and $t$ satisfy the relation $s t s^{-1}=t^{q_{v}}$. 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 $\operatorname{dim}_{\mathbf{k}} L_{v}=1$.
(ii) The conditions (P1), (P2), (P3), (P6) and (P7) follow from the definition of $\left(\mathcal{C}_{v}, L_{v}\right)$.

First we prove the condition (P4). Suppose that we have rings $\left(R_{1}, \mathfrak{m}_{R_{1}}\right),\left(R_{2}, \mathfrak{m}_{R_{2}}\right) \in$ $\mathcal{A}$, lifts $\rho_{i} \in \mathcal{C}_{v}\left(R_{i}\right)$, ideals $I_{i} \subset R_{i}$, and an identification $\phi: R_{1} / I_{1} \xrightarrow{\sim} R_{2} / I_{2}$ under which $\rho_{1}\left(\bmod I_{1}\right)=\rho_{2}\left(\bmod I_{2}\right)$. Take $\alpha_{i} \in \operatorname{Hom}_{\mathcal{A}}\left(W(\mathbf{k})[[X]], R_{i}\right)$ and $M_{i} \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R_{i}}\right)$ such that $\rho_{i}=M_{i}\left(\alpha_{i} \circ \rho_{v}\right) M_{i}^{-1}, i=1$, 2. We claim that there exist $\alpha \in \operatorname{Hom}_{\mathcal{A}}\left(W(\mathbf{k})[[X]], R_{3}\right)$ and $M \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R_{3}}\right)$ such that $M\left(\alpha \circ \rho_{v}\right) M^{-1}=\rho_{1} \oplus \rho_{2}$. By conjugating $\rho_{1}$ by some lift of $M_{2}\left(\bmod I_{2}\right)$ 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 $M_{1}\left(\bmod I_{1}\right)$ commutes with $\left(\alpha_{1}\left(\bmod I_{1}\right)\right) \circ \rho_{v}(s)$. Let $\left(\begin{array}{cc}1+m_{1} & m_{2} \\ 0 & 1+m_{3}\end{array}\right) \in$ $1+\mathrm{M}_{2}\left(\mathfrak{m}_{R_{1}}\right)$ be a lift of $M_{1}\left(\bmod I_{1}\right)$. Put $M_{1}^{\prime}:=\left(\begin{array}{cc}1+m_{1} & m_{2} \\ 0 & 1+m_{3}-x\end{array}\right)$,
where $x:=\left(q_{v}-1\right) m_{2}-m_{1}+m_{3}$. Note that $x \in I_{1}$. Then $M_{1}^{\prime} \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R_{1}}\right)$ commutes with $\alpha_{1} \circ \rho_{v}(s)$. We now replace $M_{1}$ by $\widetilde{M}_{1}:=M_{1} M_{1}^{\prime-1}$ and $\alpha_{1}$ by some $\widetilde{\alpha}_{1}: W(\mathbf{k})[[X]] \rightarrow R_{1}$ such that $\widetilde{M}_{1}\left(\widetilde{\alpha}_{1} \circ \rho_{v}\right) \widetilde{M}_{1}^{-1}=M_{1}\left(\alpha_{1} \circ \rho_{v}\right) M_{1}^{-1}$. Defining $M:=\left(\widetilde{M}_{1}, 1\right) \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R_{3}}\right)$ and $\alpha:=\left(\widetilde{\alpha}_{1}, \alpha_{2}\right): W(\mathbf{k})[[X]] \rightarrow R_{3}$, the condition ( P 4 ) is verified.

Next we prove the condition (P5). Suppose that we have a ring $R \in \mathcal{A}$ and a $\delta_{v}$-lift $\rho$ of $\bar{\rho}_{v}$ to $R$ such that each $\rho\left(\bmod \mathfrak{m}_{R}^{n}\right) \in \mathcal{C}_{v}\left(R / \mathfrak{m}_{R}^{n}\right)$. Put $\rho_{n}:=$ $\rho\left(\bmod \mathfrak{m}_{R}^{n}\right)$. Take $\alpha_{n} \in \operatorname{Hom}_{\mathcal{A}}\left(W(\mathbf{k})[[X]], R / \mathfrak{m}_{R}^{n}\right)$ and $M_{n} \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R} / \mathfrak{m}_{R}^{n}\right)$ such that $\rho_{n}=M_{n}\left(\alpha_{n} \circ \rho_{v}\right) M_{n}^{-1}$. We claim that there exist $\alpha \in \operatorname{Hom}_{\mathcal{A}}\left(R_{v}, R\right)$ and $M \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R}\right)$ such that $M\left(\alpha \circ \rho_{v}\right) M^{-1}=\rho$. Put $S_{n}:=\left\{\left(\alpha_{n}^{\prime}, M_{n}^{\prime}\right) \mid\right.$ $\left.\rho_{n}=M_{n}^{\prime}\left(\alpha_{n}^{\prime} \circ \rho_{v}\right) M_{n}^{\prime-1}\right\}$. Since $\mathcal{C}_{v}\left(R / \mathfrak{m}_{R}^{n}\right)$ is finite, $S_{n}$ is finite. For each $n, S_{n}$ is not empty set. Thus ${\underset{\zeta}{n}}^{\lim } S_{n}$ is not empty set, the condition (P5) is verified.

### 3.2 Case II

Suppose $\bar{\rho}_{v}$ is ramified and $v \nmid p$. In addition, suppose $\bar{\rho}_{v}\left(I_{v}\right)$ is of order prime to $p$. Define the functor $\mathcal{C}_{v}: \mathcal{A} \rightarrow$ Sets by

$$
\mathcal{C}_{v}(R):=\left\{\rho: G_{v} \rightarrow \mathrm{GL}_{2}(R) \mid \rho\left(\bmod \mathfrak{m}_{R}\right)=\bar{\rho}_{v}, \rho\left(I_{v}\right) \xrightarrow{\sim} \bar{\rho}_{v}\left(I_{v}\right), \operatorname{det} \rho=\delta_{v}\right\} .
$$

Moreover, if $\rho_{0}: G_{v} \rightarrow \mathrm{GL}_{2}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)$ denotes the trivial lift of $\bar{\rho}_{v}$, we define a subspace $L_{v} \subset H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$ to be the set

$$
\left\{[c] \in H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right) \mid(1+X c) \rho_{0} \in \mathcal{C}_{v}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)\right\}
$$

Lemma 2. We have
(i) $\operatorname{dim}_{\mathbf{k}} L_{v}=\operatorname{dim}_{\mathbf{k}} H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$.
(ii) The pair $\left(\mathrm{C}_{v}, L_{v}\right)$ 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 $\bar{\rho}_{v}$ is ramified and $v \nmid p$. In addition, suppose the order of $\bar{\rho}_{v}\left(I_{v}\right)$ is divisible by $p$. By Lemma 3.1 of [G], since $p \geq 7$, we may assume that $\bar{\rho}_{v}$ is given by the form

$$
\bar{\rho}_{v}=\left(\begin{array}{cc}
\varphi \bar{\chi}_{p} & \gamma \\
0 & \varphi
\end{array}\right)
$$

for a character $\varphi: G_{v} \rightarrow \mathbf{k}^{\times}$and a nonzero continuous function $\gamma: G_{v} \rightarrow \mathbf{k}$. The functor $\mathcal{C}_{v}: \mathcal{A} \rightarrow$ Sets is given by

$$
\begin{aligned}
\mathcal{C}_{v}(R):=\left\{\rho: G_{v}\right. & \rightarrow \mathrm{GL}_{2}(R) \mid \text { there are } \widetilde{\gamma} \in \operatorname{Map}\left(G_{v}, R\right) \text { and } M \in 1+\mathrm{M}_{2}\left(\mathfrak{m}_{R}\right) \\
& \text { such that } \left.\rho=M\left(\begin{array}{cc}
\widehat{\varphi} \chi_{p} & \widetilde{\gamma} \\
0 & \widehat{\varphi}
\end{array}\right) M^{-1}, \widetilde{\gamma} \bmod \mathfrak{m}_{R}=\gamma\right\} .
\end{aligned}
$$

Moreover, if $\rho_{0}: G_{v} \rightarrow \mathrm{GL}_{2}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)$ denotes the trivial lift of $\bar{\rho}_{v}$, we define a subspace $L_{v} \subset H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$ to be the set

$$
\left\{[c] \in H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right) \mid(1+X c) \rho_{0} \in \mathcal{C}_{v}\left(\mathbf{k}[X] /\left(X^{2}\right)\right)\right\} .
$$

Lemma 3. We have
(i) $\operatorname{dim}_{\mathbf{k}} L_{v}=\operatorname{dim}_{\mathbf{k}} H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}_{v}\right)$.
(ii) The pair $\left(\mathrm{C}_{v}, L_{v}\right)$ 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 $\delta: G_{K, S} \rightarrow W(\mathbf{k})^{\times}$by $\widehat{\operatorname{det} \bar{\rho}} \hat{\chi}_{p}^{-1} \chi_{p}$. 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 $W(\mathbf{k})$ 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 $\mathrm{GL}_{2}(\mathbf{k})$ or the projective image of $\bar{\rho}$ is conjugate to either $\mathrm{PGL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ or $\mathrm{PSL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ for some $r \in \mathbb{Z}_{>0}$. In the Borel case, by Theorem 2 of $[\mathrm{K}]$ we have a lift of $\bar{\rho}$ to $W(\mathbf{k})$. Thus we may assume that the projective image of $\bar{\rho}$ is equal to $\mathrm{PSL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ or $\mathrm{PGL}_{2}\left(\mathbb{F}_{p^{r}}\right)$. Then, by Lemma 17 of $[\mathrm{R} 1], \mathrm{Ad}^{0} \bar{\rho}$ is an irreducible $G_{K, S}$-module. (Note that one may replace the assumption that the image of $\bar{\rho}$ contains $\mathrm{SL}_{2}(\mathbf{k})$ in [R1] with the assumption that the projective image of $\bar{\rho}$ contains $\operatorname{PSL}_{2}\left(\mathbb{F}_{p}\right)$ without affecting the proof.) The irreducibility of $\operatorname{Ad}^{0} \bar{\rho}$ implies that of $\operatorname{Ad}^{0} \bar{\rho}(1)$.

Let $K\left(\operatorname{Ad}^{0} \bar{\rho}\right)$ be the fixed field of $\operatorname{Ker}\left(\operatorname{Ad}^{0} \bar{\rho}\right)$. Put $E=K\left(\operatorname{Ad}^{0} \bar{\rho}\right) K\left(\mu_{p}\right)$ and $D=K\left(\operatorname{Ad}^{0} \bar{\rho}\right) \cap K\left(\mu_{p}\right)$.
Lemma 4. We have

$$
H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}\right)=H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right)=0
$$

Proof. First we prove that $H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}\right)=0$. It suffices to show that $H^{1}\left(\mathrm{SL}_{2}\left(\mathbb{F}_{p^{r}}\right), \mathrm{Ad}^{0} \bar{\rho}\right)=0$ and $H^{1}\left(\mathrm{GL}_{2}\left(\mathbb{F}_{p^{r}}\right), \operatorname{Ad}^{0} \bar{\rho}\right)=0$, where $\mathrm{GL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ and $\mathrm{SL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ act on $\mathrm{Ad}^{0} \bar{\rho}$ by conjugation. By Lemma 2.48 of [DDT], we see $H^{1}\left(\mathrm{SL}_{2}\left(\mathbb{F}_{p^{r}}\right), \mathrm{Ad}^{0} \bar{\rho}\right)=0$. Since the index of $\mathrm{SL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ in $\mathrm{GL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ is prime to $p$, we have $H^{1}\left(\mathrm{GL}_{2}\left(\mathbb{F}_{p^{r}}\right), \operatorname{Ad}^{0} \bar{\rho}\right)=0$.

Next we prove that $H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right)=0$. As $D \subset K\left(\mu_{p}\right)$, we see $\operatorname{Gal}\left(K\left(\operatorname{Ad}^{0} \bar{\rho}\right) / D\right)$ contains the commutator subgroup of $\operatorname{Gal}\left(K\left(\operatorname{Ad}^{0} \bar{\rho}\right) / K\right)$. Since the projective image of $\bar{\rho}$ is equal to $\mathrm{PSL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ or $\mathrm{PGL}_{2}\left(\mathbb{F}_{p^{r}}\right)$, we see this commutator subgroup is just $\mathrm{PSL}_{2}\left(\mathbb{F}_{p^{r}}\right)$. Thus $\operatorname{Gal}\left(K\left(\operatorname{Ad}^{0} \bar{\rho}\right) / K\right) / \mathrm{PSL}_{2}\left(\mathbb{F}_{p^{r}}\right) \rightarrow$ $\operatorname{Gal}(D / K)$ is surjective, and so $[D: K]=1$ or 2 . Assume that $\left[K\left(\mu_{p}\right)\right.$ : $K]=1$, then $H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right)$ is isomorphic to $H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}\right)$. Consequently $H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right)=0$.

Assume that $\left[K\left(\mu_{p}\right): K\right] \geq 3$, or $\left[K\left(\mu_{p}\right): K\right]=2$ and $[D: K]=1$. We apply the inflation-restriction sequence to $\operatorname{Gal}(E / K)$ and its normal subgroup $\operatorname{Gal}\left(E / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)$. Since $\operatorname{Gal}\left(K_{S} / E\right)$ fixes $\operatorname{Ad}^{0} \bar{\rho}(1)$ we see $\operatorname{Ad}^{0} \bar{\rho}(1)^{\operatorname{Gal}\left(E / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)}=$ $\operatorname{Ad}^{0} \bar{\rho}(1)^{\operatorname{Gal}\left(K_{S} / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)}$. We get the exact sequence

$$
\begin{aligned}
0 & \rightarrow H^{1}\left(\operatorname{Gal}\left(K\left(\operatorname{Ad}^{0} \bar{\rho}\right) / K\right), \operatorname{Ad}^{0} \bar{\rho}(1)^{\operatorname{Gal}\left(K_{S} / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)}\right) \rightarrow H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right) \\
& \rightarrow H^{1}\left(\operatorname{Gal}\left(E / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right), \operatorname{Ad}^{0} \bar{\rho}(1)\right)^{\operatorname{Gal}\left(K\left(\operatorname{Ad}^{0} \bar{\rho}\right) / K\right)} .
\end{aligned}
$$

The last term is trivial as $\operatorname{Gal}\left(E / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)$ has order prime to $p$. As $\operatorname{Gal}\left(K_{S} / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)$ acts trivially on $\operatorname{Ad}^{0} \bar{\rho}$ we see the action of $\operatorname{Gal}\left(K_{S} / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)$ is $\left.\chi_{p}\right|_{\operatorname{Gal}\left(K_{S} / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)}$, which is nontrivial, so $\operatorname{Ad}^{0} \bar{\rho}(1)^{\operatorname{Gal}\left(K_{S} / K\left(\operatorname{Ad}^{0} \bar{\rho}\right)\right)}=0$. Thus the left term in the sequence is trivial, so $H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right)=0$.

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

$$
H^{1}\left(\operatorname{Gal}(E / K), \operatorname{Ad}^{0} \bar{\rho}(1)\right) \hookrightarrow H^{1}\left(\operatorname{Gal}\left(E / K\left(\mu_{p}\right)\right), \operatorname{Ad}^{0} \bar{\rho}(1)\right)
$$

Since $\operatorname{Ad}^{0} \bar{\rho}(1)$ is isomorphic to $\operatorname{Ad}^{0} \bar{\rho}$ as a $\operatorname{Gal}\left(E / K\left(\mu_{p}\right)\right)$-module and the cohomology group $H^{1}\left(\operatorname{Gal}\left(E / K\left(\mu_{p}\right)\right), \operatorname{Ad}^{0} \bar{\rho}\right)$ is zero, the proof is complete.

Lemma 5. If a pair $\left(\mathcal{C}_{v}, L_{v}\right)$ which is locally admissible is given for each $v \in S_{\mathrm{f}}$ and each elements $\phi \in H_{\left\{L_{v}\right.}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)$ and $\psi \in H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right)$ are not zero, then we can find a prime $w \notin S$ and a locally admissible pair $\left(\mathrm{C}_{w}, L_{w}\right)$ such that
(1) $\operatorname{dim}_{\mathbf{k}} H^{1}\left(G_{w} / I_{w}, \operatorname{Ad}^{0} \bar{\rho}\right)=\operatorname{dim}_{\mathbf{k}} L_{w}=1$,
(2) the image of $\psi$ in $H^{1}\left(G_{w} / I_{w}, \operatorname{Ad}^{0} \bar{\rho}\right)$ is not zero,
(3) the image of $\phi$ in $H^{1}\left(G_{w}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) / L_{w}^{\perp}$ is not zero.

Proof. Note that Lemma 4 implies that the restrictions of the cocycles $\psi$ and $\phi$ are non-zero homomorphisms $\phi: \operatorname{Gal}\left(K_{S} / E\right) \rightarrow \operatorname{Ad}^{0} \bar{\rho}(1)$ and $\psi: \operatorname{Gal}\left(K_{S} / E\right) \rightarrow$ $\operatorname{Ad}^{0} \bar{\rho}$. Let $E_{\phi}$ and $E_{\psi}$ be the fixed fields of the respective kernels. Then, $\operatorname{Gal}\left(E_{\phi} / E\right) \rightarrow \operatorname{Ad}^{0} \bar{\rho}(1)$ and $\operatorname{Gal}\left(E_{\psi} / E\right) \rightarrow \operatorname{Ad}^{0} \bar{\rho}$ are injective homomorphisms of $\mathbb{F}_{p}\left[G_{K, S}\right]$-modules. Since $\operatorname{Ad}^{0} \bar{\rho}$ is irreducible $G_{K, S}$-module, these morphisms are bijective, and we see $E_{\phi} \cap E_{\psi}=E_{\psi}\left(=E_{\phi}\right)$ or $E$. If the intersection is $E$, then $\operatorname{Gal}\left(E_{\phi} E_{\psi} / E\right)$ is isomorphic to $\operatorname{Gal}\left(E_{\phi} / E\right) \times \operatorname{Gal}\left(E_{\psi} / E\right)$. If the intersection is $E_{\psi}$, then $\operatorname{Gal}\left(E_{\phi} E_{\psi} / E\right)$ is isomorphic to $\operatorname{Gal}\left(E_{\psi} / E\right)$ and $\operatorname{Gal}\left(E_{\phi} / E\right)$. Therefore, $\operatorname{Gal}\left(E_{\phi} E_{\psi} / E\right)$ may be regarded as a $\mathbf{k}[\operatorname{Gal}(E / K)]$-module, moreover, natural homomorphisms $\operatorname{Gal}\left(E_{\phi} E_{\psi} / E\right) \rightarrow \operatorname{Ad}^{0} \bar{\rho}(1)$ and $\operatorname{Gal}\left(E_{\phi} E_{\psi} / E\right) \rightarrow \operatorname{Ad}^{0} \bar{\rho}$ are surjective. Since $\underset{\sim}{\operatorname{P}} \mathrm{PLL}_{2}\left(\mathbb{F}_{p^{r}}\right)$ has no non-trivial abelian quotients, the image of the morphism $\widetilde{\bar{\rho}} \times \chi_{p}: G_{K, S} \rightarrow \mathrm{PGL}_{2}(\mathbf{k}) \times \mathbf{k}^{\times}$contains $\mathrm{PSL}_{2}\left(\mathbb{F}_{p^{r}}\right) \times 1$, where $\widetilde{\bar{\rho}}$ is the projective image of $\bar{\rho}$ and $\chi_{p}$ is the $\bmod p$ cyclotomic character of $G_{K, S}$. Thus there is an element $\sigma \in \operatorname{Gal}(E / K)$ such that $\chi_{p}(\sigma)=1$ and $\bar{\rho}(\sigma)=\left(\begin{array}{cc}\lambda & \lambda \\ 0 & \lambda\end{array}\right)$, for some element $\lambda \in \mathbf{k}^{\times}$. We denote by $\widetilde{\sigma}$ a lift to $\operatorname{Gal}\left(E_{\phi} E_{\psi} / K\right)$ of $\sigma$. Let $L$ be the subset of $\operatorname{Ad}^{0} \bar{\rho}$ whose elements have the form $\left(\begin{array}{cc}* & * \\ 0 & *\end{array}\right)$ and let $L^{\prime}$ be the subset of $\operatorname{Ad}^{0} \bar{\rho}(1)$ whose elements have the form $\left(\begin{array}{cc}* & * \\ 0 & *\end{array}\right)$. Since $L$ and $L^{\prime}$ are two-dimensional, there exists $\tau \in \operatorname{Gal}\left(E_{\phi} E_{\psi} / E\right)$ such that $\psi(\tau) \notin-\psi(\widetilde{\sigma})+L$ and $\phi(\tau) \notin-\phi(\widetilde{\sigma})+L^{\prime}$.

By the Cebotarev density theorem, we can choose a place $w \notin S$ which is unramified in $E_{\phi} E_{\psi} / K$ such that $\mathrm{Frob}_{w}=\tau \widetilde{\sigma}$. Take $\mathcal{C}_{w}$ and $L_{w}$ as in Case I. By Lemma 1 of this paper and Lemma 4.8 of [BK], it follows that ( $w, \mathcal{C}_{w}, L_{w}$ )
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 $\left(\mathcal{C}_{v}, L_{v}\right)_{v \in S_{\mathrm{f}}}$ such that

$$
\sum_{v \in S_{\mathrm{f}}} \operatorname{dim}_{\mathbf{k}} L_{v} \geq \sum_{v \in S} \operatorname{dim}_{\mathbf{k}} H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right) .
$$

Then we can find a finite set of places $T \supset S$ and locally admissible pairs $\left(\mathrm{C}_{v}, L_{v}\right)_{v \in T \backslash S}$ such that

$$
H_{\left\{L_{v}^{⿺}\right\}}^{1}\left(G_{K, T}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)=0 .
$$

Proof. Suppose that $0 \neq \phi \in H_{\left\{L_{\nu}^{\perp}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)$. By the assumption of the lemma and Theorem 4.50 of $[\mathrm{H}]$, we see that $\operatorname{dim}_{\mathbf{k}} H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right) \geq$ $\operatorname{dim}_{\mathbf{k}} H_{\left\{L_{v}^{\perp}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)$. Then we can find $0 \neq \psi \in H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right)$. Thus we can find a place $w \notin S$ and a locally admissible pair $\left(\mathcal{C}_{w}, L_{w}\right)$ such that (1) $\operatorname{dim}_{\mathbf{k}} H^{1}\left(G_{w} / I_{w}, \operatorname{Ad}^{0} \bar{\rho}\right)=\operatorname{dim}_{\mathbf{k}} L_{w}$,
(2) $H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right) \rightarrow H^{1}\left(G_{w} / I_{w}, \operatorname{Ad}^{0} \bar{\rho}\right)$ is surjective,
(3) the image of $\phi$ in $H^{1}\left(G_{w}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) / L_{w}^{\perp}$ is not zero, by Lemma 5 . We have an injection

$$
H_{\left\{L_{v}^{\perp}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) \hookrightarrow H_{\left\{L_{v}^{\perp}\right\} \cup\left\{H^{1}\left(G_{w}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)\right\}}^{1}\left(G_{K, S \cup\{w\}}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)
$$

and we see that its cokernel has order equal to

$$
\# \operatorname{Coker}\left(H_{\left\{L_{v}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}\right) \rightarrow H^{1}\left(G_{w} / I_{w}, \operatorname{Ad}^{0} \bar{\rho}\right)\right)
$$

by applying Theorem 4.50 of $[\mathrm{H}]$ to

$$
H_{\left\{L_{v}^{\perp}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)
$$

and

$$
H_{\left\{L_{v}^{\perp}\right\} \cup\left\{H^{1}\left(G_{w}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)\right\}}^{1}\left(G_{K, S \cup\{w\}}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) .
$$

Thus

$$
H_{\left\{L_{\frac{1}{v}}^{1}\right.}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)=H_{\left\{L_{v}^{\perp}\right\} \cup\left\{H^{1}\left(G_{w}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)\right\}}^{1}\left(G_{K, S \cup\{w\}}, \operatorname{Ad}^{0} \bar{\rho}(1)\right),
$$

and we obtain an exact sequence

$$
\begin{aligned}
0 & \rightarrow H_{\left\{L_{v}^{\perp}\right\} \cup\left\{L_{w}^{\perp}\right\}}^{1}\left(G_{K, S \cup\{w\}}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) \rightarrow H_{\left\{L_{v}^{\perp}\right\}}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) \\
& \rightarrow H^{1}\left(G_{w}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) / L_{w}^{\perp} .
\end{aligned}
$$

Hence $\phi \notin H_{\left\{L_{v}^{\perp}\right\} \cup\left\{L_{w}^{\perp}\right\}}^{1}\left(G_{K, S \cup\{w\}}, \operatorname{Ad}^{0} \bar{\rho}(1)\right) \subset H_{\left\{L_{v}^{\frac{1}{v}}\right.}^{1}\left(G_{K, S}, \operatorname{Ad}^{0} \bar{\rho}(1)\right)$. The lemma will follow by repeating such a computation.

Let $S^{\prime}$ 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 $v \in S_{\mathrm{f}}^{\prime}$ and $v \nmid p$, take $\mathcal{C}_{v}$ and $L_{v}$ as in Case II or Case III. For places $v \mid p$, take $\mathcal{C}_{v}$ and $L_{v}$ as the collection of all $\left.\delta\right|_{G_{v}}$-lifts of $\left.\bar{\rho}\right|_{G_{v}}$ and $H^{1}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)$, respectively. By Theorem 4.52 of $[\mathrm{H}]$ and the assumption of Theorem, we have

$$
\sum_{v \mid p} \operatorname{dim}_{\mathbf{k}} L_{v}=\sum_{v \mid p} \operatorname{dim}_{\mathbf{k}} H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)+\sum_{v \mid p}\left[K_{v}: \mathbb{Q}_{p}\right] \operatorname{dim}_{\mathbf{k}} \operatorname{Ad}^{0} \bar{\rho}
$$

and thus we obtain

$$
\sum_{v \in S_{\mathbf{f}}^{\prime}} \operatorname{dim}_{\mathbf{k}} L_{v} \geq \sum_{v \in S^{\prime}} \operatorname{dim}_{\mathbf{k}} H^{0}\left(G_{v}, \operatorname{Ad}^{0} \bar{\rho}\right)
$$

## 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 $\operatorname{Gal}(\overline{\mathbb{Q}} / \mathbb{Q})$, 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

# List of MI Preprint Series, Kyushu University <br> The Grobal COE Program Math-for-Industry Education \& Research Hub 

Abstract collision systems simulated by cellular automata

## 2008-2 Eiji Onodera

The intial value problem for a third-order dispersive flow into compact almost Hermitian manifolds

2008-3 Hiroaki Kido
On isosceles sets in the 4-dimensional Euclidean space

2008-4 Hirofumi NOTSU
Numerical computations of cavity flow problems by a pressure stabilized characteristiccurve finite element scheme

2008-5 Yoshiyasu Ozeki
Torsion points of abelian varieties with values in nfinite extensions over a padic field

2008-6 Yoshiyuki Tomiyama
Lifting Galois representations over arbitrary number fields

